Australian Government
Office of the Australian Information Commissioner

GovTEAMS OFFICIAL – OAIC USER REGISTRATION		
General	https://www.govteams.gov.au/about-govteams-official	
Have you discussed using GovTEAMS Official with the Corporate Services team (including the creation of Communities if required)?	**Yes** ☐ **No** ☐	**Date** *Click to enter a date.*
What would you like to call the GovTEAMS Community?		
OAIC GovTEAMS Community administrator name & name of backup? **NOTE: Corporate Services are the default co-administators of all OAIC GovTEAMS OFFICIAL communities and will be included as Community owners**		**Name** **Backup name**
Have you included a Corporate Services team member as an Owner in your GovTEAMS Community?	**Yes** ☐ **No** ☐	
Have you discussed the privacy risks and/or security risks with the Governance & Risk team?	**Yes** ☐ **No** ☐	**Date** *Click to enter a date.*
Have you discussed handling of classified material with the Corporate Services Team?	**Yes** ☐ **No** ☐	**Date** *Click to enter a date.*
Have you obtained your Assistant Commissioner's approval (please attach a copy)?	**Yes** ☐ **No** ☐	**Date** *Click to enter a date.*
On completion please submit this form to informationmanagement@oaic.gov.au	**Name/position**	**Date** *Click to enter a date.*
Endorsed by Chief Information Officer		**Date** *Click to enter a date.*

OAIC

Uploading/downloading/reviewing material to/from/within GovTEAMS OFFICIAL?	**Yes/No**	**Details**	
a. Is the material going to be uploaded to another organisation from an OAIC GovTEAMS Community?	**Yes** ☐ **No** ☐		
b. Is the material going to be downloaded from another organisation into an OAIC GovTEAMS Community?	**Yes** ☐ **No** ☐		
c. Please indicate if you are only reviewing material in GovTEAMS	**Yes** ☐ **No** ☐		
d. Name of organisation and contact information including security clearance details of contact			
e. Name of GovTEAMS collaboration Community (OAIC or external Community)			
f. Does the material contain sensitive and/or personal information?	**Yes** ☐ **No** ☐		
g. Does the material contain classified information?	**Yes** ☐ **No** ☐		
h. **Upload**: how will the recipient be storing the material and disposing of it once finished with?			
i. **Download**: where is the material stored within OAIC systems (provide container or case number)?		**Content Manager**	**Resolve**

Australian Government

Getting started with GovTEAMS

User guide

Contents

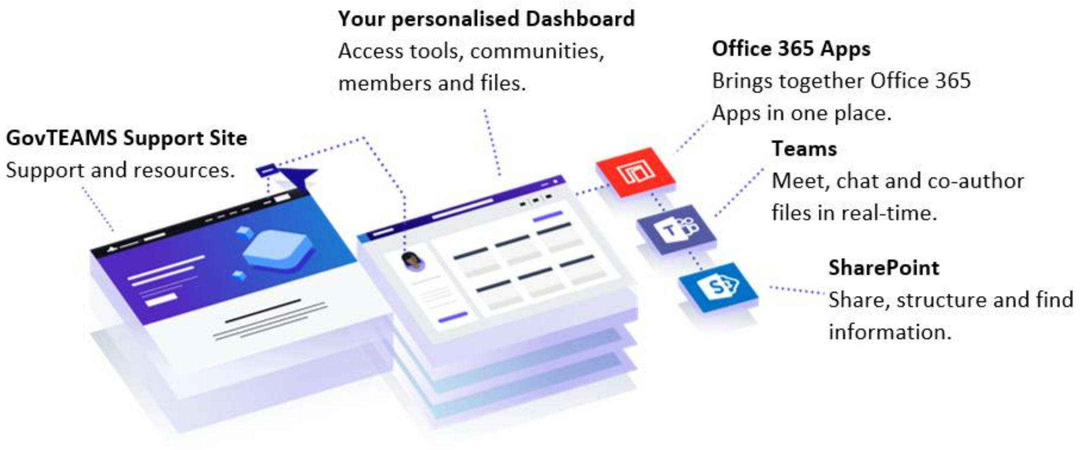
GovTEAMS

Connecting all tiers of government, industry and partners to deliver for Australians. Meet online with video or audio, instantly connect through chat and collaborate on documents together, from anywhere.

The basics

When you login to GovTEAMS you'll land on your **personalised dashboard**. You can access tools, communities, members and files from here.

The main apps you'll use in **your workspace** are Microsoft Teams and SharePoint. You'll also have access to all the available Office 365 apps in one place.


Your personalised Dashboard
Access tools, communities, members and files.
Office 365 Apps
Brings together Office 365 Apps in one place.
GovTEAMS Support Site
Support and resources.
Teams
Meet, chat and co-author files in real-time.
SharePoint
Share, structure and find information.

Why GovTEAMS?

There is nothing else like it in government.

GovTEAMS has the features you need to work better from wherever you are across boundaries:

- ✓ Your online workspace
  - Access all the tools you need in one place
  - Create communities and bring teams together
  - Promote activities, build a network or start a project
- ✓ Trusted and secure
  - Your privacy and data is our priority
  - It's secure and compliant with government standards
  - Classified to OFFICIAL: Sensitive
- ✓ Tools to make your job easier
  - Microsoft Teams – Meet, chat and co-author files in real-time
  - SharePoint – Share, structure and find information
  - Office 365 apps – Work on the go with the tools you know
- ✓ Personal profile
  - Discover communities based on your information
  - Promote your skills and help employers find you
  - Connect with likeminded people and grow your network

GovTEAMS Registration

Before you start – make sure you have access to your work email and a phone.

Who can register?

- **Commonwealth Government employees** can register as a **member**. As a member, you can access all available features. You can also be a **community owner** and invite other members and guests to your community.
- **State government employees** can register as a **guest**. You'll be added to the demonstration community to try out GovTEAMS, at no cost. Community owners can invite you to their communities. As a guest, you can only access features in the community you're invited to.
- **State government employees** can buy a **state owner account for $350** per user per annum (at least two owners are needed to create a community). As an owner, you can access all available features. You'll be able to create communities and invite other members or guests for free. Fees and invoicing processes are still being finalised.

If you're a **local government, private sector or Government Business** Enterprise employee, you can only be invited to access a community as a **guest**. As a guest, you'll be able to take part in the commuity you have been invited to join. But you can't create communities or invite/remove members.

*If you're a contractor with an Australian Public Service email address you can register as a membe

4-step registration process

1) Confirm your email address

1. To start the process, open a **Chrome or Microsoft Edge browser** on a computer or laptop and type www.govteams.gov.au/register. In the top right hand corner click, register.
2. Enter your **work email address,** tick the box **I'm not a robot** and click **submit** – a confirmation email will be sent to you. If you don't receive the email, check your junk or spam folders.
3. In the confirmation email, click **confirm email address** OR **copy and paste the link** into the web browser

2) Set-up your account

1. **Read and accept the terms and conditions**.
   a) Make sure you read all the terms and conditions as they are important and you can't press next until you've **scrolled to the bottom**.
2. **Enter your details in the form**, click **review** and if the information is correct tick the box **I acknowledge the details are correct** and click **create account**
3. Copy and save your GovTEAMS username ending in @govteams.gov.au and then click **go**

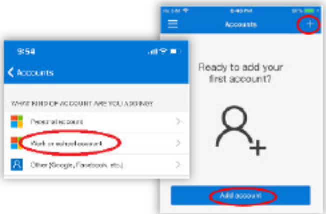
3) Log in

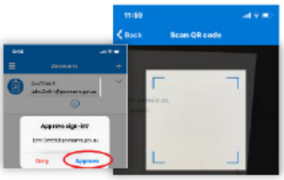
1. Choose an option:
   a) **Sign in –** first time creating an account
   b) **Multiple accounts** – you have multiple accounts
2. Sign in using your new username –firstname.surname@**govteams.gov.au** and enter the password you used to create your account
   Forgot password - Contact the Service Desk.
3. A **more information required** screen shows, click **next**
4. Click **next** to set-up the Microsoft Authenticator (you need your mobile) and then click **next**

4) Complete the Microsoft's multi-factor authentication process

To complete your multi-factor authentication process, you'll need a mobile/landine phone or the Microsoft Authenticator app on your device. You will be asked to download the Microsoft Authenticator app. If you don't want to download the app click **I want to use a different method**.

Mobile App


9:54
Accounts
WHAT KIND OF ACCOUNT ARE YOU ADDING?
Personal account
Work or school account
Other (Google, Facebook, etc.)
Accounts
Ready to add your first account?
Add account



1. Install the **Microsoft Authentication** app for Android or iOS from the app store
2. Open the app and click the **+ (plus) icon** and select **work or school account** (make sure you allow the app to send notifications and access your camera)
3. Use the app to **scan the QR code** on your laptop or computer screen (this will connect the app to your GovTEAMS account). Once you've scanned the QR code, click **next**
4. **Approve the notification** on your **phone** and click **next** on your **laptop or computer screen**
5. Select your area code from the drop down, enter your phone number and select **text me a code** or **call me** and then click **next**
6. **Enter the code sent to your phone,** click **next,** then **next** again and then click **done**
7. **A more information screen** will show, click **next**, then **done**. When the stay signed in screen shows shows, click **yes**

OR

Authentication Phone

To use this verification method, you must have access to a mobile phone that can receive messages. After step 4 – complete two-factor authentication complete the following:

1. **Select your country or region** e.g. Australia (+61) and enter your phone number.
2. Select the method:
   - **Send me a code by text message**
   - **Call me** - An automated service will call you and ask you to press the hash (#) key.
3. Click **next**
4. Enter the code supplied
5. Click **verify**
6. Click **done**

Verify your account

To make sure you can reset your password, Microsoft needs to get you to complete the multi-factor authentication process you just set up.

You will then be taken to the security info screen where you can set an additional authentication method. We recommend you do this in case you lose access to the phone you used to setup the preferred authentication method.

1. Click **add method**.
2. Select your preferred alternative option
3. Complete the required details and click **next**.
4. Using the alternative option you selected complete the verification.
5. Click **done**.

Get familiar with your dashboard

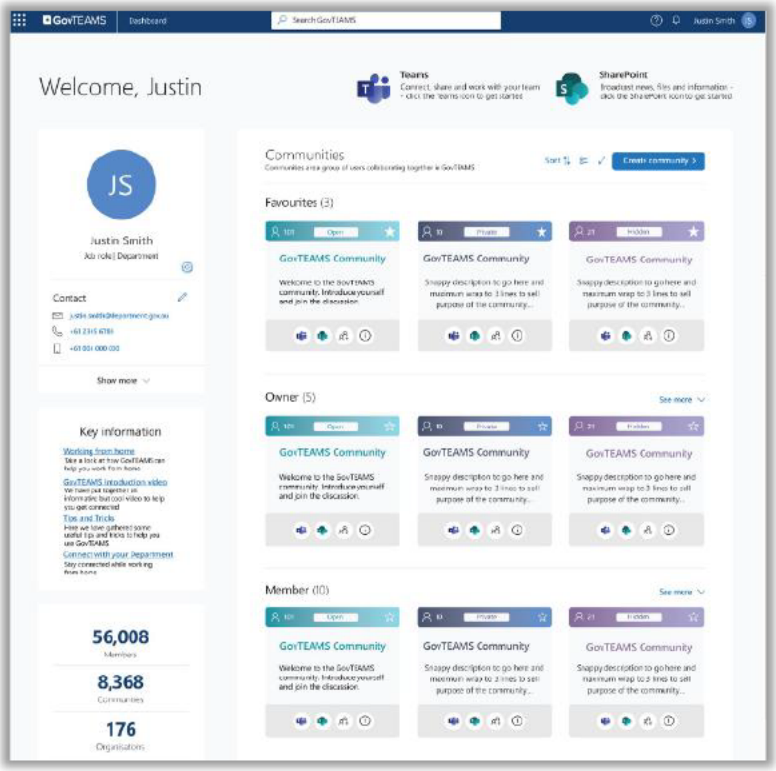
Your personalised dashboard lets you access tools, communities, members and files in one place!

From the dashboard, you can:

- Build your profile
- View and create your communities
- Discover communities, members and files
- Invite members
- Respond to requests to join a community you own
- Access the two main apps Microsot Teams and SharePoint at the top of the page
- Access other Office 365 apps by clicking on the waffle ▦ icon, top left hand corner of the page

Change your dashboard view

Set up your GovTEAMS dashboard for how you need it!



Welcome, Justin

Teams: Connect, share and work with your team – click the Teams icon to get started

SharePoint: Broadcast news, files and information – click the SharePoint icon to get started

Communities are a group of users collaborating together in GovTEAMS

Welcome to the GovTEAMS community. Introduce yourself and join the discussion.

Snappy description to go here and maximum wrap to 3 lines to sell purpose of the community...

Take a look at how GovTEAMS can help you work from home

We have put together an informative but cool video to help you get connected

Here we have gathered some useful tips and tricks to help you use GovTEAMS

Stay connected while working from home

Grid view

To view your dashboard as a grid, click on the **grid icon** next to the create community button.

List view

To view your dashboard as a list, click on the **list icon** next to the create community button

Expand view

To view your dashboard in expland view, click on the **expand icon** next to the create community button.

Sort options

Your dashboard is automatically set to be in alphabetical order A-Z. To change this setting, click on the **sort icon** it will change to Z-A.

Add you favourite communities

You can favourite communities on your dashboard:

- Click the **star icon** on a community card
- It will appears under the favourites heading at the top

Personalise profile

The more you put in, the more you'll get from GovTEAMS!

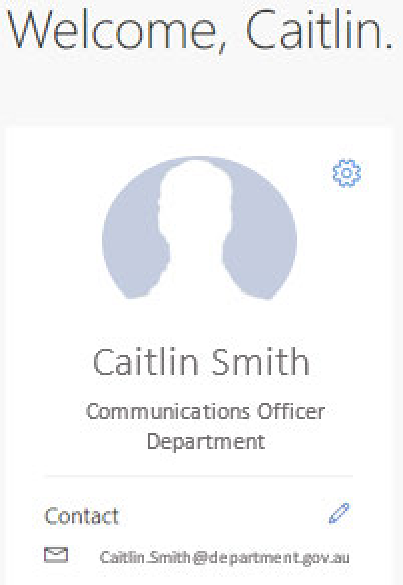
Account

Information that goes into your account is your:

- Name
- Organisation you work for
- Job title
- Level
- Email address

Update your account details from the dashboard:

1. Click on the pen icon ✎ next to contact
2. Make changes to the member details field
3. Click **save**
4. Change your email address if required
5. Click **update**



Welcome, Caitlin.

Caitlin Smith

Communications Officer

Department

Contact ✎

✉ Caitlin.Smith@department.gov.au

Profile (Delve)

Information that goes into your profile:

- About me – Tell your story to helps others get to know you
- Projects - List of projects you've worked on
- Skills and expertise
- Schools
- Interests and hobbies

Fill out your skills, expertise and interests

Think about how you want your profile to be seen by future employers. Do you want a professional and informative profile or do you want one that doesn't tell them anything about you? Remember the more you put in, the more you'll get from GovTEAMS.

To update your profile:

1. From the dashboard click update delve profile
2. Click **update profile** ✎ Update Delve profile
3. Complete the about me section textbox
4. Click **save**
5. Enter the name of a project you've worked on in the textbox under the project heading
6. Click **add project**
7. Repeat steps to add more projects and for other sections

Profile Photo

Make it easier for people to connect with you and put a face to a name!

To update your profile photo:

1. From the dashboard click **update Delve Profile**
2. Click on the camera button next to your existing profile photo
3. Click **upload a new photo**
4. Select the photo you wish to upload and **click open**
5. Use the plus and minus scale to adjust the photo
6. Click **set as profile photo**

Communities

Work how you want, with the people you need.

Create your own community

Start exploring GovTEAMS! Create your own open, private or hidden communities. **How do you create your community?**

1. Click **create community** on your dashboard
2. Read and accept the terms and conditions
3. Complete the community details form
4. You'll need to make sure you nominate a second owner of your community. Your second owner needs to already be a registered GovTEAMS member
5. You'll receive an email when your community is ready, this can take a few minutes

Get familiar with your community card

You can create different types of communities! Select a community type based on your needs. You can create the following community types:

- **Open** – your community is discoverable and any member can join
- **Private** – your community is discoverable but members will need to request to join. Don't forget, you'll need to approve these requests!
- **Hidden** – your community won't be discoverable and you'll need to invite people to join

You can invite members to any of the community types

Search and join communities

Try finding the GovTEAMS community!

1. From the dashboard, search for the GovTEAMS community in the search bar and click the arrow
2. In the search results, click **GovTEAMS community** (a side panel will show)
3. Click **join this community**
4. You'll receive an email letting you know you've been added to the community

Set-up community permissions

To set-up your community permissions:

1. From the dashboard, search for the GovTEAMS community in the search bar and click the arrow
2. In the search results, click **GovTEAMS community** (a side panel will show)
3. Click **join this community**

You'll receive an email letting you know you've been added to the community

Add a favourite

You can favourite communities to your dashboard:

1. Click the star icon ☆ on a community card and it will appear under the favourites heading at the top

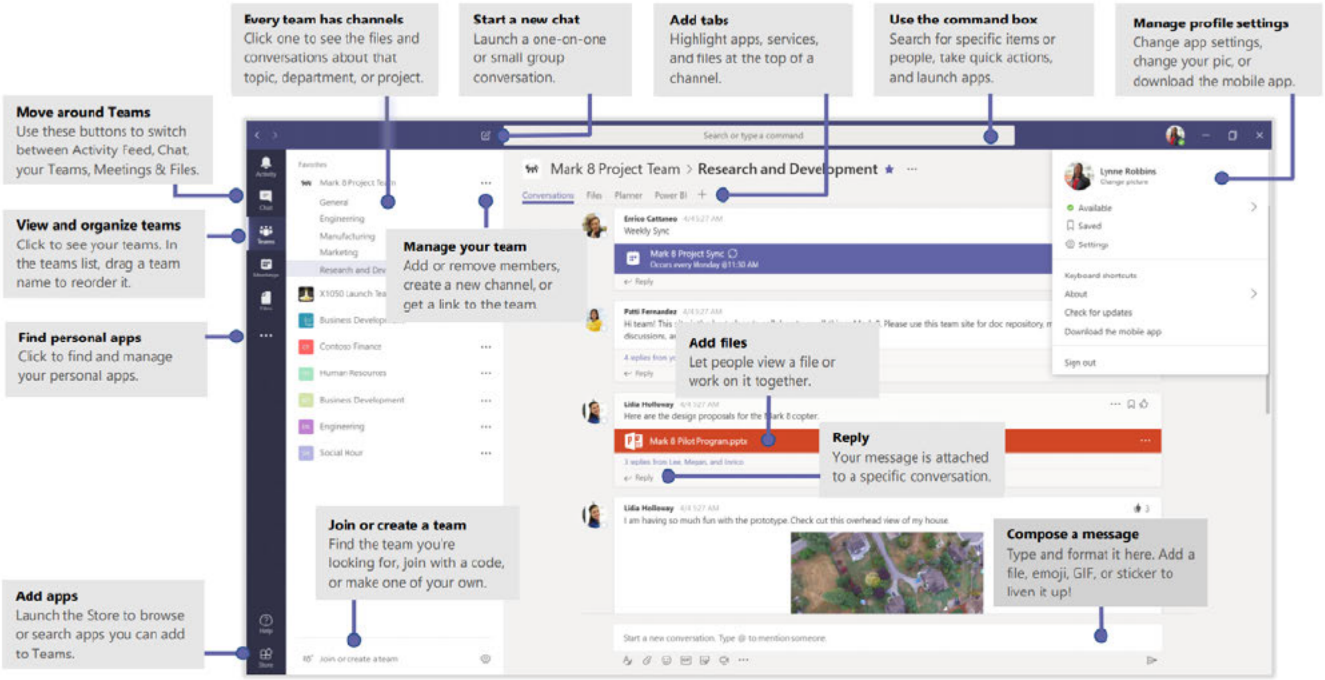
Add people to your community

Try adding a friend to your community!

1. From the dashboard, click on the people icon on your community card.
2. Enter the work email addresses of the people you want to invite and select from the drop down or select add bulk invites - you can only have one email address on each line. You can invite anyone to your community, even if they're not already registered. Click **send invite**

Interact with others

Chat, meet and co-author files in real-time with Microsoft Teams.



Every team has channels
Click one to see the files and conversations about that topic, department, or project.

Start a new chat
Launch a one-on-one or small group conversation.

Add tabs
Highlight apps, services, and files at the top of a channel.

Use the command box
Search for specific items or people, take quick actions, and launch apps.

Manage profile settings
Change app settings, change your pic, or download the mobile app.

Move around Teams
Use these buttons to switch between Activity Feed, Chat, your Teams, Meetings & Files.

View and organize teams
Click to see your teams. In the teams list, drag a team name to reorder it.

Find personal apps
Click to find and manage your personal apps.

Manage your team
Add or remove members, create a new channel, or get a link to the team.

Add files
Let people view a file or work on it together.

Reply
Your message is attached to a specific conversation.

Join or create a team
Find the team you're looking for, join with a code, or make one of your own.

Compose a message
Type and format it here. Add a file, emoji, GIF, or sticker to liven it up!

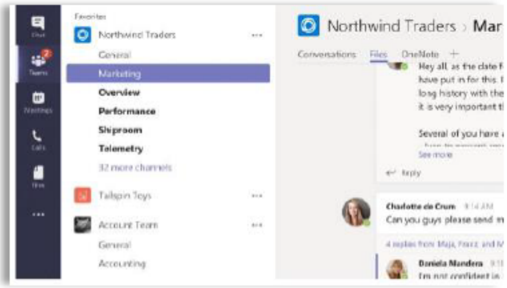
Add apps
Launch the Store to browse or search apps you can add to Teams.

Get familiar with Microsoft Teams:

To access Teams from your dashboard:

1. Click the waffle icon ▦ or click the Teams icon on your community card
2. Click **Teams**
3. Teams will launch in a new tab in your browser

Pick a community and channel



A community, in Teams, is a collection of people, conversations, files and tools—all in one place.

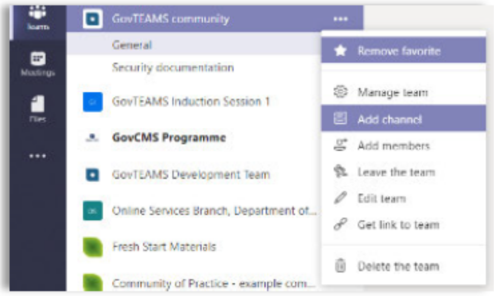
A channel is a discussion in a team, dedicated to a department, project or topic.

1. Open **Teams**
2. Select a community from the Teams tab on the left
3. Click a channel beneath the community name to explore the conversations, files and other tabs

Create a channel

You can create a channel in your community.

Having multiple channels can be useful to help you separate different types of work. On the left side of your screen is a list of communities you're a member of.



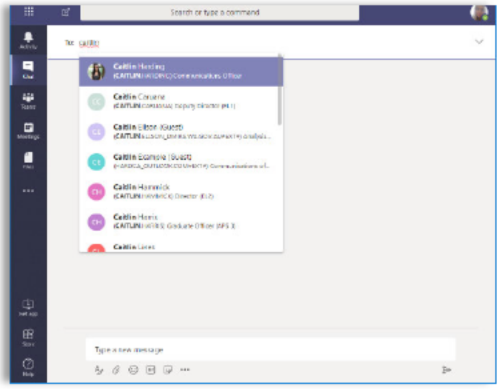
To create a channel you'll need to:

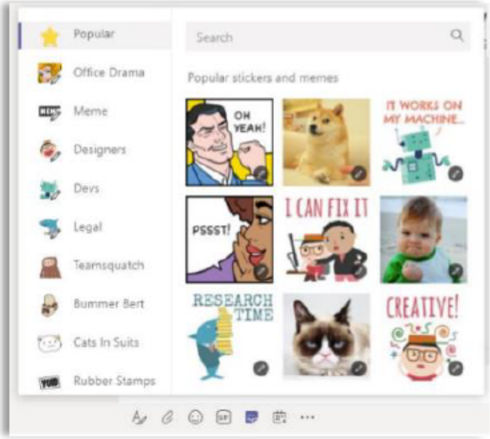
1. Click on the 3 dots next to the community name ···
2. Click **add channel**
3. Enter the channel name and description
4. Click **add**
5. The channel you created will now appear under the community name and is ready for you to use

Start a chat

You can start a chat with individuals and groups in Teams.

1. At the top left click the pen icon ✎ to start a new chat
2. Start typing the name of the person you want to chat with. This will show a list of suggested people
3. Click on the name of the person you're after
4. Start typing your message in the textbox at the bottom of the screen and click the send icon ▷
5. If you want to start a group conversation, repeat steps 3 and 4 before continuing with step 5.





Have fun with your messages!

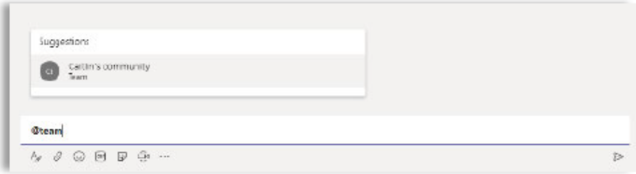
Teams lets you have a little fun with your messages. Try sending an emoji, GIF or sticker!

1. Click **sticker** under the textbox where you type your message
2. Pick a meme or sticker from one of the categories
3. You can also add an emoji or GIF using the buttons

@mention someone

To get someone's attention, type @, then their name (or pick them from the list that appears).

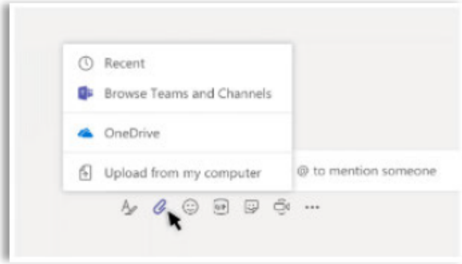
Type @team to message everyone in a team or @channel to notify everyone who favorited that channel.



Share a file

Work together in your new online workspace!

1. Click **attach** under the textbox
2. Select the file location and the file you want
3. Depending on the location of the file, you'll get options for uploading a copy, sharing a link, or other ways to share



Co-author files

Work together in real-time!

1. Find the file in the channel (or upload it)
2. Click on the file
3. Click **edit**
4. Start working in the document

You'll be able to see a coloured icon that indicates where your colleague is working so you don't duplicate effort!

Work with files

Check out all the files that are in communities!

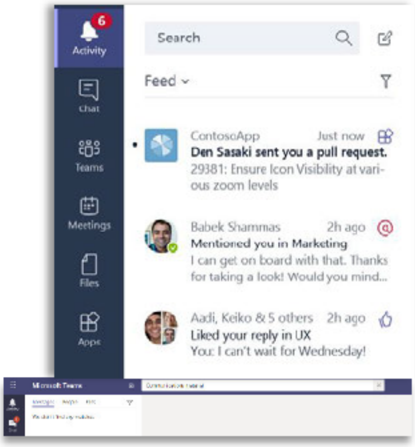
1. Click the files icon on the left to see all files shared across all of your communities or click **files** at the top of a channel to see all files shared in that channel
2. Click more options dots icon**...** next to a file to see what you can do with it. In a channel, you can instantly turn a file into a tab at the top!

See recent activity

Stay on top of things!

Click **activity** on the left. The Feed shows you all your notifications and everything that's happened lately in the channels you follow.

You can even apply filters Y to your activity feed!



ContosoApp Just now
Den Sasaki sent you a pull request.
29381: Ensure Icon Visibility at various zoom levels

Babek Shammas 2h ago
Mentioned you in Marketing
I can get on board with that. Thanks for taking a look! Would you mind...

Aadi, Keiko & 5 others 2h ago
Liked your reply in UX
You: I can't wait for Wednesday!

Search for messages, people and files

You can search for messages, people or files!

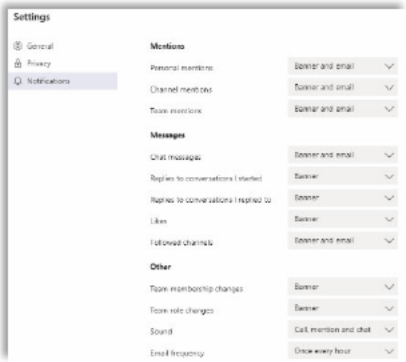
1. Start typing a name, keyword or phrase into the textbox at the top of your screen
2. Click the **messages, people** or **files** tab

Set up notifications

In Teams, you get to decide what notifications you receive!

To update your notification settings:

1. Click on your profile photo in the top right corner
2. Click **settings**
3. Click **notifications**
4. Change the settings to from the dropdown options



Mentions

Personal mentions: Banner and email
Channel mentions: Banner and email
Team mentions: Banner and email

Messages

Chat messages: Banner and email
Replies to conversations I started: Banner
Replies to conversations I replied to: Banner
Likes: Banner
Followed channels: Banner and email

Other

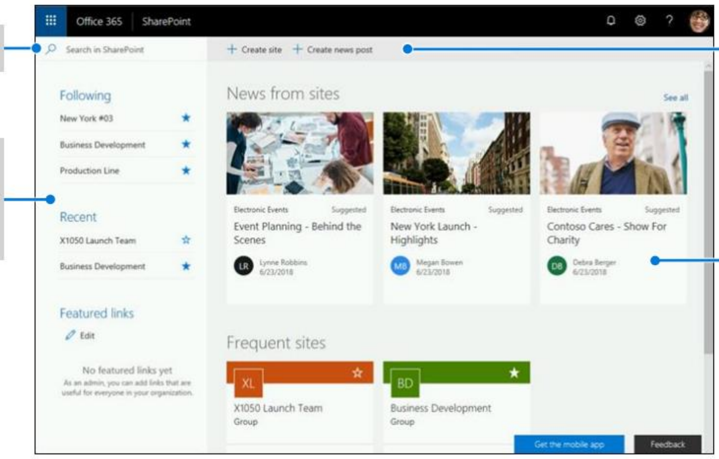
Team membership changes: Banner
Team role changes: Banner
Sound: Call, mention and chat
Email frequency: Once every hour

Whats next?

SharePoint

Create pages, document libraries and lists!

Structure, store and find information in a meaningful way that is easy to use, manage and find!



Search
Find **Sites**, **People**, or **Files**.

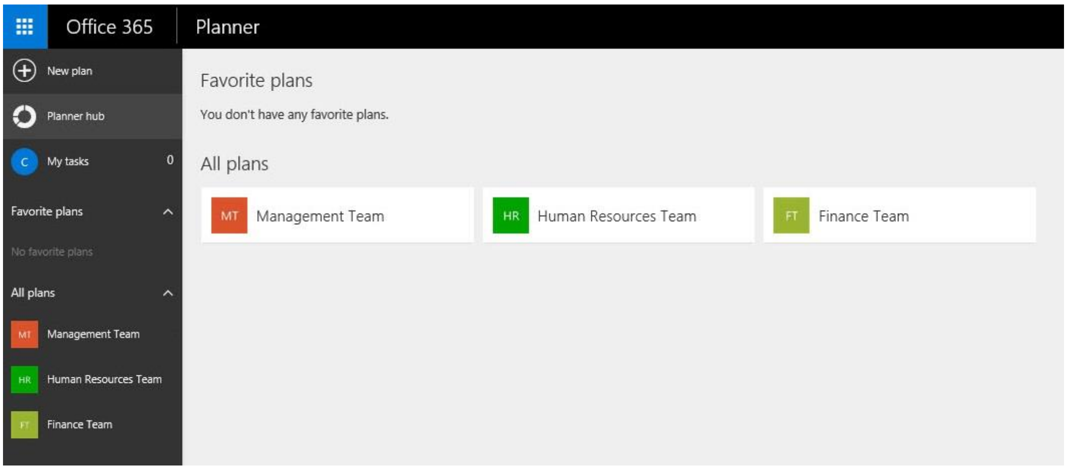
Find your sites
- **Following** displays sites you follow, like your team's site or a site from another group you work with.
- **Recent** shows any site you've gone to recently.
- **Featured links*** displays sites your company wants to showcase.

Create a site or news post

Check out featured content
- **News from sites** highlights updates from sites you follow or visit often.
- **Frequent sites** shows sites you like to go to and recent activity in them.
- **Suggested sites*** (not shown) appear based on searches you've done and recommendations from Microsoft Graph.
- Microsoft Graph must be enabled by your admin to see **Featured links** and **Suggested sites** on your SharePoint homepage.

Planner

Organise and track your team's tasks in one place!



Checklist

START AN ACCOUNT

☐ Register and login

DASHBOARD

☐ Get familiar with your dashboard

PERSONAL PROFILE

☐ Update your Personal Profile
☐ Add a profile photo

Communities

☐ Create your own community
☐ Get familiar with your community card
☐ Search and join communities
☐ Add a favourite
☐ Add people to your community

TEAMS

☐ Launch Teams
☐ Pick a community and channel
☐ Create a channel
☐ Start a chat
☐ @mention someone
☐ Share a file
☐ Co-author files
☐ Work with files
☐ See recent activity
☐ Search message, people and files
☐ Set up notifications

What's coming next

☐ Get familiar with SharePoint and Planner

We're here to help

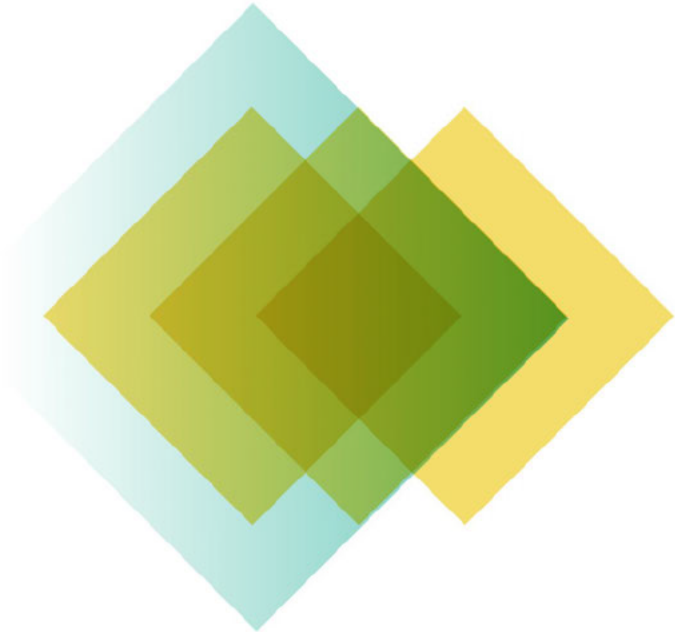
Visit our support site www.GovTEAMS.gov.au for more information.

Australian Government

Office of the Australian Information Commissioner

Information Management Policy

Document ID:	D2020/019571
Version:	1.0
Approved:	8th January 2021



January 2021

OAIC

Change history

Version	Name	Changes	Date
1.0		Original	July 2017
1.1		Word template updated	January 2019
1.2		Content update	July 2019
1.3		PSPF review	September 2020
1.4	William Dent, Agilient	Draft	21 September 2020
1.5	Ruth Mackay Assistant Commissioner, Corporate	Final	7 January 2021
2.0	Elizabeth Hampton Acting Australian Information Commissioner and Privacy Commissioner	Approved	8 January 2021

Contents

Purpose

The purpose of the Office of the Australian Information Commissioner (the OAIC) Information Management Policy (the policy) is to provide guidance and direction on the creation and management of information, and to clarify staff responsibilities. The OAIC is committed to establishing and maintaining recordkeeping practices that meet its business needs, accountability requirements and stakeholder expectations.

This policy forms part of the OAIC's Information Governance framework that includes the following elements: recordkeeping procedures for the electronic records management system (Content Manager), business rules and an Information Management Strategy to ensure the OAIC can effectively:

- Provide comprehensive evidence of decisions communications and activities
- Demonstrate that accountability requirements have been met
- Support business activities through the creation of useable and reliable records, contributing to business efficiency and effectiveness, and
- Minimise business risk by ensuring the right records are created to sustain business performance and continuity

Policy statement

The OAIC's records are its corporate memory, and are a vital asset for ongoing operations, providing valuable evidence of business decisions, activities and transactions.

The role of the OAIC is to promote and uphold privacy and information access rights. A number of Australian Government initiatives impact on the OAIC, including our strong influence in championing 'open government', promote better information management practices and provide advice and assistance to the public on their information access rights.

The OAIC is committed to implementing best recordkeeping practices and systems to ensure the creation, maintenance and protection of accurate and reliable records. All recordkeeping practices within the OAIC are to be in accordance with this policy and its supporting procedures.

The OAIC is committed to implementing the ICT provisions of the Protective Security Policy Framework (PSPF) to ensure the secure operation of the OAIC ICT systems to safeguard information and the continuous delivery of government business by applying the Australian Government Information Security Manual's cyber security principles during all stages of the lifecycle of each system.

Scope

This policy applies to all staff within the OAIC, including contractors, consultants, outsourced providers and other personnel who work on behalf of the OAIC.

This policy applies to all aspects of OAIC business, all records created during business transactions, and all business applications used to create records including email, database applications and websites.

This policy provides the overarching framework for any other corporate recordkeeping policies, practices or procedures.

Policy context

The OAIC's recordkeeping policies and practices are integrated with the broader information management regime including core business systems. The Information Management and Project Services (IMPS) team, in consultation with staff, providers and shared service arrangements within the OAIC, is responsible for the design, implementation and review of recordkeeping practices.

Responsibilities

The Information Commissioner is responsible for the authorisation of this Information Management policy, and the management of this policy within the OAIC is overseen by the Deputy Commissioner.

Executive are responsible for the implementation of this policy through resource allocation, and other management support.

The Director of Information Management and Project Services (IMPS), with the support of the Records Manager, is responsible for overseeing the design, implementation, and maintenance of this information management policy, as well as monitoring compliance of recordkeeping systems and conducting system audits. The Director of Information Management and Project Services together with the Records Manager is also responsible for the overarching management of the OAIC's recordkeeping systems, systems administration support, and education and awareness of staff to ensure recordkeeping practices within the OAIC, are consistent with the standards described in this policy.

Managers and team leaders are responsible for supporting and monitoring staff recordkeeping practices as defined by this policy.

All OAIC staff are responsible for the creation of accurate and reliable records as defined by this policy and staff are to ensure they are aware of their responsibilities for keeping and maintaining records.

Legislation and standards

The OAIC acknowledges the following legislation relate to records and information:

- *Archives Act 1983*
- *Electronic Transactions Act 2000*
- *Evidence Act 1995*
- *Freedom of Information Act 1982*
- *Privacy Act 1988*
- *Public Service Act 1999*
- *Information Management Standard – Australian Government*

The OAIC is committed to developing and maintaining recordkeeping systems that capture and maintain records with appropriate evidential characteristics in accordance with the requirements of these statutes and to developing its recordkeeping systems in accordance with Australian Standard for

Records Management (AS ISO 15489) and the National Archives of Australia Recordkeeping Metadata Standard for Commonwealth Agencies. For complete list of legislation see https://www.naa.gov.au/information-management/information-management-legislation

Whole of Australian government policies

The OAIC is committed to supporting whole of Australian-government policies to ensure information is managed and available for the relevant purpose it was intended. Such policies include

- Digital Continuity 2020 Policy
- Digital Continuity 2020 Statement
- Information Security Management Guidelines – Australian Government Security Classification System
- Australian Government information security management guidelines—Protectively marking and handling sensitive and security classified information and material
- *FOI Act 1982* reforms including the Information Publication Scheme and a focus on greater access to government information.

Recordkeeping systems

All records of lasting value are to be captured and maintained through the Content Manager and Resolve recordkeeping systems. Records that are security classified or sensitive should be maintained by the most appropriate system for that type of record.

The OAIC's recordkeeping systems are dedicated to the creation and maintenance of authentic, reliable and usable records for as long as they are required to effectively and efficiently support business functions and activities.

The recordkeeping systems will manage the following processes:

- the creation or capture of records within the recordkeeping system
- the digital storage of records
- the protection of record integrity and authenticity
- the security of records
- access to records
- the disposal of records – in accordance with approved disposal authorities

Corporate information must not be maintained in email folders, shared folders, personal drives or external storage media as these lack the necessary functionality to protect business information over time.

Managing classified material

The Australian Government Protective Security Policy Framework (PSPF) information security requirements consist of four core information security requirements that entities apply to achieve the information security outcome. The information security requirements apply to all information assets owned by the Australian Government, or those entrusted to the Australian Government by third parties, within Australia.

PSPF 8 supporting requirements are in Annex A and should be referred to for creating, storage, handling and disposal of classified and sensitive material.

These policies should be read in conjunction with the *Attorney-General's Department guidelines on identifying, marking and storing security classified material*.

Receiving security classified material

The OAIC uses a unclassified ICT network, which means that we are unable to receive, store, create or otherwise transmit security classified material in our recordkeeping systems.

When security classified material is received in the OAIC, the Information Systems Manager or Records Officer will register an electronic file in Content Manager and create a paper file for the classified document. Copies of the document are not to be stored in the OAIC's electronic systems. The paper file must be stored in the s47E(d) at the end of each business day, or otherwise when not in use.

s47E(d) the file movement must be recorded in the Notes section of corresponding Content Manager container. Similarly, if copies of classified material are made or destroyed, this must be recorded in the Notes section of the corresponding Content Manager container. For more information on how to register and track classified material, see our guide to handling classified material. D2017/007049

The OAIC also receives secure faxes via the Australian Government Solicitor's office. The procedures for transporting, managing, sending and receiving these faxes is outlined in the *OAIC Procedure for Transporting Classified Material*

Creating security classified material

If records are created that are security classified, for example a response to a Cabinet document, a computer and printer must be used that are not connected to the OAIC network and not Wi-Fi enabled. Classified material cannot be stored in Content Manager or Resolve.

s47E(d) must be used for preparing security classified material, which can then be transmitted via safe-hand delivery. Contact the Director, Information Management and Project Services for access to these facilities.

Copying, transporting, and destroying copies of security classified material

When it is necessary to create copies of security classified material, staff must ensure they stay within the vicinity of the photocopying machine until the copying is complete and remove the material immediately. Multi-function devices (MFDs) may retain images of copied documents. The Information

Management and Project Services team or ICT Security Services should be consulted in the first instance for advice on the sanitisation of these and similar devices.

Occasionally it may be necessary to transport security classified material outside the OAIC, for example if someone is travelling to a meeting off-site. Several methods can be used to transport the material, for instance, 'double enveloping', or the use of a single paper envelope in conjunction with a SCEC-endorsed briefcase, satchel, pouch or transit bag, or a 'single use' SCEC-endorsed envelope. Whatever the combination used, the inner barrier is to be tamper evident and the outer barrier is to obscure the nature of the information being transferred. Details of any transfer must be entered in the Notes section of the corresponding Content Manager container.

The procedures for transporting, managing, sending and receiving hard copy material is outlined in the *OAIC Procedure for Transporting Classified Material* .

These procedures also apply to ICT equipment and media such as CDs and DVDs that contain classified information without approved encryption. Contact the Information Management and Project Services team or ICT Security Services to establish the appropriate encryption to lower handling requirements.

Refer to the Attorney-General's guidelines on handling sensitive and security classified material for further information on preparing information for transportation.

If copies of security classified material have been made , they must be destroyed once there is no need for them. The OAIC has three B-Class shredders, which can be used to destroy documents and CDs that are classified up to and including PROTECTED. The Information Management and Project Services team can securely erase USB drives containing classified material up to and including the PROTECTED classification once they are no longer required. Documents classified as SECRET or TOP SECRET must be returned to the sender by safe hand delivery.

Access to information

The OAIC's records are a corporate resource, providing evidence of business activity and guidance for future decisions. For this reason, staff should have access to records unless there is a legitimate need to restrict access. The OAIC ensures access to sensitive and security classified information or resources is only provided to people with a need-to-know.

The OAIC ensures that people requiring ongoing access to security classified information or resources are security cleared to the appropriate level:

a. For ongoing access to PROTECTED information—Baseline security clearance or above
b. For ongoing access to SECRET information—Negative Vetting 1 security clearance or above
c. For ongoing access to TOP SECRET information—Negative Vetting 2 security clearance or above

Note: Some Australian office holders are not required to hold a security clearance.

In addition, entities must ensure that people requiring access to caveated information meet all clearance and suitability requirements imposed by the originator and caveat owner.

Examples of records that require restricted access include:

- Case management records, such as privacy complaints, FOI reviews and Assessments
- Staff personnel files
- Certain records managed by the OAIC Executive

Attachments A and B to this policy provide guidance on current security and access settings for our Resolve and Content Manager databases.

Please contact the Information Management and Project Services team if you have any questions about when to restrict access to a record, or if you are unable to access a record that you need.

Records titling

The OAIC Content Manager system allows for the creation of containers, sub containers and documents.

Containers are titled according to their records classification and a meaningful title.

Sub containers and documents are titled using a meaningful title.

(See Attachment C)

Records retention and destruction

Section 24(2) of the *Archives Act 1983* permits the destruction of a Commonwealth record in limited circumstances, such as when required by law, with the permission of National Archives or in accordance with normal administrative practice. The latter two situations will apply to the majority of OAIC records.

National Archives of Australia provides permission to destroy Commonwealth records by issuing records disposal authorities, which set out the requirements for keeping or destroying records. There are two types of records authority that the OAIC deals with – general and agency specific.

The Administrative Functions Disposal Authority (AFDA) sets out the requirements for general records and covers the retention and destruction of records relating to functions performed by most Australian Government agencies. For example, AFDA covers records relating to human resources, finance, procurement, and legal services.

Agency specific disposal authorities cover the specific business functions of the agency. The OAIC records disposal authority covers records relating to our core business functions:

- Awareness and education
- Compliance management
- Information policy review and development
- International relations
- Reviews and investigations

Each function in a records authority is split into record classes. A class provides a description of certain records that we may create in our day-to-day work, along with a retention period that tells us how long we need to keep those records for before we destroy them. As a general guide, the higher the importance of a document, the longer it will be retained. Some documents cannot be destroyed at all and must be transferred to the National Archives of Australia once no longer in use.

Normal administrative practice (NAP) allows the OAIC to destroy records that have no ongoing business value, such as administrative emails.

Staff should contact the Information Management and Project Services team when there is a requirement to delete or destroy records in order that this is carried out in accordance with the Normal Administrative Practice.

Staff may destroy records themselves under NAP, however the destruction of any other records must be done in consultation with the Records Manager.

The Normal Administrative Practice procedure contains more information about the NAP process.

Disposal of physical records

Unclassified material may be disposed of by shredding, or by using a secure blue bin (paper records only).

The OAIC has three B-Class shredders. s47E(d) s47E(d) s47E(d) [redacted] hese shredders are SCEC-endorsed and can be used to shred records up to and including the PROTECTED security classification. The three shredders can also shred CDs containing records up to and including PROTECTED.

Transfer of information

In certain circumstances, there may be a need to transfer records to other entities.

Records that have archival value and are no longer actively being used should be transferred to the National Archives of Australia. The records can still be accessed if necessary by contacting National Archives.

Another situation where there may be a need to transfer records is following machinery of government changes. As a rule, when the functions of one agency are transferred to another, the records relating to those functions are also transferred. In other words, the records follow the function. However, if the function is ceasing altogether (for example if an agency is being abolished), the records should be transferred to the portfolio agency.

System audits

The OAIC Information Management and Project Services team will conduct audits of the Resolve and Content Manager systems every 6 months, or as otherwise requested by the Executive, to ensure that access controls are working as intended and are up to date.

Communication and training

This policy will be communicated to staff through the Intranet and regular staff reminders via email from the Information Management and Project Services team. New staff will be provided with training on information management practices at the OAIC through the Induction program.

Monitor and review

This policy will be reviewed every 12 months by the Information Management and Project Services team.

s47E(d)

[redacted]

s47E(d)

[redacted]

s47E(d)

[redacted]

Attachment B: Content Manager access controls

Access to Content Manager records should be unrestricted, unless there is a business need to limit access.

Because Content Manager security groups are applied to individual containers or records, the need for access controls should be considered on a case by case basis. The table below will provide some guidance on the types of Content Manager records that require access controls.

Note that if you are restricting access to a record, you must give the Executive security group full access by adding the 'Executive' security group to the record. These controls are reviewable based on any advice received from the National Archives of Australia, and any subsequent system maturity undertaken to ensure classifications enable governance and management of information based on protective security classification and permissions.

Record type or subject matter	Can be accessed by
Personnel Files	Staff member and their direct reporting line
Assessment/Audit records	Assessment Team
Privacy case records	Privacy Case Management
FOI case records	FOI Case management
Financial records	Executive
Legal records	Legal Services Executive Other staff as requested by our Chief Privacy Officer or a member of the Executive
Records that may be considered sensitive	Limit to staff on a need to know basis, and Executive

Content Manager access can be full or partial – for example, editing a record may be limited to a particular security group, but all staff may be able to view the record. Please bear this in mind when applying access controls to records, as we should not be restricting access to records unnecessarily.

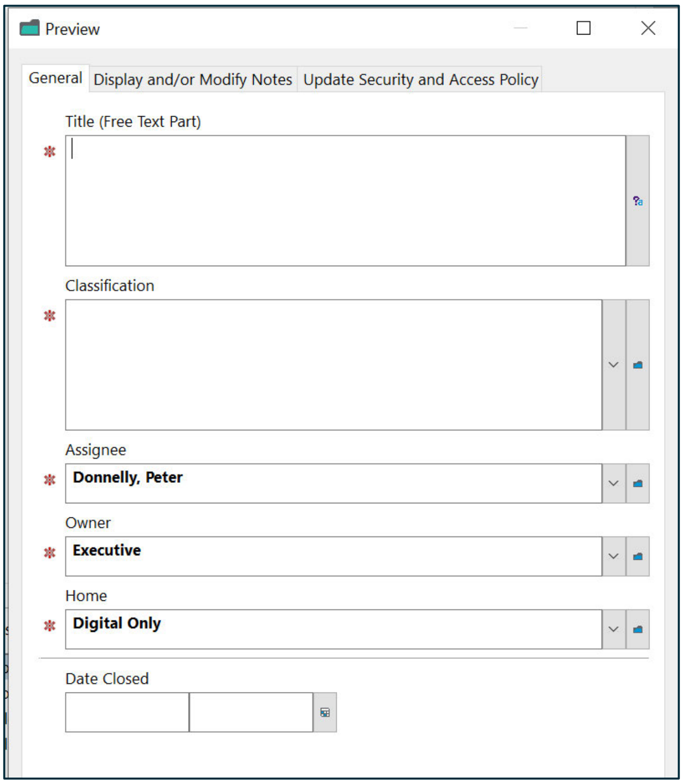
Attachment C: Content Manager titling conventions

File (Container) titling

Files in Content Manager are called Containers. There are three Container types in use. The Container Record Type is used to contain electronic documents and Sub Containers.

It is preferred that the Information Services Manager team create these Containers to ensure consistency and accuracy of Classification. To have a container created advise by email:

- Proposed Classification (If it is known what it might be. Hint - look at the classification of similar records)
- Proposed Title. This must be meaningful
- Brief description of what the file will contain
- Assignee – who will be the person assigned the record
- Owner - what group is the owner of the record
- Security Level. The options available in Content Manager for this record type are:
  - Official (default and most common)
  - Protected (This should only be applied where **Damage** to the national interest, organisations or individuals would result if the file and its contents were to be released)
- Security Markings:
  - TOP SECRET
  - SECRET
  - PROTECTED
  - CABINET
  - OFFICIAL: Sensitive
  - OFFICIAL
  - UNOFFICIAL
    - NOTE: Caveats can only be applied to security classified information, ie PROTECTED or above
    - NOTE: Apply classification or OFFICIAL: Sensitive and optional information management markers:
      - Legislative secrecy
      - Personal privacy
      - Legal privilege
    - NOTE: Security Caveats in Content Manager correspond to the Dissemination Limiting Markers documented in the Protective Security Policy Framework
    - NOTE: Only those staff with the caveat associated with their Content Manager profile you will be able to access the record.
- Any access restrictions on who may
  - View Document (the default position is that everyone can View the document)
  - View Metadata (the default position is that everyone can View the metadata)
  - Update Document (restrictions may apply)
  - Update Records Metadata (restrictions may apply)
  - Modify Record Access (restricted to Administrators)
  - Destroy Record (restricted to Administrators)
  - Contribute Content (restrictions may apply)



Preview
General
Display and/or Modify Notes
Update Security and Access Policy

Title (Free Text Part)

Classification

Assignee: Donnelly, Peter

Owner: Executive

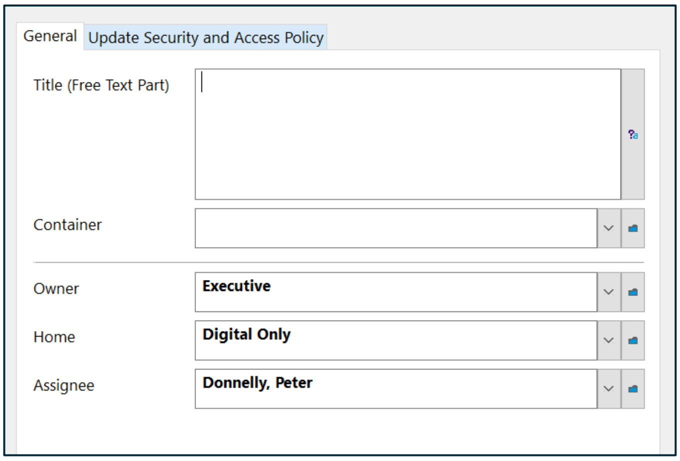
Home: Digital Only

Date Closed

Subfile (🗀 Sub container) titling

The Sub Container Record Type is used to contain electronic documents. Users may create sub containers.

- Title - use the same rules as apply for Document Titling
- Container – this is the number of the Container to which the Sub Container belongs
- Assignee – who will be the person assigned the record
- Owner - what group is the owner of the record
- Home – this will always be digital only



Title (Free Text Part)

Container

Owner: Executive

Home: Digital Only

Assignee: Donnelly, Peter

Security Classified file

This Record Type is used for registration of hard copy files which contain security classified material. These records are created by the Information Management and Project Services team.

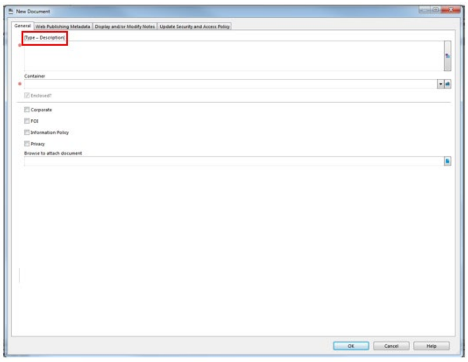
Document

1. One of the most important functions of any information management system is to ensure that the records it contains can be searched for and found for business purposes. A title that provides a concise statement of the content of the record will ensure that the right record will be found efficiently, and its content and context understood.

   If the title does not reflect the content of the container, or the individual document, it will be difficult for users to find the information they need. Effective titles distinguish one record from all others.

2. Free text is used to create a document title specific to the business unit/team. It identifies the subject of the document and ensures that a completed document title is unique and differentiates a document from all other documents in Content Manager.

   When creating a document in Content Manager a document title is entered into the (Type - description) in the registration dialogue box.



New Document
General
Web Publishing Metadata
Display and/or Modify Notes
Update Security and Access Policy
OK
Cancel
Help

(Type – Description)

Container

☑ Enclosed?

□ Corporate

□ FOI

□ Information Policy

□ Privacy

Browse to attach document

When recording the document free text title:

- keep titles as short as possible. There is a 255-character limit on the title length (including the File Title) so if possible, keep the length to less than 100 characters. Long files/document titles can result in Windows conflicts and inability to save or check out
- ensure the title comprehensively but concisely describes the document contents
- be consistent: title documents on similar business consistently, it makes them easier to find. Use agreed terms in situations where there can be variations, for example use 'personnel' – not 'staff' or 'employees'
- avoid using jargon, initials, abbreviations, and acronyms that are not commonly understood
- where acronyms are used in file names the acronym should appear in capitals. Only use accepted acronyms
- avoid words like 'the' or 'and'
- avoid using punctuation
- avoid redundancy (e.g. black darkness, burning fire) and unnecessary repetition
- avoid using underscores in titles as they increase the title length
- the title text should include
  - the name of the author of the correspondence - recorded as 'From Last Name First Name (e.g. Donnelly Peter)'. Where the author is from an organisation put the name of the organisation after the name.
  - the document subject matter
  - at the end of the title enter the creation date or the authorisation date in the form of YYYYMMDD, e.g. 20170119. Note: Content Manager captures the registration date
- an example of a title incorporating the above criteria is: “Letter from Donnelly Peter OAIC to Elizabeth Hampton - Correspondence titling convention at OAIC 20190228
- do not use vague titles such as email, briefing note, letter, etc. without further information

Appendix D: PSPF 8 supporting requirements

<table>
<tr><td><b>Requirement 1. Identifying information holdings</b></td><td>The originator <b>must</b> determine whether information being generated is official information (intended for use as an official record) and whether that information is sensitive or security classified.</td></tr>
<tr><td><b>Requirement 2. Assessing sensitive and security classified information</b></td><td>To decide which security classification to apply, the originator <b>must</b>:
i. assess the value, importance or sensitivity of official information by considering the potential damage to government, the national interest, organisations or individuals, that would arise if the information's confidentiality was compromised (refer to the following table), and
ii. set the security classification at the lowest reasonable level.
The originator must assess the information as OFFICIAL: Sensitive if:
i. a security classification does not apply, and
ii. compromise of the information's confidentiality may result in limited damage to an individual, organisation or government generally.
<table>
<tr><th>Protective marking</th><th>Business impact level</th><th>Compromise of information confidentiality would be expected to cause:</th></tr>
<tr><td><b>UNOFFICIAL</b></td><td>No business impact</td><td>No damage.
This information does not form part of official duty.</td></tr>
<tr><td><b>OFFICIAL</b></td><td>1 Low business impact</td><td>No or insignificant damage.
This is the majority of routine information.</td></tr>
<tr><td><b>OFFICIAL: Sensitive</b></td><td>2 Low to medium business impact</td><td>Limited damage to an individual, organisation or government generally if compromised.</td></tr>
<tr><td><b>PROTECTED</b></td><td>3 High business impact</td><td><b>Damage</b> to the national interest, organisations or individuals.</td></tr>
<tr><td><b>SECRET</b></td><td>4 Extreme business impact</td><td><b>Serious damage</b> to the national interest, organisations or individuals.</td></tr>
<tr><td><b>TOP SECRET</b></td><td>5 Catastrophic business impact</td><td><b>Exceptionally grave damage</b> to the national interest, organisations or individuals.</td></tr>
</table></td></tr>
<tr><td><b>Requirement 3. Declassification</b></td><td>The originator <b>must</b> remain responsible for controlling the sanitisation, reclassification or declassification of the information. An</td></tr>
</table>

	entity **must not** remove or change information's classification without the originator's approval.
Requirement 4. Marking information	The originator **must** clearly identify sensitive and security classified information, including emails, using applicable protective markings by: a. using text-based protective markings to mark sensitive and security classified information (and associated metadata), unless impractical for operational reasons b. if text-based protective markings cannot be used, using colour-based protective markings, or c. if text or colour-based protective markings cannot be used (eg verbal information), applying the entity's marking scheme for such scenarios. Entities **must** document a marking scheme for this purpose and train personnel appropriately.
Requirement 5. Using metadata to mark information	Entities **must** apply the Australian Government Recordkeeping Metadata Standard to protectively mark information on systems that store, process or communicate sensitive or security classified information: a. for security classified information, apply the 'Security Classification' property (and where relevant, the 'Security Caveat' property) b. for OFFICIAL: Sensitive information, apply the 'Dissemination Limiting Marker' property c. where an entity wishes to categorise information content by the type of restrictions on access, apply the 'Rights' property.
Requirement 6. Caveats and accountable material	Caveats **must** be marked as text and (with the exception of the NATIONAL CABINET caveat) only appear in conjunction with a security classification. The NATIONAL CABINET caveat can appear in conjunction with either the OFFICIAL: Sensitive marking or a security classification. Entities **must** ensure that accountable material: i. has page and reference numbering ii. is handled in accordance with any special handling requirements imposed by the originator and caveat owner, and iii. has an auditable record of all incoming and outgoing material, transfer, copy or movements. For all caveated information, entities **must** apply the protections and handling requirements established by caveat owners in the Australian Government Security Caveats Guidelines.
Requirement 7. Storage	Entities **must** ensure sensitive and security classified information is stored securely in an appropriate security container for the approved

	zone in accordance with the minimum protection requirements set out in **Annexes A to D**.
Requirement 8. Transfer	Entities **must** ensure sensitive and security classified information is transferred and transmitted by means that deter and detect compromise and that meet the minimum protection requirements set out in **Annexes A to D**.
Requirement 9. Disposal	Entities **must** ensure sensitive and security classified information is disposed of securely in accordance with the minimum protection requirements set out in **Annexes A to D**. This includes ensuring sensitive and classified information is appropriately destroyed when it has passed minimum retention requirements or reaches authorised destruction dates.

COOKE,Molly

Subject: GovTEAMS Official [SEC=OFFICIAL]
Attachments: OAIC GovTEAMS OFFICIAL - OAIC User Registration form - TEMPLATE.DOCX; GovTEAMS Getting Started Guide.PDF

Hi xxx

In order that we can set up an OAIC GovTEAMS OFFICIAL Community for you to share files with external organisations could you please complete the attached form, obtain your Asst Commissioner's approval and forward both to Brenton (copying me in) for his review & approval?

Once approved I will set up the Community. Note that both Brenton Attard & myself are always included in the User list as 'Owners'.

OAIC Users will be required to set up a GovTEAMS OFFICIAL account. A Getting Started Guide is attached.

Once the Community has been set up please advise the names & email addresses of external guest users who should be invited to join the Community & share information.

Note that material classified PROTECTED and above must not be store in GovTEAMS OFFICIAL.

For further background information see https://www.govteams.gov.au/. Happy to provide further information and a demonstration if required.

Let me know if you have any questions.

Regards
Catherine

Info cards

Assessing sensitive and security classified information

When you create official information (which is the majority of our information) you must determine whether it is **sensitive or security classified**.

If it is sensitive or classified information you will need to apply protective security markings and may need to store it outside our records management system.

You determine the nature of information by assessing the impact the release of the information would have if it was compromised.

protective security website
You will find more information about assessing information, including a table that assists you to assess damage to the national interest, government, organisations or individuals on the protective security website.

Refer to the detailed information in PSPF Policy 8: Sensitive and Classified information [PDF]

Tags: Security | Information management

Published 13 August 2021

View all info cards

Australian Government

Department of Home Affairs

Protective Security Policy Framework

8 Classification system

Table of Contents

A. Purpose

1. This policy details how Australian Government entities (entities) correctly assess the security classification of their information and adopt marking, handling, storage and disposal arrangements that guard against information compromise. This policy covers mobile devices that are authorised to process, store and communicate Australian Government information and data.

2. Information is a valuable resource. Protecting the confidentiality, integrity and availability of information is critical to business operations.

v2018.8

a. **Confidentiality** of information refers to the limiting of access to information to authorised persons for approved purposes.

b. **Integrity** of information refers to the assurance that information has been created, amended or deleted only by the intended authorised means and is correct and valid.

c. **Availability** of information refers to allowing authorised persons to access information for authorised purposes at the time they need to do so.

3. A security classification (OFFICIAL: Sensitive, PROTECTED, SECRET and TOP SECRET) is only applied to information (or assets that hold information, such as laptops, USBs) if it requires protection because the impact of compromise of the information or asset would be low to medium or above.

4. The requirements in this policy do not displace obligations imposed on entities through other policies, legislation or regulations, or by any other means.

B. Requirements

B.1 Core requirement

Each entity must:

i. identify information holdings

ii. assess the security classification of information holdings, and

iii. implement operational controls for these information holdings proportional to their value, importance and sensitivity.

B.2 Supporting requirements

Supporting requirements help Australian Government entities to maintain the confidentiality, integrity and availability of official information—including where the entity is the originator of information (the entity that initially generated or received the information).

Supporting requirements

#	Supporting requirements
Requirement 1. Identifying information holdings	The originator **must** determine whether information being generated is official information (intended for use as an official record) and whether that information is security classified.
Requirement 2. Assessing security classified information	a. To decide which security classification to apply, the originator **must**: i. assess the value, importance or sensitivity of official information by considering the potential damage to government, the national interest, organisations or individuals, that would arise if the information's confidentiality was compromised (refer to the following table), and ii. set the security classification at the lowest reasonable level.

			Security classified information			
	UNOFFICIAL	**OFFICIAL**	**OFFICIAL: Sensitive**	**PROTECTED**	**SECRET**	**TOP SECRET**
	No business impact	1 Low business impact	2 Low to medium business impact	3 High business impact	4 Extreme business impact	5 Catastrophic business impact
Compromise of information confidentiality would be expected to cause ➔	**No damage.** This information does not form part of official duty.	**No or insignificant damage.** This is the majority of routine information.	**Limited damage** to an individual, organisation or government generally if compromised.	**Damage** to the national interest, organisations or individuals.	**Serious damage** to the national interest, organisations or individuals.	**Exceptionally grave damage** to the national interest, organisations or individuals.

Requirement 3. Declassification	The originator **must** remain responsible for controlling the sanitisation, reclassification or declassification of the information. An entity **must not** remove or change information's classification without the originator's approval.
Requirement 4. Marking information	The originator **must** clearly identify security classified information, including emails, using applicable protective markings by: a. using text-based protective markings to mark security classified information (and associated metadata), unless impractical for operational reasons b. if text-based protective markings cannot be used, using colour-based protective markings, or c. if text or colour-based protective markings cannot be used (eg verbal information), applying the entity's marking scheme for such scenarios. Entities **must** document a marking scheme for this purpose and train personnel appropriately.
Requirement 5. Using metadata to mark information	Entities **must** apply the Australian Government Recordkeeping Metadata Standard to protectively mark information on systems that store, process or communicate security classified information: a. for security classified information, apply the 'Security Classification' property (and where relevant, the 'Security Caveat' property) b. where an entity wishes to categorise information content by the type of restrictions on access, apply the 'Rights' property.
Requirement 6. Caveats and accountable material	a. Caveats **must** be marked as text and (with the exception of the NATIONAL CABINET caveat) only appear in conjunction with a security classification of PROTECTD or higher. The NATIONAL CABINET caveat can appear in conjunction with a security classification of OFFICIAL: Sensitive marking or higher. b. Entities **must** ensure that accountable material: i. has page and reference numbering ii. is handled in accordance with any special handling requirements imposed by the originator and caveat owner, and iii. has an auditable record of all incoming and outgoing material, transfer, copy or movements. c. For all caveated information, entities **must** apply the protections and handling requirements established by caveat owners in the Australian Government Security Caveats Guidelines.
Requirement 7. Minimum protections and handling requirements	a. Entities **must** ensure OFFICIAL and security classified information is used, stored, carried and travelled with securely in accordance with the minimum protection requirements set out in **Annexes A to C**. b. Entities **must** ensure information is transferred and transmitted by means that deter and detect compromise and that meet the minimum protection requirements set out in Annexes A-C.
Requirement 8. Disposal	Entities **must** ensure OFFICIAL and security classified information is disposed of securely in accordance with the minimum protection requirements set out in **Annexes A to C**. This includes ensuring security classified information is appropriately destroyed when it has passed minimum retention requirements or reaches authorised destruction dates.
Requirement 9. Security classified discussions	Entities **must** ensure security classified discussions are only held in approved locations as set out in **Annex D**.

C. Guidance

C.1 Official information

5. Official information is all information created, sent or received as part of the work of the Australian Government. This information is an official record and it provides evidence of what an entity has done and why.

6. Official information can be collected, used, stored and transmitted in many forms including electronic, physical and verbal (eg discussions and presentations). See **Annex D** for sensitive security classified discussions.

7. The National Archives of Australia Australian Government Information Management Standard notes that information is a valuable asset. It contributes to good government through supporting efficient business, informing decision-making, demonstrating government accountability and transparency, mitigating risks, adding economic value and protecting rights and entitlements.

8. It is a core requirement of this policy that entities implement operational controls to protect information holdings in proportion to their value, importance and sensitivity. Although this policy is focused on security classified information, all official information requires an appropriate degree of protection as information (and assets holding information) are subject to both intentional and accidental threats. In addition, related processes, systems, networks and people have inherent vulnerabilities. A deliberate or accidental threat that compromises information security could have an adverse impact on government business.

9. The Department of Home Affairs recommends entities apply the minimum protections outlined in **Annexes A-C** for OFFICIAL information that is not assessed as being sensitive or security classified information.

10. Information compromise includes, but is not limited to:

    a. loss

    b. misuse

    c. interference

    d. unauthorised access

    e. unauthorised modification

    f. unauthorised disclosure.

C.1.1 Official information designated for public release

11. Information assessed as OFFICIAL may be authorised for public release, access or circulation (for example, entity publications or website content) by the originator, within the limits of authority conferred on them by the entity. If designated for public release, then either:

a. omit the optional OFFICIAL protective marking from the information, or

b. mark the information to reflect that it is intended and suitable for public release or publication, either with or without the non-mandatory OFFICIAL protective marking.

12. While not mandatory, entities may elect to adopt the AGRkMS ‘Rights Type Scheme’ term, ‘Authorised Public Access’. This term can be applied with or without the non-mandatory OFFICIAL protective marking.

13. Information intended for public release or publication could have sensitivity requirements or restrictions before release—for example, Budget papers. In this case, the point at which the information will be publicly available is recommended to be marked.

14. All personal information held—even if it is publicly available—is to be handled in accordance with the Australian Privacy Principles (APPs) in the *Privacy Act 1998*.

C.2 Official and security classified information

15. **Requirement 1** mandates that the originator (the entity that initially generated the information, or received the information from outside the Australian Government) determine whether official information is security classified information.

16. The Australian Government uses four security classifications: OFFICIAL: Sensitive, PROTECTED, SECRET and TOP SECRET. The relevant security classification is based on the likely damage resulting from compromise of the information’s confidentiality.

17. All other information from business operations and services requires a routine level of protection and is treated as OFFICIAL. Information that does not form part of official duty is treated as UNOFFICIAL.

18. OFFICIAL and UNOFFICIAL are not security classifications and are not mandatory markings.

19. The below guidance also relates to assessing whether an asset (eg a laptop) holds security classified information, and as such is treated as a classified asset.

C.2.1 The originator of information

20. The originator is the entity that initially generated the information, or first received the unmarked information (ie an Australian Government or third-party approved security classification has not been applied) from outside the Australian Government, and assessed the value, importance or sensitivity of the information by considering the potential damage that would arise if the information's confidentiality was compromised, and assigned the corresponding protective marking or classification.

21. **Requirement 3** mandates that the originator remains responsible for controlling the information. The originator is usually the person that created or first assessed the information. However, to ensure continuity, the entity may set the originator as the person, role, delegation or section within the entity that is best placed to be responsible for controlling the information.

22. If the entity, or functions of the entity, are abolished or merged, for example as part of a Machinery of Government change, then the entity assuming the former entity's responsibilities, is now considered the originator.

Case study: Originator impacted by Machinery of Government change

An officer working in Entity X is the originator of a PROTECTED document. The section in which the officer works is scheduled to transfer to Entity Y on 22 December 2022, however the officer has transferred to another role in the entity, and will therefore not be transferring to Entity Y. In this case, the section in Entity Y that is assuming the responsibility for the incoming functions from Entity X, becomes the originator for the PROTECTED document in question. A senior officer in Entity Y assigns responsibility for the document (or multiple incoming documents) either to a person, role or section within Entity Y to be the originator of the information from the date of transfer. Entity X documents the transfer to Entity Y, and Entity Y documents the decision to reassign the responsibility.

C.2.2 Proper use of security classifications

23. It is important that the management of information enables agencies to meet business, government and community needs and expectations—this involves balancing the need to protect information with the need to ensure appropriate access. Appropriately limiting the quantity, scope or timeframe of security classified information:

    a. promotes an open and transparent democratic government

    b. provides for accountability in government policies and practices that may be subject to inappropriate or over-classification

    c. allows external oversight of government operations and programs

    d. promotes efficiency and economy in managing information across government.

24. Over-classification of information can result in:

    a. access to official information being unnecessarily limited or delayed

    b. onerous administration and procedural overheads that add to costs

    c. classifications being devalued or ignored by personnel and receiving parties.

25. It is not consistent with this policy to apply a security classification to information in order to:

    a. restrain competition

    b. hide violations of law, inefficiency, or administrative error to prevent embarrassment to an individual, organisation or entity

    c. prevent or delay the release of information that does not need protection.

C.2.3 Who assesses information security classification

26. The person responsible for generating or preparing information on behalf of an entity (or for actioning information produced outside the Australian Government) assesses whether the information is sensitive or needs to be security classified.

27. Only the originator can change the security classification applied to its information. If the application of a classification is considered inappropriate, the original classification decision can be queried with the originator.

C.2.4 When to assess information security classification

28. Assessing the security classification of information when it is first created, or received from outside the Australian Government, helps protect the information. Significant changes, for example a Machinery of Government change, also present an opportunity to re-assess the security classification of information. The originator can also set a specific date or event for automatic declassification (for guidance on declassification, refer to C.2.6 Sanitising, reclassifying or declassifying information).

C.2.5 How to assess information security classification

29. **Requirement 2** mandates that the originator assess the security classification of information by considering the potential impact on the national interest, government, organisations or individuals that could arise from compromise of the information's confidentiality.

30. The more valuable, important or sensitive the official information, the greater the impact on government business that would result from its compromise. By assessing the 'Business Impact Level' if confidentiality of the information is compromised, the originator can determine whether information requires a security classification or requires a routine level of protection.

31. The Business Impact Levels tool (see **Table 1**) provides examples of potential damage from compromise of information's confidentiality. The tool assists in the consistent classification of information and the assessment of impacts on government business. Entities may develop their own sub-impact categories.

32. The potential damage from compromise of information's confidentiality determines the classification of that information. A simple flow diagram is provided at **Figure 1** to help assess whether information is security classified, based on the potential damage from compromise of the information's confidentiality.

33. The Business Impact Levels tool can also be used for secondary assessments of the potential damage from compromise of the availability or integrity of information. While assessing the Business Impact Level of compromise of the information's availability or integrity does not affect whether the information is security classified information, it may indicate that additional security measures (such as ICT, personnel or physical controls) could be warranted.

Guidance on minimum protections for handling information that is assessed and determined to be security classified is provided at C.5 Minimum protections for security classified information

Examples of OFFICIAL: Sensitive information

Examples of OFFICIAL: Sensitive information may include:

- official information governed by legislation that restricts or prohibits its disclosure, imposes certain use and handling requirements, or restricts dissemination (such as information subject to legal professional privilege or some types of 'personal information', including 'sensitive information' under section 6 of the *Privacy Act* that may cause limited harm to an individual if disclosed or compromised). Where compromise of personal information, including sensitive information (under the Privacy Act) would lead to damage, serious damage or exceptionally grave damage, this information warrants classification. Government-held financial details and tax file numbers may be another example of OFFICIAL: Sensitive information—while they are not sensitive information for the purposes of the Privacy Act, the compromise of this information could still lead to limited damage to individuals.
- commercial or economic data that, if compromised, would undermine an Australian organisation or company, or
- official information that, if compromised, would impede development of government policies.

Table 1 Business Impact Levels tool – Assessing damage to the national interest, government, organisations or individuals

	Protective marking (non-mandatory)	Security classified information (mandatory)			
	OFFICIAL	**OFFICIAL: Sensitive**	**PROTECTED**	**SECRET**	**TOP SECRET**
	1 Low business impact	**2 Low to medium business impact**	**3 High business impact**	**4 Extreme business impact**	**5 Catastrophic business impact**
Sub-impact category ↓	**The majority of official information created or processed by the public sector.** This includes routine business operations and services. OFFICIAL is not a security classification and compromise of OFFICIAL information would result in **no or insignificant damage to individuals, organisations or government.**	**OFFICIAL information that due to its sensitive nature requires limited dissemination.** Compromise of OFFICIAL: Sensitive information would be expected to cause **limited damage to an individual, organisation or government.**	**Valuable, important and sensitive information.** Compromise of PROTECTED information would be expected to cause **damage to the national interest, organisations or individuals.**	**Very valuable, important and sensitive information.** Compromise of SECRET information would be expected to cause **serious damage to the national interest, organisations or individuals.**	**The most valuable, important and sensitive information.** Compromise of TOP SECRET information would be expected to cause **exceptionally grave damage to the national interest, organisations or individuals.**
Potential impact on individuals from compromise of the information					
Dignity or safety of an individual (or those associated with the individual)	Information from routine business operations and services. Includes personal information as defined in the Privacy Act.[i] This may include information (or an opinion) about an identifiable individual (eg members of the public, staff etc) but would not include information defined as sensitive information under the Privacy Act.	Limited damage to an individual is: a. potential harm, for example injuries that are not serious or life threatening or b. discrimination, mistreatment, humiliation or undermining an individual's dignity or safety that is **not life threatening**.	Damage to an individual is discrimination, mistreatment, humiliation or undermining of an individual's dignity or safety that leads to potentially **significant harm or potentially life-threatening injury**.	Serious damage is discrimination, mistreatment, humiliation or undermining people's dignity or safety that could reasonably be expected to **directly threaten or lead to the loss of life of an individual or small group**.	Exceptionally grave damage is: a. widespread loss of life b. discrimination, mistreatment, humiliation or undermining people's dignity or safety that could reasonably be expected to directly lead to the death of a large number of people.
Potential impact on organisations from compromise of the information					
Entity operations, capability and service delivery	Information from routine business operations and services.	Limited damage to entity operations is: a. a degradation in organisational capability to an extent and duration that, while the **entity can perform its primary functions**, the effectiveness of the functions is noticeably reduced b. minor loss of confidence in government.	Damage to entity operations is: a. a degradation in, or loss of, organisational capability to an extent and duration that the **entity cannot perform one or more of its primary functions** b. major loss of confidence in government.	Serious damage to entity operations is: a. a severe degradation in, or loss of, organisational capability to an extent and duration that the **entity cannot perform any of its functions** b. directly threatening the internal stability of Australia.	Not applicable. Impacts on an entity or organisation due to compromise of information are assessed as to the level of impact to the national interest.
Entity assets and finances, eg operating budget	Information compromise would result in insignificant impact to the entity assets or annual operating budget.	Limited damage to entity assets or annual operating budget is equivalent to **$10 million to $100 million**.	Damage is: a. substantial financial loss to an entity b. **$100 million to $10 billion** damage to entity assets.	Not applicable. Impacts on an entity or organisation at this scale are considered a matter of national interest.	Not applicable. Impacts on an entity or organisation due to compromise of information are assessed as to the level of impact to the national interest.
Legal compliance, eg information compromise would cause non-compliance with legislation,[ii] commercial confidentiality or legal professional privilege	Information compromise would not result in legal and compliance issues.	Limited damage is: a. issues of legal professional privilege for communications between legal practitioners and their clients b. contract or agreement non-compliance c. failure of statutory duty d. breaches of information disclosure limitations under legislation resulting in less than two years' imprisonment.	Damage is: a. failure of statutory duty or breaches of information disclosure limitations under legislation resulting in two or more years' imprisonment.	Not applicable. Impacts on an entity or organisation at this scale are considered a matter of national interest.	Not applicable. Impacts on an entity or organisation due to the compromise of information are assessed as to the level of impact to the national interest.
Aggregated data[iii]	An aggregation of routine business information.	A significant aggregated holding of information that, if compromised, would cause limited damage to the national interest, organisations or individuals.	A significant aggregated holding of sensitive information that, if compromised, would cause damage to the national interest, organisations or individuals.	A significant aggregated holding of sensitive or classified information that, if compromised, would cause serious damage to the national interest, organisations or individuals.	A significant aggregated holding of sensitive or classified information that, if compromised, would cause exceptionally grave damage to the national interest, organisations or individuals.
Potential impact on government or the national interest from compromise of the information					
Policies and legislation	Information compromise from routine business operations and services. For example, this may include information in a draft format (not otherwise captured by higher business impact level).	Limited damage to government is impeding the development or operation of policies.	Damage to the national interest is: a. impeding the development or operation of major policies b. revealing deliberations or decisions of Cabinet, or matters submitted, or proposed to be submitted, to Cabinet[iv] (not otherwise captured by higher level business impacts).	Serious damage to the national interest is: a. a severe degradation in development or operation of multiple major policies to an extent and duration that the policies can no longer be delivered.	Exceptionally grave damage to the national interest is the collapse of internal political stability of Australia or friendly countries.
Australian economy	Information from routine business operations and services.	Limited damage to government is: a. undermining the financial viability of one or more individuals, minor Australian-based or owned organisations or companies	Damage to the national interest is: a. undermining the financial viability of a major Australian-based or owned organisation or company b. disadvantaging a number of major Australian organisations or companies	Serious damage to the national interest is: a. undermining the financial viability of an Australian industry sector (multiple major organisations in the same sector)	Exceptionally grave damage to the national interest is the collapse of the Australian economy.

	Protective marking (non-mandatory)	Security classified information (mandatory)			
	OFFICIAL	**OFFICIAL: Sensitive**	**PROTECTED**	**SECRET**	**TOP SECRET**
	1 Low business impact	**2 Low to medium business impact**	**3 High business impact**	**4 Extreme business impact**	**5 Catastrophic business impact**
Sub-impact category ↓	**The majority of official information created or processed by the public sector.** This includes routine business operations and services. OFFICIAL is not a security classification and compromise of OFFICIAL information would result in **no or insignificant damage to individuals, organisations or government.**	**OFFICIAL information that due to its sensitive nature requires limited dissemination.** Compromise of OFFICIAL: Sensitive information would be expected to cause **limited damage to an individual, organisation or government.**	**Valuable, important and sensitive information.** Compromise of PROTECTED information would be expected to cause **damage to the national interest, organisations or individuals.**	**Very valuable, important and sensitive information**. Compromise of SECRET information would be expected to cause **serious damage to the national interest, organisations or individuals.**	**The most valuable, important and sensitive information.** Compromise of TOP SECRET information would be expected to cause **exceptionally grave damage to the national interest, organisations or individuals.**
		b. disadvantaging a major Australian organisation or company.	c. short-term material impact on national finances or economy.	b. long-term damage to the Australian economy to an estimated total in excess of $20 billion.	
National infrastructure	Information from routine business operations and services.	Limited damage to government is damaging or disrupting state or territory infrastructure.	Damage to the national interest is damaging or disrupting significant state or territory infrastructure.	Serious damage to the national interest is shutting down or substantially disrupting significant national infrastructure.	Exceptionally grave damage to the national interest is the collapse of all significant national infrastructure.
International relations	Information from routine business operations and diplomatic activities.	Limited damage to government is minor and incidental damage or disruption to diplomatic relations.	Damage to the national interest is: a. short-term damage or disruption to diplomatic relations b. disadvantaging Australia in international negotiations or strategy.	Serious damage to the national interest is: a. severely disadvantaging Australia in major international negotiations or strategy b. directly threatening internal stability of friendly countries, leading to widespread instability c. raising international tension or severely disrupting diplomatic relations resulting in formal protest or sanction.	Exceptionally grave damage to the national interest is directly provoking international conflict or causing exceptionally grave damage to relations with friendly countries.
Crime prevention, defence or intelligence operations	Information from routine business operations and services.	Limited damage to government is: a. impeding the detection, investigation, prosecution of, or facilitating the commission of low-level crime b. affecting the non-operational effectiveness of Australian or allied forces without causing risk to life.	Damage to the national interest is: a. impeding the detection, investigation, prosecution of, or facilitating the commission of an offence with two or more years imprisonment b. affecting the non-operational effectiveness of Australian or allied forces that could result in risk to life.	Serious damage to the national interest is major long-term impairment to the ability to investigate or prosecute serious organised crime[v] affecting the operational effectiveness, security or intelligence capability of Australian or allied forces.	Exceptionally grave damage to the national interest is significantly affecting the operational effectiveness, security or intelligence operations of Australian or allied forces.

Table 1 notes:

[i] Section 6 of the *Privacy Act 1988* provides definitions of 'personal information' and 'sensitive information':

> '***personal information*** means information or an opinion about an identified individual, or an individual who is reasonably identifiable:
>
> (a) whether the information or opinion is true or not; and
> (b) whether the information or opinion is recorded in a material form or not.'
>
> '***sensitive information*** means:
>
> (a) information or an opinion about an individual's:
> (i) racial or ethnic origin; or
> (ii) political opinions; or
> (iii) membership of a political association; or
> (iv) religious beliefs or affiliations; or
> (v) philosophical beliefs; or
> (vi) membership of a professional or trade association; or
> (vii) membership of a trade union; or
> (viii) sexual orientation or practices; or
> (ix) criminal record;
> (that is also personal information); or
> (b) health information about an individual; or
> (c) genetic information about an individual that is not otherwise health information; or
> (d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
> (e) biometric templates.'

Where compromise of personal information, especially sensitive information under the Privacy Act would lead to damage, serious damage or exceptionally grave damage to individuals, this information warrants classification.

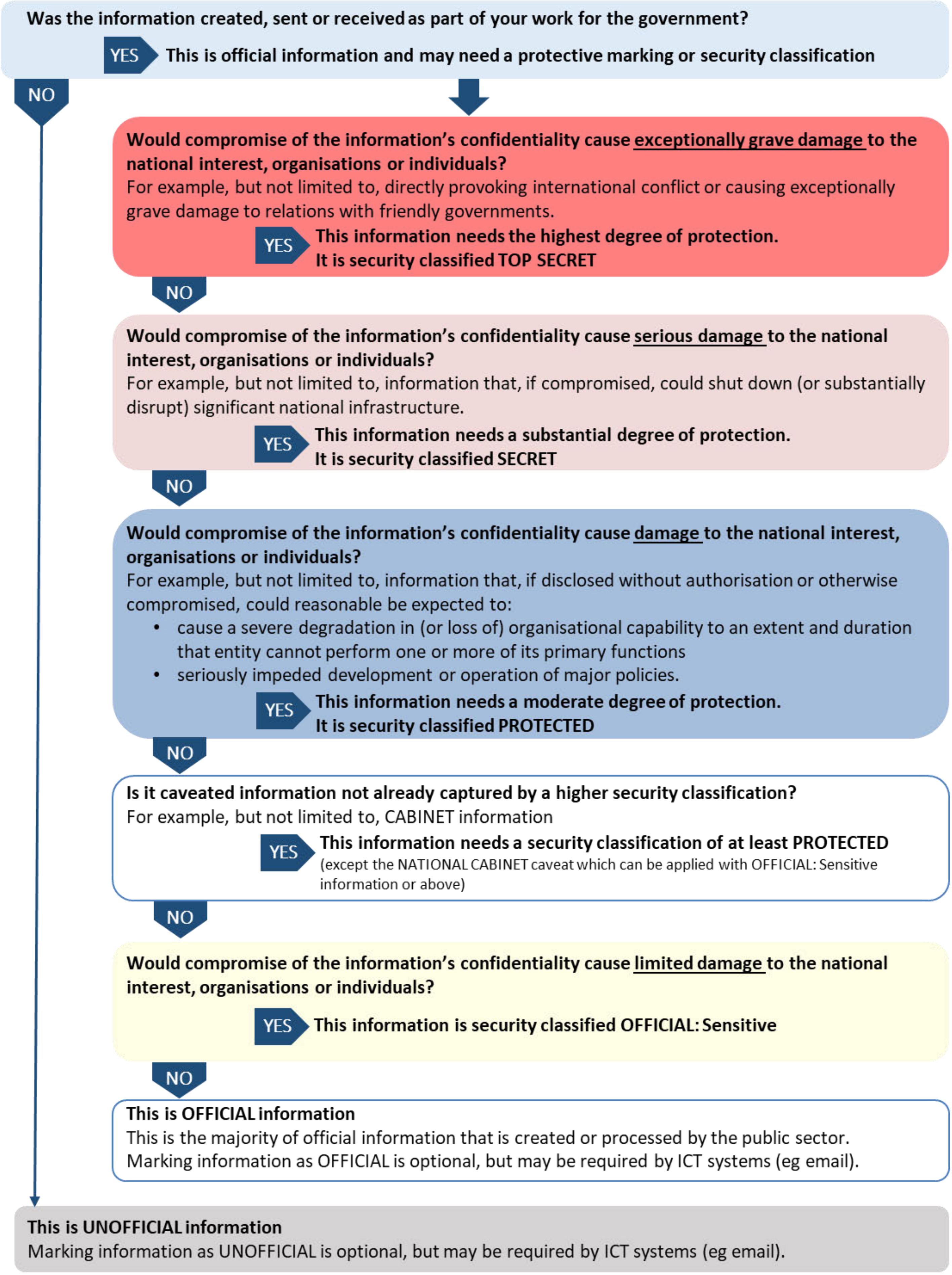
[ii] In its report Secrecy Laws and Open Government in Australia the Australian Law Reform Commission identified 506 secrecy provisions in 176 pieces of legislation, including 358 distinct criminal offences. Examples of legislation including secrecy provisions include: *Social Security Act 1991* and *Social Security (Administration) Act 1999, Taxation Administration Act 1953, Census and Statistics Act 1905*, and, more generally, the *Criminal Code Act 1995*.

[iii] A compilation of information may be assessed as requiring a higher security classification where the compilation is significantly more valuable than its individual components. This is because the collated information reveals new and more sensitive information or intelligence than would be apparent from the main source records and would cause greater damage than individual documents. When viewed separately, the components of the information compilation retain their individual classifications. See Annex H for guidance on assessing aggregated and integrated data.

[iv] This includes official records of Cabinet, Cabinet business lists, minutes, submissions, memoranda or matters without submission, and any other information that has been submitted or proposed to be submitted to Cabinet.

[v] Serious organised crime as defined in the Convention Against Transnational Organised Crime.

Figure 1 Assessing whether information is sensitive or security classified



Was the information created, sent or received as part of your work for the government?

YES **This is official information and may need a protective marking or security classification**

NO

Would compromise of the information's confidentiality cause exceptionally grave damage to the national interest, organisations or individuals?

For example, but not limited to, directly provoking international conflict or causing exceptionally grave damage to relations with friendly governments.

YES **This information needs the highest degree of protection. It is security classified TOP SECRET**

NO

Would compromise of the information's confidentiality cause serious damage to the national interest, organisations or individuals?

For example, but not limited to, information that, if compromised, could shut down (or substantially disrupt) significant national infrastructure.

YES **This information needs a substantial degree of protection. It is security classified SECRET**

NO

Would compromise of the information's confidentiality cause damage to the national interest, organisations or individuals?

For example, but not limited to, information that, if disclosed without authorisation or otherwise compromised, could reasonable be expected to:

- cause a severe degradation in (or loss of) organisational capability to an extent and duration that entity cannot perform one or more of its primary functions
- seriously impeded development or operation of major policies.

YES **This information needs a moderate degree of protection. It is security classified PROTECTED**

NO

Is it caveated information not already captured by a higher security classification?

For example, but not limited to, CABINET information

YES **This information needs a security classification of at least PROTECTED** (except the NATIONAL CABINET caveat which can be applied with OFFICIAL: Sensitive information or above)

NO

Would compromise of the information's confidentiality cause limited damage to the national interest, organisations or individuals?

YES **This information is security classified OFFICIAL: Sensitive**

NO

This is OFFICIAL information

This is the majority of official information that is created or processed by the public sector. Marking information as OFFICIAL is optional, but may be required by ICT systems (eg email).

This is UNOFFICIAL information

Marking information as UNOFFICIAL is optional, but may be required by ICT systems (eg email).

C.2.6 Sanitising, reclassifying or declassifying information

34. **Requirement 3** mandates that the originator of the information remains responsible for controlling the sanitisation, reclassification or declassification of its information. No other entity may change the information's classification unless authorised to do so by the originator.

35. Information may require modification (sanitising) to allow its wider distribution and potential use. Information can be changed to reduce its security classification by editing, redacting or altering information to protect intelligence, sources, methods, capabilities, analytical procedures or privileged information. Once sanitised, the information can be declassified or reclassified (see **Table 2**).

Table 2 Definitions reclassification and declassification of information

Term	Definition
Reclassification	The administrative decision to change the security classification of information based on a reassessment of the potential impacts of its compromise. Reclassification may raise or lower the security classification of information.
Declassification	The administrative decision to reduce the security classification of information to OFFICIAL (an unclassified state) when it no longer requires security classification handling protections.

36. The Department of Home Affairs recommends entities develop an approach for noting when the originator has approved the reclassification or declassification of information. For example:

> ~~TOP SECRET~~ SECRET (declassification approved by originator [*insert name, role, delegation or section*], on [*insert date*], document reference number [*insert document management system reference of originator's approval*]).

37. The Department of Home Affairs recommends entities establish procedures so that information is automatically declassified:

    a. if the originator set a specific date or event for declassification based on an assessment of the period in which the information might cause damage, when that date or event occurs.

    b. if the originator did not set a specific date or event for declassification, when the open access period under the *Archives Act 1983* commences. For guidance on open access periods, see the National Archives of Australia website.

38. The Department of Home Affairs also recommends entities establish procedures to encourage regular review of classified information for continuing sensitivity (ie if the compromise of the information would still cause damage) using the impact-based classification assessment described in C.2.4 When to assess information security classification. For example, these reviews could be done after a project is completed or when a file is withdrawn from (or returned to) use. Information is declassified or reclassified to a lower classification when a reassessment of its Business Impact Level indicates it no longer meets the original Business Impact Level to which its classification applies.

39. Consistent with **Requirement 4**, information that has been reclassified or declassified must be clearly identified using an applicable protective marking to reflect the new assessment of the Business Impact Level—see C.5.1 Protective markings for security classified information.

C.2.7 Historical security classifications

40. There are historical security classifications and other protective markings (eg CONFIDENTIAL classification) that no longer reflect Australian Government policy. For assistance in applying appropriate handling protections (and assessing damage to the national interest, organisations or individuals) to historical classifications, see **Annex E**.

C.3 Caveats and accountable material

41. Caveats are a warning that the information has special protections in addition to those indicated by the security classification of PROTECTED or higher (or in the case of the NATIONAL CABINET caveat, OFFICIAL: Sensitive or higher).

42. The Australian Government Security Caveats Guidelines establishes four categories of caveats:

    a. codewords (sensitive compartment information)

    b. foreign government markings

    c. special handling instructions

    d. releasability caveats.

43. **Table 3** describes caveats commonly used across government.

44. Caveats are not classifications and must appear with an appropriate security classification of PROTECTED or higher (or in the case of the NATIONAL CABINET caveat, OFFICIAL: Sensitive or higher).

45. Accountable material is information that requires the strictest control over its access and movement. Accountable material includes:

    a. TOP SECRET security classified information

    b. some types of caveated information, being:

        i. all codeword information

        ii. select special handling instruction caveats, particularly CABINET information at any security classification

    c. any classified information designated as accountable material by the originator.

46. What constitutes accountable material may vary from entity to entity and could include budget papers, tender documents and sensitive ministerial briefing documents.

47. **Requirement 6** mandates that caveated information and accountable material be clearly marked and handled in accordance with the originator and the caveat holder's special handling requirements as established in the Australian Government Security Caveats Guidelines. These special caveat requirements apply in addition to the classification handling requirements. Additional information about handling caveats is available in the Sensitive Material Security Management Protocol and the Australian Government Security Caveats Guidelines on a need-to-know basis on GovTEAMS.

48. **Requirement 3** requires the originator's approval to remove or change a security classification applied to information. To be consistent with **Requirement 3**, the prior agreement of the originating entity also needs to be obtained to remove a caveat.

Table 3 Caveat types

Caveat types	What kinds of information does this type of caveat cover	What special handling requirements does this caveat impose
Codewords (sensitive compartmented information)	Use of codewords is primarily within the national security community. A codeword indicates that the information is of sufficient sensitivity that it requires protection in addition to that offered by a security classification. Each codeword identifies a special need-to-know compartment. A compartment is a mechanism for restricting access to information by defined individuals who have been 'briefed' on the particular sensitivities of that information and any special rules that may apply. The codeword is chosen so that its ordinary meaning is unrelated to the subject of the information.	It may be necessary to take precautions beyond those indicated by the security classification to protect the information. These will be specified by the entity that owns the information, for instance those with a need to access the information will be given a special briefing first.
Foreign government markings	Foreign government markings are applied to information created by Australian agencies from foreign source information.	PSPF policy 7: Security governance for international sharing requires that, where an international agreement or international

Caveat types	What kinds of information does this type of caveat cover	What special handling requirements does this caveat impose
		arrangement is in place, entities must safeguard security classified foreign entity information or assets in accordance with the provisions set out in the agreement or arrangement. Foreign government marking caveats require protection at least equivalent to that required by the foreign government providing the source information.
Special handling instructions	Use of special handling instructions is primarily within the national security community. Some special handling instructions are used more broadly across government, as follows:	Special handling instructions indicate particular precautions for information handling.
	EXCLUSIVE FOR (named person) The EXCLUSIVE FOR caveat identifies information intended for access by a named recipient only.	Access to EXCLUSIVE FOR information is limited to a named person, position title or designation.
	CABINET The CABINET caveat identifies any information that: a. is prepared for the purpose of informing the Cabinet b. reveals the decision and/or deliberations of the Cabinet c. is prepared by departments to brief their ministers on matters proposed for Cabinet consideration d. has been created for the purpose of informing a proposal to be considered by the Cabinet.	The Cabinet Handbook specifies handling requirements for Cabinet documents. This includes applying a security classification of at least PROTECTED to all Cabinet documents and associated records.
	NATIONAL CABINET The NATIONAL CABINET caveat identifies any information that which has been specifically prepared for National Cabinet or its subcommittees.	The Cabinet Handbook specifies handling requirements for Cabinet documents. Information marked with the NATIONAL CABINET caveat is to be handled in accordance with Cabinet conventions and within legal frameworks and processes such as Freedom of Information, parliamentary inquiries and judicial processes. This caveat can be applied to information classified as OFFICIAL: Sensitive and above.
Releasability caveats	There are three releasability caveats used across government:	Releasability caveats limit access to information based on citizenship.
	Australian Eyes Only (AUSTEO) The AUSTEO caveat indicates only appropriately cleared Australian citizens can access the information. Additional citizenships do not preclude access.	Information marked AUSTEO is only passed to, or accessed by, Australian citizens. While a person who has dual Australian citizenship may be given AUSTEO-marked information, in no circumstance may the Australian citizenship requirement be waived.
	Australian Government Access Only (AGAO) The AGAO caveat indicates information that can only be accessed by appropriately cleared Australian citizens and appropriately cleared representatives of Five-Eyes Governments on exchange, secondment, long-term posting or attachment within the National Intelligence Community and the Department of Defence.	AGAO information must not be distributed to the Five Eyes foreign representative's parent agency or government. AGAO information may not be shared with any other foreign nationals. Where appropriate, all entities may apply the AGAO caveat to classified information. However, entities other than members of the National Intelligence Community and the Department of Defence must handle AGAO material as if it were marked AUSTEO.
	Releasable To (REL) The Releasable To (REL) caveat identifies information that has been released or is releasable to citizens of the indicated countries only.	For example, REL AUS/CAN/GBR/NZL/USA means that the information may be passed to citizens of Australia, Canada, United Kingdom, New Zealand and the United States of America only.

Caveat types	What kinds of information does this type of caveat cover	What special handling requirements does this caveat impose
	Countries are identified using three letter country codes from International Standard ISO 3166-1:2013 Codes for the representation of names of countries and their subdivisions – Alpha 3 codes.	The caveat is an exclusive marking that disqualifies a third-party national seconded or embedded in an Australian or foreign government entity from accessing the information.

C.4 Information management markers

49. **Information management markers are an optional way for entities to identify information that is subject to non-security related restrictions on access and use. They are subset of the controlled list of terms for the 'Rights Type' property in the National Archives of Australia's AGRkMS.**

50. **Information management markers are not protective markers.**

51. **The information management markers are described in Table 4.**

Table 4 Assessing whether to use an information management marker (IMM)

Whether to use an IMM	Which IMM to use	Notes
If the information is subject to legal professional privilege	Use the **legal privilege** IMM – Restrictions on access to, or use of, information covered by legal professional privilege.	Compromise of the confidentiality of information subject to legal professional privilege is likely to cause at least limited damage to the national interest, organisations or individuals. The Department of Home Affairs recommends that the legal privilege IMM only be used with **OFFICIAL: Sensitive or above**.
If the information is subject to one or more legislative secrecy provisions	Use the **legislative secrecy** IMM – Restrictions on access to, or use of, information covered by specific legislative secrecy provisions. – Apply with a warning notice that informs the recipient of relevant provisions.	Legislative secrecy provisions impose confidentiality obligations on individuals or entities. Compromise of the confidentiality of information subject to legislative secrecy provisions is likely to cause at least limited damage to the national interest, organisations or individuals. The legislative secrecy IMM is used to draw attention to the applicability of one or more specific secrecy provisions. The Department of Home Affairs recommends that the recipient is informed of the specific provision by including a warning notice placed at the top or bottom of each page of a document or in the body of an email that expressly identifies the specific secrecy provisions under which the information is covered. **Examples of warning notices:** • Legislative Secrecy Warning: Unless you have written consent from the [insert authority or relevant position], it is an offence under section XX of the XXX Act to [insert details of restrictions]. • This information is subject to [insert reference to section of relevant legislation]. Compromise or improper handling of this information may result in [insert relevant penalty]. This information can only be incorporated in other material which bears the legislative secrecy IMM and contains this warning notice. The Department of Home Affairs recommends that the legislative secrecy IMM only be used with **OFFICIAL: Sensitive or above**.

If the information is personal information as defined in the *Privacy Act 1988*	Use the **personal privacy** IMM – Restrictions under the Privacy Act on access to, or use of, personal information collected for business purposes.	The Privacy Act requires entities to protect the personal information they hold from misuse, interference, loss, and from unauthorised access, modification or disclosure. The Act defines personal information as 'information or an opinion about an identified individual, or an individual who is reasonably identifiable'. The Privacy Act also defines 'sensitive information' which includes personal information about an individual's: – racial or ethnic origin – political opinions – membership of a political organisation – religious beliefs or affiliations – philosophical beliefs – membership of a professional or trade organisation or trade union – sexual orientation or practices – criminal record – health or genetic information – some aspects of biometric information The Privacy Act generally affords a higher level of privacy protection to sensitive information than to other personal information. The Department of Home Affairs recommends that the personal privacy IMM only be used with **OFFICIAL: Sensitive or above**.

C.5 Minimum protections for security classified information

52. In addition to the following guidance, **Annexes A to C** establish the key operational controls to protect security classified information.

53. Consistent with Requirement 2 of PSPF policy 2: Management structures and responsibilities, each entity is required to develop and use procedures to cover all elements of protective security, including protecting security classified information.

54. The Department of Home Affairs recommends entity personnel consult with their own entity security team for advice on the application of protections for security classified information. Entity-specific procedures may require personnel to implement the protections in particular ways or to apply a higher level of protection, in order to meet business needs or to address the entity's security risk environment.

C.5.1 Protective markings for security classified information

55. Applying protective markings to security classified information indicates that the information requires protection, and dictates the level of protection required. Protective markings help control and prevent compromise of information as they are an easily recognisable way for information users (visually) and systems (such as an entity's email gateway) to identify the level of protection the information requires.

56. **Requirement 4** mandates that the originator clearly identify security classified information by using applicable protective markings. **Requirement 5** mandates that entities apply the AGRkMS to protectively mark information on systems that store, process or communicate security classified information.

57. The OFFICIAL marker may be used to identify information that is an Australian Government record that is not security classified. Similarly, the UNOFFICIAL marker may be used to identify information generated for personal or non-work related purposes. Use of these markers is not mandatory.

C.5.1.1 Applying text-based protective markings

58. **Requirement 4** indicates text-based protective markings are the preferred method to identify security classified information. Figure 2 Protectively marking physical (printed) information provides an example of applying protective markings.

Figure 2 Protectively marking physical (printed) information

In this example, paragraph 1 contains the most valuable, important and sensitive information in the document. The information in this paragraph dictates the document's overall classification.

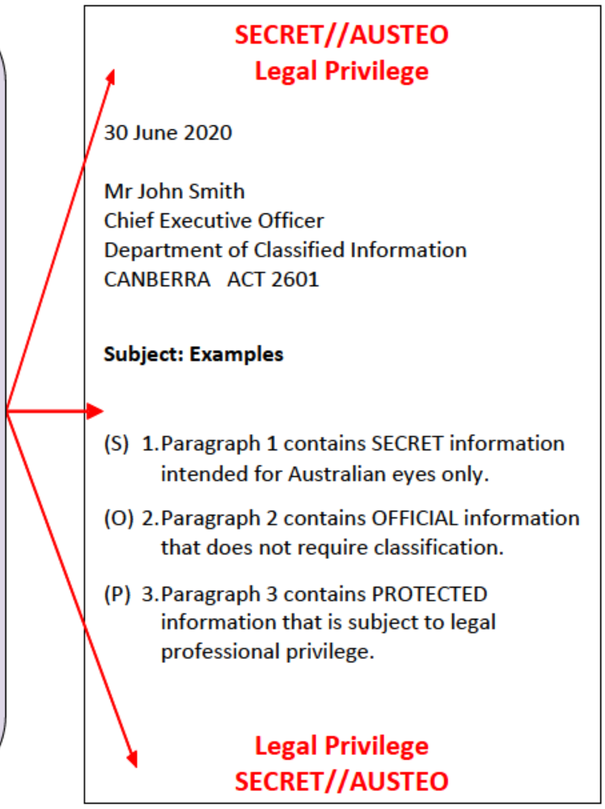
Compromise of the information in paragraph 1 could be expected to cause serious damage to the national interest, organisations or individuals. The information in paragraph 1 is classified as SECRET. This means the document's overall classification is also SECRET.

Additionally, the information in paragraph 1 can only be accessed by Australian citizens and the AUSTEO caveat has been applied. For guidance on caveats, see C.3 Caveats and accountable material .

Paragraph 3 contains information that is subject to legal professional privilege. For guidance on (optional) information management markers, see C.4 Information management markers.

To meet the protective marking requirements, the SECRET marking is conspicuously applied to the top and bottom of the page. An AUSTEO caveat marking is also applied. The double forward slash helps to clearly differentiate each marking. As this entity uses the optional information management markers, the legal privilege marking is also applied.

The entity has also used the optional paragraph grading indicators to mark each paragraph separately.



SECRET//AUSTEO
Legal Privilege

30 June 2020

Mr John Smith
Chief Executive Officer
Department of Classified Information
CANBERRA ACT 2601

Subject: Examples

(S) 1. Paragraph 1 contains SECRET information intended for Australian eyes only.

(O) 2. Paragraph 2 contains OFFICIAL information that does not require classification.

(P) 3. Paragraph 3 contains PROTECTED information that is subject to legal professional privilege.

Legal Privilege
SECRET//AUSTEO

C.5.1.2 Applying protective markings if text-based markings cannot be used

59. If text-based markings cannot be used (eg on certain media or assets), **Requirement 4** mandates that colour-based markings must be used. **Annexes A to C** identify the recommended colours to use for a colour-based marking system.

60. Colour-based markings use the RGB model, which refers to Red (R), Green (G) and Blue (B) colours that can be combined in various proportions to obtain any colour in the visible spectrum. **Table 5** specifies the recommended RGB colour-based marking that applies to each security classification. There are no specific RGB colours for OFFICIAL: Sensitive and OFFICIAL information, although a Yellow colour is recommended for OFFICIAL: Sensitive.

Table 5 RGB and CMYK cell colour for colour-based markings

Security classification	Colour-based marking	RGB cell colour	CMYK cell colour
OFFICIAL: Sensitive	Yellow	R 255, G 242, B 204	C 0%, M 5%, Y 20%, K 0%
PROTECTED	Blue	R 79, G 129, B 189	C 58%, M 32%, Y 0%, K 26%
SECRET	Pink/Salmon	R 229, G 184, B 183	C 0%, M 20%, Y 20%, K 10%
TOP SECRET	Red	R 255, G 0, B 0	C 0%, M 100%, Y 100%, K 0%

61. If both text-based and colour-based markings cannot be used (eg for verbal information), entities must use a scheme to identify security classified information. **Requirement 4** mandates that the scheme must be documented and that entities must train personnel appropriately. For example, a scheme could include an entity policy for meetings that may include discussion of classified information—that participants identify at the commencement of the meeting the level of security classified information to be discussed.

62. Other markings, for example entity-specific markings, are not recognised by this policy. A standard set of markings ensures common understanding, consistency and interoperability across systems and government entities. Other markings may confuse users about appropriate handling protections.

C.5.1.3 Applying protective markings through metadata

63. Metadata is a term used for 'data about data'. On ICT systems, text-based protective markings are supplemented by the use of metadata to describe, among other things, key security characteristics of information.

64. For electronic records management systems, the National Archives of Australia produces the AGRkMS to provide standardised metadata terms and definitions for consistency across government. The minimum metadata set is a practical application of the standard that identifies the metadata properties essential for agency management and use of business information. **Requirement 5** mandates that entities apply the AGRkMS metadata properties.

65. From an information security perspective, there are three metadata properties of importance:

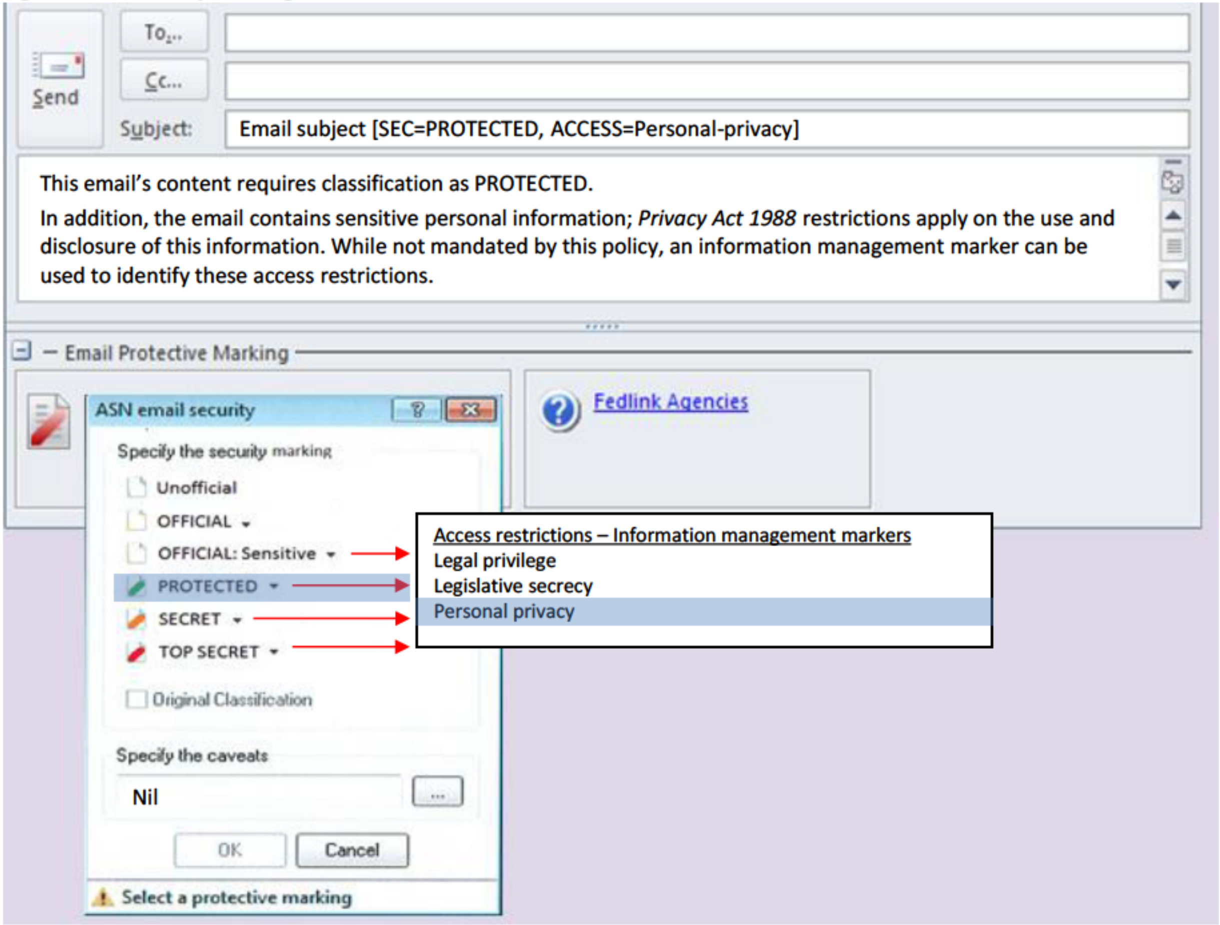
    a. security classification property—identifies the security classification of the information and is used to identify information that is restricted to users with appropriate security clearance permissions. **Requirement 5** mandates application of this property for all classified information

    b. security caveat property—can be used with the security classification property. This property identifies that the information requires additional special handling and that only people cleared and briefed to see it may have access. **Requirement 5** mandates application of this property for caveat information

    c. rights property—optional property to identify non-security related restrictions on the use or access to records. The National Archives of Australia has established a subset of rights property terms for common usage as information management markers to categorise information.

66. For emails, the preferred approach is for entities to apply protective markings to the internet message header extension, in accordance with the Email Protective Marking Standard at **Annex F**. This helps with construction and parsing by email gateways and servers, and allows for information handling based on the protective marking. Where an internet message header extension is not possible, protective markings are placed in the subject field of an email. See **Figure 3** for an example of a protectively marked email.

Figure 3 Protectively marking an email



Subject: Email subject [SEC=PROTECTED, ACCESS=Personal-privacy]

This email's content requires classification as PROTECTED.

In addition, the email contains sensitive personal information; *Privacy Act 1988* restrictions apply on the use and disclosure of this information. While not mandated by this policy, an information management marker can be used to identify these access restrictions.

Specify the caveats: Nil

67. When printed, an email is considered a physical document, as such, a visual presentation of the protective marking (such as a separate line in the email) is important.

C.5.2 Limiting disclosure and access to security classified information

68. The vast majority of official information can be shared, where appropriate. The PSPF policy 9: Access to information states that:

> *Each entity must enable appropriate access to official information. This includes ... ensuring that those who access security classified information are appropriately security cleared and need to know that information.*

C.5.2.1 Limiting by need-to-know principle

69. PSPF policy 9: Access to information establishes that the need-to-know principle applies for all access to security classified information. Limiting access by staff and others (eg contractors) to information on a need-to-know basis guards against the risk of unauthorised access or misuse of information. Personnel are not entitled to access information merely because it would be convenient for them to know or because of their status, position, rank or level of authorised access.

70. The Department of Home Affairs recommends that entities consider staff access to OFFICIAL information on a need-to-know basis, although this is not a requirement of the PSPF.

C.5.2.2 Limiting by security clearance level

71. PSPF policy 9: Access to information establishes the level of security clearance required to access security classified information. This requirement is restated in **Annexes A to C**.

72. For further guidance on obtaining personnel security clearances see PSPF policy 12: Eligibility and suitability of personnel.

C.5.2.3 Keeping records of disclosure and access

73. Monitoring and auditing the dissemination of information plays an important role in information protection.

74. For highly classified or caveated information (such as TOP SECRET information or accountable material), it is critical to maintain an auditable register (such as a Classified Document Register or electronic document management system or repository) of all incoming and outgoing information and material, transfers or copying, along with regular spot check audits. Personnel can conduct spot check audits by sighting documents listed in the register and documenting the process (eg counter-signing the register).

75. The Department of Home Affairs recommends that entities:

    a. keep an audit log or register for documents at other classification levels (particularly for SECRET information), or registered information received from other entities.

    b. develop procedures for regular spot checks to ensure accountable material (including TOP SECRET information) is accounted for and being handled, used and stored appropriately. For example, do a spot check of 5 per cent of TOP SECRET files per month, with 100 per cent of TOP SECRET files checked within a two-year period

    c. use receipts for transfer of all security classified information. Receipts can be used to identify the date and time of dispatch, the dispatching officer's name and a unique identifying number. Additionally, receipts can be used as a mechanism to control the incoming transfer of information (eg a two-part receipt placed in the inner envelope with the information means the addressee can keep one portion and sign and return the other to the sender).

76. There may be other legislative requirements for record keeping. For example, under the *Privacy (Australian Government Agencies – Governance) APP Code 2017*, a Privacy Officer is required to maintain a record of an entity's personal information holdings and a register of privacy impact assessments.

77. Markings such as page and reference numbering can be used to identify and track classified information. There may be other reasons to use reference markings, for example **Requirement 6** mandates the use of page and reference numbering for all accountable material, even if it is not security classified.

C.5.3 Using security classified information

78. It is a core requirement of this policy that entities 'implement operational controls for their information holdings, proportional to their value, importance and sensitivity'. Consistent with this requirement, PSPF policy 15: Physical security for entity resources, mandates that:

    > *Each entity must implement physical security measures that minimise or remove the risk of…information and physical asset resources being made inoperable or inaccessible, or being accessed, used or removed without appropriate authorisation.*

79. When security classified information is being 'used'—able to be read, viewed, heard or comprehended—it may be at higher risk of compromise. Different physical environments pose different risks for information compromise.

80. Entities can minimise risk through the application of operational controls, complementing the physical security measures required under PSPF policy 15. The Department of Home Affairs recommends entities establish procedures that facilitate personnel maintaining good security practices while using security classified information, including:

    a. maintaining *awareness* of their environment, including who will or could access, use or remove information for which the officer is responsible and whether they could be exposed to information they are not authorised to access.

    b. exercising *judgement* to assess environmental suitability

    c. taking *appropriate steps* to minimise the risk of an unauthorised person accessing, using or removing the information.

    d. employing appropriate *physical handling* of information, for example when carrying or when the information is not in active use.

81. **Annexes A to C** establish the physical security zones where different levels of security classified information can be used.

C.5.3.1 Using information when working away from the office

82. Working away from the office is all work undertaken by personnel away from entity facilities, including using mobile computing and communications. PSPF policy 15: Physical security for entity resources recommends that when personnel are working away from the office:

> *…entities consider the security risks of the environments in which their personnel operate, the type of information that will be used and how that information will be accessed.*

Relevant definitions

Use: Information is in **use** if it can be read, viewed, heard or comprehended by a person.

Entity facility: An entity facility means the physical security zones of an Australian agency or department, and includes Australian Government embassies, high commissions and consulates.

Teleworkers: personnel with remote ICT access in a fixed location.

Regular ongoing home-based work: is where an arrangement exists between an individual and their agency/manager for them to work from home on an ongoing basis. Any other work done at home is **occasional home-based work**.

83. The Department of Home Affairs recommendations for maintaining good security practices when using security classified information in an entity facility (C.5.3 Using security classified information) are also relevant where security classified information is used when working away from the office.

84. Business requirements may mean personnel need to use or store security classified information in:

    a. other entities' facilities (eg to attend a meeting)

    b. alternative office spaces (eg another entity's facility, state or territory government facilities, allied secure and accredited facilities)

    c. private homes (eg for regular ongoing home-based work or occasional home-based work)

    d. public spaces (eg public transport, cafés, restaurants, hotels and transit lounges) within Australia

    e. facilities overseas (eg to attend a meeting with foreign country officials).

85. In some situations, for practical reasons personnel may need to hold the information for a period of time before reaching the location in which they will use the information—for example, taking information home the night before an early meeting or early travel to another city within Australia.

86. The officer who removes security classified information from a security zone is the responsible officer. The responsible officer has custody of the information and is responsible for handling the information in accordance with the minimum protections for the classification. **Annexes A to C** establish the minimum protections for using security classified information outside the entity's facility, including outlining information that may not be taken out of entity facilities.

87. Where the responsible officer:

    a. needs to store security classified information outside an entity facility, the guidance at C.5.4 Storing security classified information applies

    b. needs to carry security classified information from one location, to use at a second location (for example, from their entity facility to use at home or to attend a meeting in another entity's facility), the guidance at C.5.5 Carrying security classified information applies

    c. needs to transfer security classified information to another individual, the guidance at C.5.6 Transferring and transmitting security classified information applies.

C.5.3.2 Using information and data on mobile computing and communications

88. Mobile computing and communications encompass work using computing and communications devices such as laptops, notebooks, tablets, smart mobile phones and personal digital assistants. Given their portable nature, these mobile devices provide a platform for entity mobility by enabling personnel to use, store and communicate security classified information away from the traditional desktop environment.

89. The Department of Home Affairs' recommendations for maintaining good security practices when using security classified information in an entity facility (C.5.3 Using security classified information) are also relevant where security classified information is being used via a mobile device, whether within or outside an entity facility. Similarly, the guidance at C.5.4 Storing security classified information applies.

90. **Annexes A to C** establish the minimum protections for accessing, storing or communicating security classified information on government-issued mobile devices and non-government issued mobile devices.

a. A **government-issued mobile device** is a mobile or portable computing communications device that is owned and issued by an Australia Government entity to access government systems and data and is approved by the relevant authority to process, store or communicate entity information of a specified classification. This includes mobile phones, handheld computers, tablets, laptops and personal digital assistants configured, encrypted and managed to the Australian Signals Directorate's (ASD) standards and guidance (as detailed in the Australian Government Information Security Manual). This also includes Australian Government-issued mobile devices that for operational reasons are connected to isolated networks, for example standalone or air gapped devices. If these requirements are met, then a government-issued mobile device is considered in a 'secured state'.

b. Non-government mobile devices comprise:

    i. **Authorised non-government device** – mobile or portable computing communications devices (including mobile phones, handheld computers, tablets, laptops and digital assistants) owned or issued by a non-government source (for example commercial organisation, non-government organisation, industry-issued or privately owned) that is configured, encrypted and managed in accordance with ASD standards and guidance, and the residual risk is accepted by the Australian Government entity system risk owner to access, process, store or communicate OFFICIAL, OFFICIAL: Sensitive, PROTECTED Australian Government information or data. Non-government devices must not access, process, store or communicate SECRET or TOP SECRET information or data. If these requirements are fully met, then a non-government mobile device is considered in a 'secured state'. If these requirements are not fully met, then the device is considered in an 'unsecured state'.

    ii. **All other mobile devices –** devices that are not owned, issued or authorised by the entity. These devices must not be authorised to access, process, store or communicate government OFFICIAL: Sensitive or above information, and must not enter Zones 4-5 or where SECRET or TOP SECRET information or devices are present. If use of these devices required in a Zone 3, then use is subject to risk assessment and Chief Security Officer approval.

91. For virtual desktop solutions (for example Azure Virtual Desktop or Citrix) and applications (PROTECTED and below, for example, GovTEAMS PROTECTED and GovTEAMS OFFICIAL), apply the requirements of PSPF policy 11: *Robust ICT systems* and the Australian Government Information Security Manual.

92. The Department of Home Affairs recommends entities ensure that use of privately-owned mobile devices do not present an unacceptable security risk.

93. For more detailed guidance on using mobile devices, including granting access to government information or systems by personal (or privately-owned) mobile devices, see the Australian Government Information Security Manual.

C.5.3.3 Using information on official travel outside Australia

94. Special care is necessary when security classified information (physical or held on a mobile device) is removed from entity facilities for use outside Australia.

95. The Department of Home Affairs recommends entities establish entity procedures to:

    a. consider country-specific advice

    b. if required, consult with the Department of Foreign Affairs and Trade (DFAT) for practical advice, including on the availability of transfer and storage options using resources available through Australian Government embassies, high commissions and consulates, and

    c. authorise officers to travel with security classified information.

96. **Annexes A to C** establish the minimum protections for travelling with security classified information outside Australia.

C.5.4 Storing security classified information

97. When security classified information is unattended (ie it is not under the immediate control or in the physical presence of the person responsible for it), **Annex A** mandates entities ensure the information is stored securely in an appropriate security container for the approved zone. Securely storing security classified official information protects the information from compromise.

98. **Requirement 7** also applies to mobile devices holding security classified information. These items may also need protections as a valuable asset (see PSPF policy 15: Physical security for entity resources). The Department of Home Affairs recommends that mobile devices be stored in a secured state, where the device is configured and managed in accordance with the Australian Cyber Security Centre's standards and guidance and encryption is active when the device is not in use. The Australian Government Information Security Manual includes guidelines on encryption for mobile devices.

99. The Department of Home Affairs recommends that mobile devices are not stored in locations where meetings or discussions of a higher classification are held unless the mobile device is protected by visual and audio suppression container.

100. The National Archives of Australia Australian Government Information Management Standard requires that entities store information securely and preserve it in a usable condition for as long as required for business needs and community access. In accordance with the Information Management Standard, a secure and suitable storage environment is one that prevents unauthorised access, duplication, alteration, removal and destruction.

101. Ways to minimise duplication or alteration of information include:

    a. reproducing security classified information only when necessary

    b. immediately destroying spare or spoilt copies (such destruction is defined as 'normal administrative practice' in the *Archives Act 1983* and does not need specific permission from the National Archives of Australia). For guidance on destroying security classified information, see C.5.7.1 Destroying security classified information

102. **Annexes A to C** establish the minimum protections for storing security classified information and mobile devices holding information. For guidance on physical security zones, see the PSPF policy 16: Entity facilities.

C.5.4.1 Clear desk, session and screen locking procedures

103. The Department of Home Affairs recommends entities establish clear desk, session and screen locking procedures. These procedures are an additional way to protect information when unattended. These procedures promote awareness of the requirements to protect information from compromise and assist entity personnel to secure all files, documents (electronic as well as paper), security classified material (including portable and attractive items, for example iPads, mobile phones, memory sticks, portable hard drives etc) and other official information in their custody.

104. The Department of Home Affairs recommends entities' procedures prompt personnel to ensure that:

    a. no security classified information is left unattended on a desk (ie it is stored appropriately)

    b. ICT equipment (computers and media devices) is locked when not in use

    c. electronic media and devices containing security classified information are secured

    d. all portable and attractive items are secured

    e. keys to classified storage devices are secured

    f. keys are not left in doors and drawers (at the end of the day or for an extended period of time).

105. For further information on applying session and screen locking procedures, see the Australian Government Information Security Manual.

C.5.5 Carrying security classified information

106. It is important to implement effective protections when carrying security classified information from one location to use in another location, including to attend meetings inside entity facilities, outside and between entity facilities. Higher levels of protection are required if security classified information is carried through a less secure zone (eg carrying SECRET material through a Zone 1 or carrying TOP SECRET information through a Zone 1 or Zone 2) or outside the entity in public spaces.

107. The Department of Home Affairs recommends that mobile devices are not carried into meetings or discussions of a higher classification unless the mobile device is protected by visual and audio suppression container.

108. **Annexes A to C** outline the minimum protections for carrying each level of security classified information, including for carrying outside entity facilities and between entity facilities.

109. ASIO-T4 and the Security Construction and Equipment Committee (SCEC) provide advice on security equipment for protecting classified information while carrying it. This includes advice on SCEC-endorsed tamper evident seals and packaging, as well as guidance on selecting briefcases suitable for the carriage of security classified information. The advice is available on the Protective Security Policy GovTEAMS community.

110. For guidance on transferring information to another person or entity, see C.5.6 Transferring and transmitting security classified information.

C.5.6 Transferring and transmitting security classified information

111. **Requirement 7** mandates that entities ensure security classified information is transferred and transmitted by means that deter and detect compromise.

112. Examples of transferring information include:

    a. handing information to a person within an office environment (ie within entity facilities)

    b. sending information through the entity's internal mail to a person who works in the same building

    c. sending information through the entity's internal mail to a person who works in a different building

    d. handing or sending information to a person in another entity

    e. giving a person a secure approved USB or other storage device that holds the information.

113. Examples of transmitting information include:

    a. emailing information to a person within the entity or in a different entity

    b. verbally communicating information to a person within the entity or another entity (eg by telephone or videoconference).

114. To ensure security classified information is only transferred or transmitted to people with a need-to-know, entities are encouraged to identify information recipients by:

    a. a specific position, appointment or named individual

    b. where physical information is being transferred:

        i. a full location address (eg not a post office box for physical delivery, as this may be unattended)

        ii. an alternative individual or appointment where relevant (eg for TOP SECRET information).

    c. where information is being electronically transmitted, an email address exclusive to those individuals with a need-to-know (eg not a mailbox with unrestricted access).

C.5.6.1 Transferring physical security classified information

115. When transferring physical security classified information, the Department of Home Affairs recommends adopting security measures to:

    a. obscure that the information is security classified

    b. deter and detect unauthorised access to the information.

116. The security measures required to protect security classified information and caveated information and material during physical transfer depend on the security classification level of the information, where the information is going from and to, and the transfer method used.

117. **Annexes A to C** establish the minimum protections to transfer each level of security classified information. Where transfer is between physical locations:

    a. a tamper-evident double barrier is used to protect security classified information. The most common method to achieve this is 'double-enveloping'

    b. a secure transfer method is used, such as by entity safe hand or safe hand by an endorsed courier.

118. It may also be appropriate or required for entities to follow record-keeping procedures when transferring security classified information, such as use of receipts.

119. The PSPF does not impose requirements for the transfer of OFFICIAL information (as opposed to OFFICIAL: Sensitive information). The Department of Home Affairs recommends entities ensure that OFFICIAL information is transferred by means which deter and detect compromise (see **Annexes A-C**).

Explanation of double enveloping

'Double enveloping' consists of:

- a tamper evident inner barrier to detect unauthorised access
- an outer barrier to obscure the information's security classification and deter unauthorised access.

The inner 'envelope' can consist of:

- an envelope or pouch sealed with a SCEC-approved tamper evident seal so that any tampering is detected, or
- a SCEC-approved single use envelope.

The Department of Home Affairs recommends marking the classification conspicuously on the inner envelope (eg at the top and bottom of the front and back of the envelope).

The outer 'envelope' is some form of sealed opaque covering. It could be a regular mail envelope, a SCEC-approved single-use outer envelope, security briefcase, satchel, pouch or transit bag. It may display information identifying the recipient and any receipt or reference numbers, if required. The Department of Home Affairs recommends avoiding displaying any details on the outer envelope (such as protective markings) that indicate that the information is security classified information.

Explanation of safe handing

'Safe hand' means information is dispatched to the addressee in the care of an authorised person or succession of authorised people who are responsible for its carriage and safekeeping. The authorised person could be the responsible officer who removes the information from the entity facility. An authorised person could also be an endorsed courier. 'Entity safe handing' is where all of the authorised persons in the chain are officers of the entity dispatching the information.

Sending information via safe hand establishes an audit trail that provides confirmation that the addressee received the information and helps to ensure the item is transferred in an authorised and secure facility or vehicle. To deter and detect any information tampering, at each handover, a receipt is obtained showing (at a minimum) the identification number, the time and date of the handover, and the name and signature of the recipient.

Sending information via safe hand requires:

- a unique identification number; generally, this will be a receipt number
- that information be in a security briefcase (see the SCEC-Security Equipment Guide on Briefcases for the carriage of security classified information on GovTEAMS) or an approved mailbag (for information, see the SCEC-approved security equipment evaluated product list)
- that information be retained in personal custody.

Safe hand via an endorsed courier

Using an endorsed courier provides a level of assurance for the confidentiality of information being transferred, where it is not possible to use entity personnel to carry the information. This method of transfer is not suitable for protecting valuable or attractive assets such as pharmaceuticals or money. Special arrangements, such as armed escorts may be necessary in certain circumstances.

A number of commercial courier companies have been endorsed by SCEC to provide safe hand courier services. Contact ASIO-T4 by email outreach@asio.gov.aul or see the ASIO-T4 Protective security circular (PSC) 172 (available on a need-to-know basis on GovTEAMS) for advice on SCEC-endorsed safe hand courier services.

Special handling requirements may apply to caveated information. This may preclude the use of a commercial safe hand courier when using certain caveats. For guidance on caveats, see C.3 Caveats and accountable material .

C.5.6.2 Using devices to transfer or transmit security classified information

120. Devices that are able to store and communicate information, such as laptops, notebooks, tablets, smart mobile phones, personal digital assistants and USBs, can be used to both transfer and transmit information. Ways to deter and detect information compromise and unauthorised access when devices are used include password protection, encrypting information at rest and remote wiping capabilities.

121. Where devices cannot be protected by these means, the Department of Home Affairs recommends entities apply the protections used for physical information (see C.5.6.1 Transferring physical security classified information).

122. Where a device is being used to transfer security classified information to another entity—ie the device will be retained by the receiving entity—it may be appropriate for entities to consider additional controls such as receipts (see C.5.2.3 Keeping records of disclosure and access). For guidance on protecting information on ICT systems, see PSPF policy 11: Robust ICT systems.

C.5.6.3 Transferring security classified information outside Australia

123. Special care is necessary when transferring security classified information (physical or held on a storage device) outside Australia.

124. **Annexes A to C** establish the minimum protections for transferring security classified information outside Australia, including outlining information that may not be transferred outside Australia.

125. The Department of Home Affairs recommends entities:

    a. consider country-specific advice

    b. check with the DFAT about the most appropriate method to transfer security classified information outside Australia

    c. establish entity procedures if overseas transfers form a routine part of their business.

C.5.6.4 Electronically transmitting security classified information

126. Entities electronically transmit information when it is sent or communicated over the internet, through a secure network infrastructure (ie OFFICIAL: Sensitive, PROTECTED, SECRET or TOP SECRET networks) or over public network infrastructure and unsecured spaces. Examples of electronical transmission include using email, facsimile, instant messaging services, GovTEAMS, telephone and videoconference.

127. Information is at increased risk when electronically transmitted, particularly when information is transmitted outside of a controlled environment (eg when an entity does not have control over the entire transmission network).

128. Encryption can be used to assist in protecting information from compromise where insufficient physical security is provided for the protection of information communicated over network infrastructure.

129. Where the electronic transmission involves verbal communication (such as telephone or videoconference), the Department of Home Affairs' recommendations for maintaining good security practices when using classified information are relevant (C.5.3 Using security classified information).

130. **Table 6** outlines the minimum protections to deter and detect compromise when transmitting information electronically. For detailed guidance on protecting transmissions over networks, including information on cryptography, see the Australian Government Information Security Manual.

Table 6 Minimum network and encryption levels for transmitting information electronically

Classification/marking	Minimum protections
TOP SECRET **(and SECRET Codeword)**	a. Communicate information over TOP SECRET secure network. b. Use ASD's High Assurance Cryptographic Equipment to encrypt TOP SECRET information for any communication that is not over a TOP SECRET network.
SECRET	a. Communicate information over SECRET secure networks (or networks of higher classification).

Classification/marking	Minimum protections
	b. Use ASD's High Assurance Cryptographic Equipment to encrypt SECRET information for any communication that is not over a SECRET network or network of higher classification.
PROTECTED	a. Communicate information over PROTECTED networks (or networks of higher classification). b. Encrypt PROTECTED information for any communication that is not over a PROTECTED network or network of higher classification.
OFFICIAL: Sensitive	Communicate information over OFFICIAL: Sensitive networks (or networks of higher classification). Encrypt OFFICIAL: Sensitive information transferred over public network infrastructure, or through unsecured spaces (including Zone 1 security areas), unless the residual security risk of not doing so has been recognised and accepted by the entity. An entity may wish to consider other security measures or mitigating protections already in place, such as: a. validating the recipient's address before sending information in an unencrypted form b. sending sensitive information or large amounts of non-sensitive information as an encrypted or password protected attachment. Australian Privacy Principle 11 imposes additional obligations regarding the transmission of 'personal information' (as defined under the *Privacy Act*); the Office of the Australian Information Commissioner's Guide to Securing Personal Information provides guidance on the reasonable steps that entities may be required to take under the Privacy Act to protect the personal information they hold, including when such information is being transferred or transmitted.
OFFICIAL	a. Communicate information over public network infrastructure or through unsecured spaces (including Zone 1 security areas). b. Encryption recommended.

131. While encryption of OFFICIAL information (as opposed to OFFICIAL: Sensitive information) is not a mandated requirement, entities are required to implement operational controls for all information holdings proportional to their value, importance and sensitivity. The Department of Home Affairs recommends entities ensure that OFFICIAL information is transmitted by electronic means which deter and detect compromise, including use of encryption to assist in protecting OFFICIAL information.

C.5.7 Disposing of security classified information

132. Not all information and records are kept forever. Information is managed for as long as it has business value; some information will have long-term historical and social value. **Requirement 8** mandates that entities dispose of security classified information in a secure manner. The careless disposal of security classified information is a serious source of leakage of information and can undermine public confidence in the Australian Government.

133. The National Archives of Australia's Information Management Standard Principle 6 states:

> *Keep business information for as long as required after which time it should be accountably destroyed or transferred.*
>
> *Assess business information against current records authorities to determine which information can be destroyed or transferred.*
>
> *Confirm that there is no need to keep business information beyond the authorised retention period. Examples of needs to keep business information longer include:*
>
> - *anticipated requests for access*
> - *likely legal action*
> - *a significant increase in public interest in the topic*
> - *a disposal freeze issued by the Archives for business information on that issue or event.*

134. Under the Archives Act information disposal includes:

a. its destruction

b. the transfer of its custody or ownership, or

c. damage or alteration.

135. Section 26 of the Archives Act prohibits altering records that are over 15 years old without authorisation from the National Archives.

136. Information disposal includes the: physical destruction of paper records; destruction of electronic records including deleting emails, documents or other data from business systems; transfer of records to another entity as the result of machinery of government changes; and transfer to the National Archives of Australia.

137. Under Section 24 of the Archives Act information disposal can only take place when it is:

   a. approved by the National Archives of Australia

   b. required by another law, or

   c. part of normal administrative practices that the National Archives of Australia does not disapprove.

138. For guidance, see the National Archives of Australia website, Dispose of information.

C.5.7.1 Destroying security classified information

139. A variety of methods can be used for the secure destruction of information in physical form.

140. ASIO-T4 approves specifications for equipment used to destroy physical security classified information. Commonly used destruction methods include:

   a. pulping

   b. burning

   c. pulverising using hammermills

   d. disintegrating by cutting and reducing the waste particle size

   e. shredding using crosscut shredders (strip shredders are not approved for destruction of security classified information).

141. The Australian Government Information Security Manual provides guidance on sanitisation and destruction of ICT equipment and storage media. Methods for destroying digital information include:

   a. digital file shredding

   b. degaussing by demagnetising magnetic media to erase recorded data

   c. physical destruction of storage media through pulverisation, incineration or shredding

   d. reformatting, if it can be guaranteed that the process cannot be reversed.

142. Commercial providers may be used to destroy security classified information. The Department of Home Affairs recommends that entities review the appropriateness of a commercial provider's collection process, transport, facility, procedures and approved equipment when considering external destruction services. These considerations can be made against ASIO-T4 Criteria – agency-assessed and approved destruction service (available on a need-to-know basis on GovTEAMS). Appropriate procedures include ensuring:

   a. security classified information is attended at all times and the vehicle and storage areas are appropriately secured

   b. that destruction is performed immediately after the material has arrived at the premises

   c. that destruction of security classified information is witnessed by an entity representative

   d. destruction service staff have a security clearance to the highest level of security classified information being transported and destroyed, or appropriately security cleared entity staff escort and witness the destruction.

143. A number of commercial providers hold National Association for Information Destruction AAA certification for destruction service (with endorsements as specified in PSC 167 External destruction of security classified information – available on a need-to-know basis on GovTEAMS). These commercial providers are able to destroy security classified information.

144. The Department of Home Affairs recommends information classified TOP SECRET or accountable material be destroyed within entity premises; the originating entity may request notification of destruction. The originator of some accountable material may apply special handling conditions that prevent information destruction being contracted out.

145. While Error! Reference source not found.8 mandates that security classified information is disposed of securely, this policy does not impose security requirements for how destruction of OFFICIAL information is to occur. The Department of Home Affairs recommends entities establish procedures for the secure disposal of OFFICIAL information.

146. There may be other legislative requirements that apply to the disposal of information. For example, Australian Privacy Principle 11.2 imposes obligations on the destruction and de-identification of personal information under the Privacy Act.

C.6 What to do in the case of an emergency, breach or security violation involving classified information

147. Exceptional situations or emergencies may arise that prevent application of this policy. The PSPF policy 5: Reporting on security requires entities to report details about exceptional circumstances that affect an entities ability to fully implement this policy and indicate the measures taken to mitigate or otherwise manage identified security risks. The PSPF policy 5: Reporting on security also mandates that affected entities are advised of any unmitigated security risks.

148. Any compromise of classified information is considered a security incident. The PSPF policy 2: Management structures and responsibilities requires entities to investigate, respond to and report on security incidents.

149. In line with this, the Department of Home Affairs recommends entities report:

a. any compromise of security classified information to the information's originator as soon as practicable

b. matters relating to national security (such as compromise of SECRET or TOP SECRET information) to the Director-General, Australian Security Intelligence Organisation.

C.7 Security classified discussions

150. **Requirement 9** mandates that the discussions involving security classified information are only held in locations as set out in **Annex D**.

151. The Department of Home Affairs recommends that mobile devices are not taken into meetings or discussions of a higher classification unless the mobile device is protected by visual and audio suppression container.

152. For information on measures for the protection of security classified discussions, including audio security, see PSPF policy 15: Physical security for entity resources.

D. Find out more

153. Other legislation and policies that may be relevant to the handling of official government information include the:

a. *Archives Act 1983* and supporting Commonwealth records management policies such as:

i. National Archives of Australia Information Management Standard

i. National Archives of Australia Digital Continuity 2020 policy

b. Australian Government Information Security Manual

c. *Privacy Act 1988* and the Office of the Australian Information Commissioner Guides and APP guidelines.

D.1 Change log

Table 6 Amendments in this policy

Version	Date	Section	Amendment
V2018.0	Sep 2018	Throughout	Not applicable. This is the first issue of this policy.

Version	Date	Section	Amendment
V2018.1	Oct 2018	Table 11, Annex A and Annex B	Table 11 – minor amendments to align with Security Caveat guidelines Annex A – clarification of classifications replaced on 1 October 2018 and ceasing on 1 October 2020. Annex B – added final Email Protective Marking Standard. This is the first version of the standard under the new PSPF. This version aligns with 2018 PSPF classification reforms agreed by the Government Security Committee (GSC) in December 2017 for commencement from 1 October 2018 (with entity transition through to October 2020): a. Rename UNCLASSIFIED to OFFICIAL b. Consolidate DLMs to a single security marking, OFFICIAL: Sensitive c. Remove CONFIDENTIAL classification d. Add CABINET special handling caveat e. Introduce link to information management markers metadata. This version also aligns to caveat reforms, as agreed by the GSC's National Intelligence and Security Subcommittee in March 2018: a. Remove EO caveat b. Include Foreign Government markings in caveat hierarchy.
V2018.2	Nov 2018	C.3.1, Table 7, Table 11, Annex A Table 2, Annex B Email protective marking standard, and Supporting resources	C.3.1—Guidance on email marking protective markings is now an Annex to this policy. Table 7—updated references to protection requirements when taking security classified documents out of the office; when transferred between physical establishments in Australia and outside of Australia. Table 11—Updates to Special handling instructions; and Releasability caveats. Table 2 Annex B—Updates to How to transmit or transfer CONFIDENTIAL classified information or remove it from and entity facility. Annex B Email protective email marking standard
V2018.3	November 2019	Policy rewrite	Policy reviewed and updated to clarify the core and supporting requirements. Updates focused on the use and storage of classified information, particularly when outside the office. For more information on the changes see the Summary of changes to PSPF policy 8.
V2018.4	September 2020	Supporting requirement 6, sections C.3 and C.5.1.3, Figure 1 and Annex G.	Requirement 6 and corresponding guidance (C.3 and C.5.1.3) —amended to accommodate new NATIONAL CABINET caveat approved by GSC on 18 August 2020. This caveat, unlike other security caveats, can be applied with OFFICIAL: Sensitive and above. Figure 1—amended to include NATIONAL CABINET caveat in hierarchy. Annex G, Email Protective Marking Standard—changes to accommodate NATIONAL CABINET caveat and GSC approved changes to the REL (Releasable To) caveat to align handling requirements with other releasability caveats.
V2018.5	October 2021	Tables 3 and 4, section C.5.1.1	Table 3 – AGAO caveat – replaced specific entities with 'National Intelligence Community' members and Department of Defence. Table 4 – warning notice to accompany Legislative Secrecy IMM C.5.1.1 – aligned hierarchy with Australian Government Security Caveat Guidelines.
V2018.6	February 2022	Annexes H and I	Annex H – two new case studies. Annex I – enhanced guidance on classifying aggregated or integrated data.
V2018.7	November 2022	Supporting requirements, sections C.1.1, C2.1, C.5.3.2, and Annexes	Requirement 7 and Annexes A-C – physical information and mobile devices. Requirement 8 (moved from Requirement 9). Requirement 9 and Annex D – security classified discussions. Guidance on 'originator', information designated for public release and types of mobile devices
V2018.8	August 2023	Throughout	Change OFFICIAL: Sensitive from DLM to security classification. Policy renamed to PSPF policy 8: Classification system

Annex A. Minimum protections and handling requirements for physical information[1]

	TOP SECRET	SECRET	PROTECTED	OFFICIAL: SENSITIVE	OFFICIAL
INSIDE ENTITY FACILITIES					
Text-based marking	Documents (including emails): Yes Recommended application: • Centre top and centre bottom of each page. • Capitals, bold text, large fonts, and distinctive colour (red preferred).	Documents (including emails): Yes Recommended application: • Centre top and centre bottom of each page. • Capitals, bold text, large fonts and distinctive colour (red preferred).	Documents (including emails): Yes Recommended application: • Centre top and centre bottom of each page. • Capitals, bold text, large fonts and distinctive colour (red preferred).	Documents (including emails): Yes Recommended application: • Centre top and centre bottom of each page. • Capitals, bold text, large fonts and distinctive colour (red preferred).	Documents (including emails): Optional Recommended application: • Centre top and centre bottom of each page. • Capitals, bold text, large fonts and distinctive colour (red preferred).
Alternative marking	Colour-based marking (red preferred) or apply entity's marking scheme.	Colour-based marking (salmon pink preferred) or apply entity's marking scheme.	Colour-based marking (blue preferred) or apply entity's marking scheme.	Colour-based marking (yellow preferred) or apply entity's marking scheme.	Colour-based marking (grey preferred) or apply entity's marking scheme.
Paragraph marking[2]	(TOP SECRET) or abbreviated to (TS).	(SECRET) or abbreviated to (S)	(PROTECTED) or abbreviated to (P).	(OFFICIAL: Sensitive) or abbreviated to (O:S).	(OFFICIAL) or abbreviated to (O).
Access control	Need-to-know principle: Yes Security clearance: NV2 (minimum) Temporary access: NV1 (minimum), supervised[3]	Need-to-know principle: Yes Security clearance: NV1 (minimum) Temporary access: Supervised[3]	Need-to-know principle: Yes Security clearance: Baseline (minimum) Temporary access: Supervised[3]	Need-to-know principle: Yes Security clearance: Nil, employment screening only for entity personnel.	Need-to-know principle: Recommended Security clearance: Nil, employment screening only for entity personnel. *Access controls N/A if information approved for public release*
Use – Zone 1	No	No	Yes	Yes	Yes
Use – Zone 2	No	No	Yes	Yes	Yes
Use – Zone 3	Yes	Yes	Yes	Yes	Yes
Use – Zone 4	Yes	Yes	Yes	Yes	Yes
Use – Zone 5	Yes	Yes	Yes	Yes	Yes
Leave unattended	No, store securely when unattended.	No, store securely when unattended.	Yes, apply entity procedures	Yes, apply entity procedures	Yes
Store – Zone 1	No	No	No	Yes, lockable container	Yes, subject to entity procedures
Store – Zone 2	No	No	Yes, Class C container	Yes, lockable container	Yes, subject to entity procedures
Store – Zone 3	No. Exceptional circumstances[4] – Class A container, max 5 days	Yes, Class B container	Yes, lockable container	Yes, lockable container	Yes
Store – Zone 4	Yes, Class B container, max 5 days	Yes, Class C container	Yes, lockable container	Yes, subject to entity procedures. Lockable container recommended.	Yes
Store – Zone 5	Class B container	Yes, Class C container	Yes, lockable container	Yes, subject to entity procedures. Lockable container recommended.	Yes
Carry – Zone 1	Not recommended. If required, opaque envelope/folder that indicates Classification and place in security briefcase, pouch or satchel	Yes, in opaque envelope/folder that indicates Classification place in security briefcase, pouch or satchel	Yes, in opaque envelope/folder	Yes, opaque envelope/folder recommended.	Yes, apply entity procedures.
Carry – Zone 2	Not recommended. If required, opaque envelope/folder that indicates Classification and place in security briefcase, pouch or satchel	Yes, in opaque envelope/folder that indicates Classification	Yes, in opaque envelope/folder	Yes, opaque envelope/folder recommended.	Yes, apply entity procedures.
Carry – Zone 3	Yes, in opaque envelope/folder that indicates Classification	Yes, in opaque envelope/folder that indicates Classification	Yes, in opaque envelope/folder	Yes, opaque envelope/folder recommended.	Yes, apply entity procedures.
Carry – Zone 4	Yes, in opaque envelope/folder that indicates Classification	Yes, opaque envelope/folder recommended	Yes, in opaque envelope/folder recommended	Yes, opaque envelope/folder recommended.	Yes, apply entity procedures.
Carry – Zone 5	Yes, in opaque envelope/folder that indicates Classification	Yes, opaque envelope/folder recommended	Yes, in opaque envelope/folder recommended	Yes, opaque envelope/folder recommended.	Yes, apply entity procedures.
Transfer - inside	Yes, transfer by hand or entity safe hand and apply 'carry' requirements. Can be uncovered if in close proximity and office environment presents low risk of unauthorised viewing. Written manager approval required for transfer in Zones 1-2. All transfers require a receipt.	Yes, transfer by hand or entity safe hand and apply 'carry' requirements. Can be uncovered if in close proximity and office environment presents low risk of unauthorised viewing. All transfers require a receipt.	Yes, transfer by hand or entity safe hand and apply 'carry' requirements. Can be uncovered if in close proximity and the office environment presents low risk of unauthorised viewing. All transfers require a receipt.	Yes, place in opaque envelope/folder and apply entity procedures to transfer by hand or internal mail.	Yes, apply entity procedures for transfer by hand or internal mail.
Dispose[5]	Class A shredder, supervise and document.	Class A shredder	Class B shredder	Apply entity procedures for disposal	Apply entity procedures for disposal
OUTSIDE ENTITY FACILITIES (including for home-based work)					
Use – outside	No, do not use outside entity facilities.	No, do not use outside entity facilities	Not recommended. If required, apply entity procedures and exercise judgement to assess environmental risk.	Yes, apply entity procedures and exercise judgement to assess environmental risk	Yes

[1] Additional restrictions may apply for caveated information, refer to the Australian Government security caveat guidelines for minimum handling and protections for caveated information including codeword.

[2] Refer to paragraph grading indicators in section C.5.1.1 Applying text-based protective markings.

[3] Refer to PSPF policy 9: Access to information for information on granting temporary access to security classified information.

[4] Refer to PSPF policy 1: Role of accountable authority for information on exceptional circumstances.

[5] Ensure information is destroyed when it has passed minimum retention requirements or reaches authorised destruction dates. See Section C.5.7 for further information on disposing of security classified information.

[6] Outside entity facilities includes all public spaces such as cafes, public and private transport, airport transit lounges and non-government offices, including private sector offices.

	TOP SECRET	SECRET	PROTECTED	OFFICIAL: SENSITIVE	OFFICIAL
Use – at home	No, do no use at home.	No, do not use for regular home-based work. Occasional: No, but if unavoidable, obtain manager approval and exercise judgement to assess environmental risk.	Regular: Yes, apply entity procedures, which must include a security risk assessment of the proposed work environment. Occasional: Yes, apply entity procedures on need for security risk assessment and exercise judgement to assess environmental risk.	Yes, apply entity procedures on need for a security risk assessment and exercise judgement to assess environmental risk	Yes
Leave unattended	No.	No. If occasional home-based work approved, for brief absences, store in Class B (or higher) container that has been approved by the Accountable Authority or their delegate.	No, store security when unattended. For brief absences from home, apply entity procedures and exercise judgement to assess environmental risk.	Yes, can be left unattended for short periods subject to entity procedures and judgement to assess environmental risk.	Yes
Store – outside	No, do not store outside entity facilities.	No. For brief absence from home, see 'leave unattended'.	Not recommended. If required, store in Class C (or higher) container. For brief absence from home, see 'leave unattended'.	Yes, opaque envelope/folder in lockable container recommended.	Yes, lockable container recommended.
Store – at home	No, do not store at home.	No. If unavoidable, refer to 'carry' outside entity requirement, retain in personal custody (strongly preferred), and return to entity facilities as soon as practicable.	Regular: Class C (or higher) container. Occasional: apply 'carry' outside entity requirements to store in security briefcase, pouch or satchel, with tamper-evident packaging recommended.	Yes, opaque envelope/folder recommended, and subject to environmental risk, store in lockable container.	Yes
Carry – outside	Not recommended. If required, obtain written manager approval and place in tamper-evident packaging within security briefcase, pouch or satchel and retain in personal custody.	Yes, place in security briefcase, pouch or satchel and always retain in personal custody. Tamper-evident packaging recommended.	Yes, place in security briefcase, pouch or satchel. Tamper-evident packaging recommended if aggregate information increases risk.	Yes, recommend carry is opaque envelope/folder.	Yes, apply entity procedures
Transfer – outside[7]	Yes, written manager approval, apply 'carry' outside entity requirements and transfer by entity safe hand; or place in tamper-evident packaging and transfer by safe hand courier rated BIL 5 or DFAT courier. All transfers require a receipt.	Yes, apply 'carry' outside entity requirements and transfer by hand, entity safe hand, safe hand courier rated BIL 4 or DFAT courier. If transfer by courier, use tamper evident packaging. All transfers require a receipt.	Yes, apply 'carry' outside entity requirements and transfer by hand, entity safe hand, safe hand courier rated BIL 4 or DFAT courier. If transfer by courier, use tamper evident packaging. All transfers require a receipt.	Yes, place in opaque envelope/folder and apply entity procedures to minimise risk of unauthorised access (eg sealed envelope). Transfer by hand, mail or courier and exercise judgement to assess whether registered or other secure mail appropriate.	Yes, apply entity procedures for transfer by hand, external mail or courier.
TRAVEL IN AUSTRALIA					
Travel	Not recommended. If required, written manager approval, apply 'carry' outside entity requirements and any additional entity travel procedures. Do not 'use' until in appropriate Zone at destination.	Not recommended. If required, apply 'carry' outside entity requirements and any additional entity travel procedures. Do not 'use' until in appropriate Zone at destination.	Yes, apply 'carry' outside entity requirements and any additional entity travel procedures.	Yes, apply 'carry' outside entity requirements, any additional entity travel procedures and exercise judgement to assess environmental risk.	Yes, apply entity procedures and exercise judgement to assess environmental risk
Air travel luggage	Not recommended. If unavoidable, retain in personal custody as carry-on luggage. If airline requires carry-on baggage to be checked at the gate, **do not travel.**	Not recommended. If unavoidable, retain as carry-on luggage. If airline requires baggage to be checked at the gate, place in tamper-evident packaging within a security briefcase, pouch or satchel, try to observe entering and exiting the cargo hold and reclaim as soon as possible. If tamper-evident packaging not available, **do not travel.**	Yes, retain as carry-on luggage. If airline requires carry-on luggage to be checked at the gate, try to observe entering/existing the cargo hold and reclaim as soon as possible.	Yes, apply entity procedures.	Yes
Leave unattended	No, do not leave unattended, retain in custody.	No, do not leave unattended.	Not recommended. For brief absences from hotel room, apply entity procedures and exercise judgement to assess environmental risk.	Yes, apply entity procedures and exercise judgement to assess environmental risk.	Yes, subject to entity procedures.
Store while travel	No, do not store, retain in custody.	No, do not store while travelling (eg in hotel room). If required, can be stored in Australian entity facility meeting 'store' inside entity requirements.	No, do not store will travelling. If required, can be stored in Australian entity facility meeting 'store' inside entity requirements. For brief absence from hotel room, see 'leave unattended'.	Yes, apply 'store' outside entity requirements.	Yes, lockable container recommended.
TRAVEL OUTSIDE AUSTRALIA					
Travel	No, do not travel with TS information. Seek DFAT advice on options to access information at overseas destination or see 'transfer' outside entity requirements.	Not recommended. Seek DFAT advice on options to access information at overseas destination. If required, apply 'carry' outside entity requirements and any additional entity travel procedures, and consider country-specific travel advice. Do not 'use' until in appropriate Zone at destination.	Not recommended. Seek DFAT advice on options to access information at overseas destination. If required, apply 'carry' outside entity requirements and any additional entity travel procedures, and consider country-specific travel advice. Do not 'use' until in appropriate Zone at destination.	Yes, apply 'carry' outside entity requirements, any additional entity travel procedures, and consider country-specific travel advice.	Yes, apply entity procedures
Air travel luggage	No, do not travel with TS information.	Not recommended. If required, retain as carry-on luggage. If airline requires carry-on baggage to be checked at the gate, **do not travel**.	Not recommended. If required, retain as carry-on luggage. If airline requires carry-on baggage to be checked at the gate, **do not travel**.	Yes, apply 'carry' outside entity requirements, any additional entity procedures and exercise judgement to assess environmental risk.	Yes
Leave unattended	No, do not travel with TS information.	No, do not leave unattended.	No, do not leave unattended.	Yes, apply entity procedures, exercise judgement to assess environmental risk.	Yes, subject to entity procedures.
Store while travel	No, do not travel with TS information.	No, do not store while travelling (eg in hotel room). If required, can be stored in Australian entity facility meeting 'store' inside entity requirements.	No, do not store while travelling (eg in hotel room). If required, can be stored in Australian entity facility meeting 'store' inside entity requirements.	Yes, apply 'store' outside entity requirements and consider country-specific travel advice.	Yes, lockable container recommended.

[7] Transfer outside includes transfer to an officer in a different government facility or entity.

Annex B. Minimum protections and handling requirements for government-issued mobile devices

A **government-issued mobile device** is a mobile or portable computing communications device that is owned and issued by an Australian Government entity to access the entity's systems and data and is approved by the relevant authority[8] to process, store or communicate entity information of a specified security classification. This includes mobile phones, handheld computers, tablets, laptops and personal digital assistants configured, encrypted and managed to ASD standards and guidance. If these requirements are met, then a government-issued mobile device is considered in a 'secured state'. If these requirements are not met, refer to **Annex C** for 'unsecured state' requirements.

	TOP SECRET[8]	SECRET[8]	PROTECTED	OFFICIAL: SENSITIVE	OFFICIAL
INSIDE ENTITY FACILITIES					
Access control	Need-to-know principle: Yes Security clearance: NV2 (minimum)	Need-to-know principle: Yes Security clearance: NV1 (minimum)	Need-to-know principle: Yes Security clearance: Baseline (minimum)	Need-to-know principle: Yes Security clearance: Nil, employment screening only	Need-to-know principle: Recommended Security clearance: Nil, employment screening only
Use – Zone 1	No	No	Yes	Yes	Yes
Use – Zone 2	No	No (unless exceptional circumstances)	Yes	Yes	Yes
Use – Zone 3	Yes, subject to ASD approval and conditions for use[8] and entity CSO approval.	Yes, subject to ASD approval and conditions for use[8]. If TS information/device present, also subject to risk assessment and entity CSO approval.	Yes, but if TS or SECRET information/device present, subject to risk assessment and entity CSO approval	Yes, but if TS or SECRET information/device present, subject to risk assessment and entity CSO approval	Yes, but if TS or SECRET information/device present, subject to risk assessment and entity CSO approval
Use – Zone 4	Yes, subject to ASD approval and conditions for use [8] and entity CSO approval.	Yes, subject to entity CSO approval.	Yes, but if TS or SECRET information/device present, subject to risk assessment and entity CSO approval	Yes, but if TS or SECRET information/device present, subject to risk assessment and entity CSO approval.	Yes, but if TS or SECRET information/device present, subject to risk assessment and entity CSO approval.
Use – Zone 5	Yes, subject to ASD approval and conditions for use [8] and entity CSO approval.	No, unless ASD approve during Zone 5 certification and subject to ASD conditions for use.	No, unless ASD approve during Zone 5 certification and subject to ASD conditions for use.	No, unless ASD approve during Zone 5 certification and subject to ASD conditions for use.	No, unless ASD approve during Zone 5 certification and subject to ASD conditions for use.
Leave unattended	No, store securely when not in use.	No, store securely when not in use.	Yes, if locked or turned off	Yes, if locked or turned off	Yes
Store – Zone 1	No	No	Yes, Class C container	Yes, lockable container recommended	Yes, lockable container recommended
Store – Zone 2	No	No. Exceptional circumstances, store turned off in Class B container	Yes, lockable container recommended	Yes, lockable container recommended	Yes, locked or turned off recommended
Store – Zone 3	No. Exceptional circumstances – store turned off in Class A container, max 5 days	Yes, store turned off in Class C container	Yes, lockable container recommended	Yes, lockable container recommended	Yes, locked or turned off recommended
Store – Zone 4	No. Exceptional circumstances – store turned off in Class B container, max 5 days.	Yes, store turned off in Class C container. Store away from irregular TOP SECRET discussions.	Yes, locked or turned off when not in use.	Yes, locked or turned off recommended.	Yes, locked or turned off recommended.
Store – Zone 5	Yes, stored turned off in Class B container	Yes, store turned off in Class C container	Yes if approved by ASD during Zone 5 certification. Store turned off and away from TOP SECRET or SECRET discussions.	Yes if approved by ASD during Zone 5 certification. Store turned off and away from TOP SECRET or SECRET discussions.	Yes if approved by ASD during Zone 5 certification. Store turned off and away from TOP SECRET or SECRET discussions.
Carry – inside entity	Yes, if locked or turned off and apply entity procedures and relevant Zone procedures.	Yes, if locked or turned off and apply entity procedures and relevant Zone procedures	Yes, apply entity procedures and relevant Zone procedures, and carry locked or turned off recommended.	Yes, apply entity procedures and relevant Zone procedures, and carry locked or turned off recommended.	Yes, apply entity procedures and relevant Zone procedures, and carry locked or turned off recommended.
Transmit	TOP SECRET secure network, otherwise use ASD's High Assurance Cryptographic Equipment to encrypt TOP SECRET information.	SECRET (or higher) secure network, otherwise use ASD's High Assurance Cryptographic Equipment to encrypt SECRET information.	PROTECTED (or higher) network, otherwise encryption required.	OFFICIAL: Sensitive (or higher) network. Encrypt if transferred over public network infrastructure or through unsecured spaces (including Zone 1), unless residual risk of not doing so has been recognised and accepted by the CSO.	Encryption recommended, particularly for information communicated over public network infrastructure.
Dispose	Refer to Australian Government Information Security Manual – ICT equipment sanitisation and destruction				
OUTSIDE ENTITY FACILITIES (including for home-based work)[6]					
Use – outside	No, do not use outside entity facilities.	No, do not use outside entity facilities.	Yes, apply entity procedures and exercise judgement to assess environmental risk. Privacy screen recommended.	Yes, apply entity procedures and exercise judgement to assess environmental risk.	Yes
Use – at home	No, do not use at home.	Regular: No. Occasional: Not recommended, if required obtain manager approval, apply entity procedures on need for a security risk assessment and exercise judgement to assess environmental risk.	Regular: Yes, apply entity procedures, which must include a security risk assessment of the proposed work environment. Occasional: Yes, apply entity procedures on need for security risk assessment and exercise judgement to assess environmental risk.	Yes, apply entity procedures on need for security risk assessment and exercise judgement to assess environmental risk.	Yes
Leave unattended	No, store securely when not in use	No, store securely when unattended. For brief absences from home, exercise judgement to store in a Class C (or higher) container that has been approved as a proper place of custody by the Accountable Authority or their delegate.	Yes, if in secured state and locked or turned off, subject to entity procedures.		Yes, locked or turned off recommended
Store – outside	No, do not store outside entity facilities.	No, do not store outside entity facilities.	Yes, lockable container recommended	Yes, lockable container recommended	Yes, lockable container recommended
Store – at home	No do not store at home.	Regular: No.	Yes, apply entity procedures and exercise judgement to assess environmental risk.	Yes, apply entity procedures and exercise judgement to assess environmental risk.	Yes, apply entity procedures.

[8] ASD is the relevant authority for TOP SECRET and SECRET government-issued mobile devices and capabilities and may set additional restrictions or conditions for use. ASD may also approve alternative mitigation arrangements, including outside entity facilities, to support operational or ministerial briefing requirements. The entity is the relevant authority for other government-issued mobile devices.

	TOP SECRET[8]	SECRET[8]	PROTECTED	OFFICIAL: SENSITIVE	OFFICIAL
		Occasional: Not recommended. If required apply 'carry outside entity requirements and retain in personal custody. For brief absence from home, see 'leave unattended'.			
Carry – outside	Not recommended. If required, seek manager approval, and carry turned off and in tamper-evident packaging in security briefcase, pouch or satchel recommended.	Yes, if locked or turned off and apply entity procedures.	Yes, apply entity procedures	Yes, apply entity procedures	Yes, apply entity procedures
Transmit	TOP SECRET secure network, otherwise use ASD's High Assurance Cryptographic Equipment to encrypt TOP SECRET information.	SECRET secure network, otherwise use ASD's High Assurance Cryptographic Equipment to encrypt SECRET information.	PROTECTED (or higher) network, otherwise encryption required.	OFFICIAL: Sensitive (or higher) network. Encrypt if transferred over public network infrastructure or through unsecured spaces (including Zone 1), unless residual risk of not doing so has been recognised and accepted by the CSO.	Encryption recommended for information communicated over public network infrastructure.
TRAVEL IN AUSTRALIA					
Travel	Not recommended. If unavoidable, written manager approval, apply 'carry' outside entity requirements and any additional entity procedures. Do not 'use' until in appropriate Zone at destination.	Not recommended. If required, apply 'carry' outside entity requirements and any additional entity procedures. Do not 'use' until in appropriate Zone at destination.	Yes, apply 'carry' outside entity requirements and any additional entity procedures. If 'use' required while travelling, a privacy screen is recommended.	Yes, apply 'carry' outside entity requirements and any additional entity procedures, and exercise judgment to assess environmental risk.	Yes
Air travel luggage	Not recommended. If unavoidable, retain in personal custody in carry-on luggage and apply 'carry outside' requirements. If airline requires carry-on luggage to be checked-in, **do not travel.**	Not recommended. If unavoidable, retain as carry-on luggage. If airline requires baggage to be checked at the gate (eg premium luggage), place in tamper-evident packaging within a security briefcase, pouch or satchel and try to observe entering and exiting the cargo hold and reclaim as soon as possible. If tamper-evident packaging not available, **do not travel.**	Yes, retain as carry-on luggage. If airline requires carry-on luggage to be checked at the gate (eg premium luggage), try to observe entering/existing the cargo hold and reclaim as soon as possible.	Yes, retain as carry-on luggage recommended.	Yes
Leave unattended	No, do not leave unattended, retain in custody.	No, do not leave unattended, retain in custody.	Not recommended. For brief absences from hotel room, apply entity procedures and exercise judgement to assess environmental risk.	Yes, apply entity procedures and exercise judgement to assess environmental risk.	Yes, apply entity procedures and exercise judgement to assess environmental risk.
Store while travel	No, do not store while travelling, including in hotel. Storage in Australian entity facility accepted.	No, do not store while travelling (eg in hotel room). If required, can be stored in Australian entity facility meeting 'store' inside entity requirements.	Not recommended. For brief absence from hotel room, see 'leave unattended'.	Yes, apply 'store' outside entity requirements.	Yes, apply 'store' outside entity requirements.
TRAVEL OUTSIDE AUSTRALIA					
Travel	No, do not travel with mobile device. Seek DFAT advice on options to access mobile device at overseas destination.	Not recommended. Seek DFAT advice on options to access mobile device at overseas destination.	Not recommended. Seek DFAT advice on options to access mobile device at overseas destination. If required, apply 'carry' outside entity requirements and any additional entity travel procedures, and consider country-specific travel advice.	Yes, apply 'carry' outside entity requirements, any additional entity travel procedures, and consider country-specific travel advice.	Yes, apply entity procedures and exercise judgement to assess environmental risk.
Air travel luggage	No, do not travel with mobile device.	Not recommended. If required, retain as carry-on luggage. If airline requires carry-on baggage to be checked at the gate, **do not travel**.	Not recommended. If required, retain as carry-on luggage. If airline requires carry-on baggage to be checked at the gate, **do not travel**.	Yes, apply 'carry' outside entity requirements, any additional entity procedures and exercise judgement to assess environmental risk.	Yes, apply 'carry' outside entity requirements
Leave unattended	No, do not travel with mobile device.	No, do not leave unattended.	No, do not leave unattended.	Yes, apply entity procedures, exercise judgement to assess environmental risk, and consider country-specific travel advice.	Yes, apply entity procedures.
Store while travel	No, do not travel with mobile device.	No, do not store while travelling (eg in hotel room). If required, can be stored in Australian entity facility meeting 'store' inside entity requirements.	No, do not store while travelling (eg in hotel room). If required, can be stored in Australian entity facility meeting 'store' inside entity requirements.	Yes, apply 'store' outside entity requirements and consider country-specific travel advice.	Yes, apply 'store' outside entity requirements
MOBILE DEVICE PROVIDED AT OVERSEAS DESTINATION					
Use	Yes, in an appropriate Zone and apply 'use' in entity requirements.	Yes, in an appropriate Zone and apply 'use' in entity requirements	Apply 'use' in entity requirements	Apply 'use' in entity requirements	Apply 'use' in entity requirements
Store	Yes, in an appropriate Zone and apply 'store' in entity requirements	Yes, in an appropriate Zone and apply 'store' in entity requirements	Apply 'store' in entity requirements	Apply 'store' in entity requirements	Apply 'store' in entity requirements
Carry	No, if unavoidable, apply 'carry' outside entity requirements and any additional entity procedures.	No, if unavoidable, apply 'carry' outside entity requirements and any additional entity procedures.	Apply 'carry' outside entity requirements and any additional entity travel procedures.	Apply 'carry' outside entity requirements and any additional entity travel procedures.	Apply 'carry' outside entity requirements
Leave unattended	No, do not leave unattended.	No, do not leave unattended.	Retain in personal custody or store in Australian entity facility meeting 'store' inside entity requirements.	Yes, apply entity procedures, exercise judgement to assess environmental risk, and consider country-specific travel advice.	Yes, apply entity procedures.

Annex C. Minimum protections and handling requirements for non-government mobile devices

Non-government mobile devices include:

- **Authorised non-government device** – mobile or portable computing communications devices (including mobile phones, handheld computers, tablets, laptops and digital assistants) owned or issued by a non-government source (for example commercial organisation, non-government organisation, industry issued or privately-owned) that is managed, configured and encrypted in accordance with ASD standards and guidance, and the residual risk is accepted by the Commonwealth entity system risk owner to access, process, store or communicate OFFICIAL, OFFICIAL: Sensitive and PROTECTED Australian Government information or data. Non-government devices ***must not*** access, process, store or communicate SECRET or TOP SECRET information or data. If these requirements are fully met, then a non-government mobile device is considered in a 'secured state'. If these requirements are not fully met, refer to 'unsecured state' requirements.

- **All other mobile devices** – devices that are not owned, issued or authorised by the entity. These devices ***must not*** be authorised to access, process, store or communicate government OFFICIAL: Sensitive or above information, and ***must not*** enter Zones 4-5 or where SECRET or TOP SECRET information or devices are present. If use of these devices required in a Zone 3, then use is subject to risk assessment and Chief Security Officer approval.

	Authorised non-government device - approved to access, process, store or communicate government information or data					All other mobile devices
	TOP SECRET	SECRET	PROTECTED	OFFICIAL: SENSITIVE	OFFICIAL	
INSIDE ENTITY FACILITIES						
Access control	Not applicable	Not applicable	Need-to-know principle: Yes Security clearance: Baseline (minimum)	Need-to-know principle: Yes Security clearance: Nil, employment screening only	Need-to-know principle: Recommended Security clearance: Nil, employment screening only	Not applicable
Use – Zone 1	Not applicable	Not applicable	Yes, subject to entity procedures.	Yes, subject to entity procedures.	Yes, subject to entity procedures.	Yes
Use – Zone 2	Not applicable	Not applicable	Yes, subject to entity procedures.	Yes, subject to entity procedures.	Yes, subject to entity procedures.	Yes
Use – Zone 3	Not applicable	Not applicable	If TS or SECRET information/device present: No. If unavoidable, then subject to risk assessment and entity CSO approval. Otherwise, Yes.	If TS or SECRET information/device present: No. If unavoidable, then subject to risk assessment and entity CSO approval. Otherwise, Yes.	If TS or SECRET information/device present: No. If unavoidable, then subject to risk assessment and entity CSO approval. Otherwise, Yes.	If TS or SECRET information/devices present: No. If unavoidable, then subject to risk assessment and entity CSO approval. Otherwise, Yes.
Use – Zone 4	Not applicable	Not applicable	If TS or SECRET information/device present: No. If unavoidable, then subject to risk assessment and entity CSO approval. Otherwise, Yes.	If TS or SECRET information/device present: No. If unavoidable, then subject to risk assessment and entity CSO approval. Otherwise, Yes.	If TS or SECRET information/device present: No. If unavoidable, then subject to risk assessment and entity CSO approval. Otherwise, Yes.	No, not permitted in Zone 4
Use – Zone 5	Not applicable	Not applicable	No, unless ASD approved (and subject to ASD conditions of use) during Zone 5 certification and entity CSO approval.	No, unless ASD approved (and subject to ASD conditions of use) during Zone 5 certification and entity CSO approval.	No, unless ASD approved (and subject to ASD conditions of use) during Zone 5 certification and entity CSO approval.	No, not permitted in Zone 5.
Leave unattended	Not applicable	Not applicable	Yes, subject to entity procedures and locked or turned off.	Yes, subject to entity procedures.	Yes, subject to entity procedures.	Not applicable
Store – Zone 1	Not applicable	Not applicable	No, store in higher zone.	Secured: lockable container recommended Unsecured: lockable cabinet	Yes	Yes, subject to entity procedures.
Store – Zone 2	Not applicable	Not applicable	Class C container	Secured: lockable container recommended Unsecured: lockable cabinet	Yes	Yes, subject to entity procedures.
Store – Zone 3	Not applicable	Not applicable	If TS or SECRET information/device present: No. Otherwise, Yes in Class C container.	If TS or SECRET information/device present: No. Otherwise, Yes, and: Secured: lockable container recommended Unsecured: lockable cabinet	If TS or SECRET information/device present: No. Otherwise, Yes.	If TS or SECRET information/devices present: No. Otherwise, Yes.
Store – Zone 4	Not applicable	Not applicable	If TS or SECRET information/devices present: No. Otherwise, Yes, locked or turned off when not in use, and: Secured: lockable container recommended Unsecured: No.	If TS or SECRET information/device present: No. Otherwise, Yes, locked or turned off recommended, and: Secured: lockable container recommended Unsecured: lockable cabinet	If TS or SECRET information/device present: No. Otherwise, Yes, locked or turned off recommended, and: Secured: lockable container recommended Unsecured: lockable cabinet	No, not permitted in Zone 4.
Store – Zone 5	Not applicable	Not applicable	No, unless ASD approved during Zone 5 certification and entity CSO approval.	No, unless ASD approved during Zone 5 certification and entity CSO approval.	No, unless ASD approved during Zone 5 certification and entity CSO approval.	No, not permitted in Zone 5.
Carry – Zones 1-2	Not applicable	Not applicable	Secured: Yes Unsecured: Yes, apply entity procedures	Secured: Yes Unsecured: Yes, apply entity procedures	Secured: Yes Unsecured: Yes, apply entity procedures	Yes, subject to entity procedures.
Carry – Zone 3	Not applicable	Not applicable	If TS or SECRET information/device present: No. Otherwise: Yes. If unsecured, apply entity procedures.	If TS or SECRET information/device present: No. Otherwise: Yes. If unsecured, apply entity procedures.	If TS or SECRET information/device present: No. Otherwise: Yes. If unsecured, apply entity procedures.	If TS or SECRET information/devices present: No. Otherwise: Yes, subject to entity procedures.
Carry – Zone 4	Not applicable	Not applicable	If TS or SECRET information/device present: No. Otherwise: Yes. If unsecured, apply entity procedures.	If TS or SECRET information/device present: No. Otherwise: Yes. If unsecured, apply entity procedures.	If TS or SECRET information/device present: No. Otherwise: Yes. If unsecured, apply entity procedures.	No, not permitted in Zone 4.
Carry – Zone 5	Not applicable	Not applicable	No	No	No	No, not permitted in Zone 5.
Transmit	Not applicable	Not applicable	PROTECTED (or higher) network, otherwise encryption required.	OFFICIAL: Sensitive (or higher) network. Encrypt if transferred over public network infrastructure or through unsecured spaces (including Zone 1), unless residual risk of not	Encryption recommended for information communicated over public network infrastructure.	Not applicable

	Authorised non-government device - approved to access, process, store or communicate government information or data					All other mobile devices
	TOP SECRET	SECRET	PROTECTED	OFFICIAL: SENSITIVE	OFFICIAL	
				doing so has been recognised and accepted by the CSO.		
Dispose	Not applicable	Not applicable	Refer to Australian Government Information Security Manual – ICT equipment sanitisation and destruction			Not applicable
OUTSIDE ENTITY FACILITIES (including for home-based work) [6]						
Use – outside entity	Not applicable	Not applicable	Yes, apply entity procedures and exercise judgement to assess environmental risk.	Yes, apply entity procedures and exercise judgement to assess environmental risk.	Yes	Not applicable
Use – at home	Not applicable	Not applicable	Regular: Yes, apply entity procedures, which must include a security risk assessment of the proposed work environment. Occasional: Yes, apply entity procedures on need for security risk assessment and exercise judgement to assess environmental risk.	Yes, apply entity procedures on need for security risk assessment and exercise judgement to assess environmental risk.	Yes	Not applicable
Leave unattended	Not applicable	Not applicable	Yes, if in secured state, locked or turned off, apply entity procedures and exercise judgement to assess environmental risk.	Secured: Yes Unsecured: follow 'store' outside entity requirements.	Yes, locked or turned off recommended	Not applicable
Store – outside entity	Not applicable	Not applicable	Secured: Yes, lockable container recommended Unsecured: Class C (or higher) container	Secured: Yes Unsecured: Yes, lockable container	Yes, lockable container recommended	Not applicable
Store – at home	Not applicable	Not applicable	Yes, apply entity procedures and exercise judgement to assess environmental risk.	Apply entity procedures and exercise judgement to assess environmental risk.	Yes, apply entity procedures.	Not applicable
Carry outside entity	Not applicable	Not applicable	Secured: Yes Unsecured: Yes, inside a security briefcase, pouch or satchel and consider tamper-evident packaging	Secured: Yes Unsecured: Yes, apply entity procedures	Yes, apply entity procedures	Not applicable
TRAVEL IN AUSTRALIA						
Travel	Not applicable	Not applicable	Yes, apply 'carry' outside entity requirements and any additional entity procedures.	Yes, apply 'carry' outside entity requirements and any additional entity travel procedures, and exercise judgment to assess environmental risk.	Yes	Not applicable
Air travel luggage	Not applicable	Not applicable	Yes, retain as carry-on luggage. If airline requires carry-on luggage to be checked at the gate, try to observe entering/existing the cargo hold and reclaim as soon as possible.	Yes, retain as carry-on luggage recommended.	Yes	Not applicable
Leave unattended	Not applicable	Not applicable	Not recommended. For brief absences from hotel room, apply entity procedures and exercise judgement to assess environmental risk.	Yes, apply entity procedures and exercise judgement to assess environmental risk.	Yes, apply entity procedures and exercise judgement to assess environmental risk.	Not applicable
Store while travel	Not applicable	Not applicable	Not recommended. For brief absence from hotel room, see 'leave unattended'.	Yes, apply 'store' outside entity requirements.	Yes, apply 'store' outside entity requirements.	Not applicable
TRAVEL OUTSIDE AUSTRALIA						
Travel	Not applicable	Not applicable	Not recommended. Seek DFAT advice on options to access mobile device at overseas destination. If required, apply 'carry' outside entity requirements and any additional entity travel procedures, and consider country-specific travel advice.	Yes, apply 'carry' outside entity requirements, any additional entity travel procedures, and consider country-specific travel advice.	Yes, apply entity procedures and exercise judgement to assess environmental risk.	Not applicable
Air travel luggage	Not applicable	Not applicable	Not recommended. If required, retain as carry-on luggage. If airline requires carry-on baggage to be checked at the gate, **do not travel**.	Yes, apply 'carry' outside entity requirements, any additional entity procedures and exercise judgement to assess environmental risk.	Yes, apply 'carry' outside entity requirements	Not applicable
Leave unattended	Not applicable	Not applicable	No, do not leave unattended.	Yes, apply entity procedures, exercise judgement to assess environmental risk, and consider country-specific travel advice.	Yes, apply entity procedures.	Not applicable
Store while travel	Not applicable	Not applicable	No, do not store while travelling (eg in hotel room). If required, can be stored in Australian entity facility meeting 'store' inside entity requirements.	Yes, apply 'store' outside entity requirements and consider country-specific travel advice.	Yes, apply 'store' outside entity requirements	Not applicable

Annex D. Security classified discussions

Annex D sets out the locations where audible dissemination of information (eg briefings, discussions and meetings either in person or using a mobile device) involving security classified information may be held.

Annex D supplements the guidance on implementing physical and audio security measures to prevent deliberate or accidental overhearing detailed in SPF policy 15: Physical security for entity resources.

Refer to Annexes B-C for mobile devices approved to access, process, store or communicate government security classified information or data.

	Security classified discussions			
Location of discussion	**TOP SECRET**	**SECRET**	**PROTECTED**	**OFFICIAL: SENSITIVE**
Zone 1	No	No	No	Yes, but exercise judgement
Zone 2	No	No	Yes, but exercise judgement	Yes
Zone 3	No	No, but ASIO Technical Notes permit irregular discussions[1]	Yes	Yes
Zone 4	No, but ASIO Technical Notes permit irregular discussions[1]	Yes	Yes	Yes
Zone 5	Yes	Yes	Yes	Yes
Outside entity - public spaces	No	No	No[2]	Yes, but exercise judgement
Outside entity – home based work	No[2]	No[2]	Yes, but exercise judgement	Yes, but exercise judgement
While travelling	No[2]	No[2]	No[2]	Yes, but exercise judgement

[1] ASIO Technical Notes define 'irregular discussions' as those that are unpredictable, non-ongoing or unannounced.

[2] If required for operational or ministerial briefing purposes, then yes providing appropriate alternative mitigations are in place and, where required, agreed by the relevant authority or originator of the information.

Annex E. Historical classifications and markings

Annex E Table 1 Historical classifications and sensitivity markings

Historical classification or sensitivity marking	Key dates	Current sensitive or classified information level equivalency	Handling
CONFIDENTIAL classification	PSPF recognition of the CONFIDENTIAL classification discontinued on 1 October 2018. Recognition of CONFIDENTIAL classification ceased on 1 October 2020.	None established. Consider the harm and apply corresponding security classification marking	Historical handling protections remain. See Annex E Table 2 and Table 3 for Protection and handling of CONFIDENTIAL information
For Official Use Only (FOUO) dissemination limiting marker (DLM)	FOUO DLM replaced on 1 October 2018. Recognition of the FOUO DLM ceased on 1 October 2020.	FOUO is equivalent to the current OFFICIAL: Sensitive level.	Handling of FOUO information is as per PSPF requirements for OFFICIAL: Sensitive information.
Sensitive DLM	Sensitive DLM replaced on 1 October 2018. Recognition of the Sensitive DLM ceased on 1 October 2020.	Unless otherwise classified, Sensitive is equivalent to the current OFFICIAL: Sensitive level. The (optional) *Legislative secrecy* information management marker may be applied with a warning notice.	Handling of Sensitive information is as per the identified classification level.
Sensitive: Cabinet DLM	Sensitive: Cabinet DLM replaced on 1 October 2018. Recognition of the Sensitive: Cabinet DLM ceased on 1 October 2020.	The Sensitive: Cabinet DLM is equivalent to the current CABINET caveat.	Handling of Sensitive: Cabinet information is as per: a. the identified classification level and a. PSPF (and supporting Security Caveats Guidelines) requirements for the CABINET caveat.
Sensitive: Legal DLM	Sensitive: Legal DLM replaced on 1 October 2018. Recognition of the Sensitive: Legal DLM ceased on 1 October 2020.	Unless otherwise classified, Sensitive: Legal is equivalent to the current OFFICIAL: Sensitive level. The (optional) *Legal privilege* information management marker may be applied.	Handling of Sensitive: Legal information is: a. if classified, as per the identified classification level b. if not classified, as per PSPF requirements for OFFICIAL information.
Sensitive: Personal DLM	Sensitive: Personal DLM replaced on 1 October 2018. Recognition of the Sensitive: Personal DLM ceased on 1 October 2020.	Unless otherwise classified, Sensitive: Personal is equivalent to the current OFFICIAL: Sensitive level. The (optional) *Personal privacy* information management marker may be applied.	Handling of Sensitive: Personal information is: a. if classified, as per the identified classification level b. if not classified, as per PSPF requirements for OFFICIAL information.
HIGHLY PROTECTED classification	Recognition of the HIGHLY PROTECTED classification ceased on 1 August 2012.	HIGHLY PROTECTED is equivalent to the current SECRET classification.	Handling of HIGHLY PROTECTED information is as per PSPF requirements for SECRET information.
RESTRICTED classification	Recognition of the RESTRICTED classification ceased on 1 August 2012.	RESTRICTED is equivalent to the current OFFICIAL: Sensitive level.	Handling of RESTRICTED information is as per PSPF requirements for OFFICIAL: Sensitive information.
X-IN-CONFIDENCE classification	Recognition of the X-IN-CONFIDENCE classification ceased on 1 August 2012.	X-IN-CONFIDENCE is equivalent to the current OFFICIAL: Sensitive level.	Handling of X-IN-CONFIDENCE information is as per PSPF requirements for OFFICIAL: Sensitive information.

Protection and handling of CONFIDENTIAL information

The historical classification CONFIDENTIAL does not have an equivalent level of classification under the current PSPF. Information that was classified as CONFIDENTIAL before October 2020 has a business impact level of very high. This means that the compromise of CONFIDENTIAL information's confidentiality would be expected to cause significant damage to the national interest, organisations or individuals. Annex E Table 2 provides the sub-impact categories for this business impact level.

Annex E Table 2 Business Impact Level of CONFIDENTIAL information: Business Impact Level 3A

Sub-impact categories	Significant damage is:
Impacts on national security	causing damage to national security.
Impacts on entity operations	a. causing a severe degradation in, or loss of, organisational capability to an extent and duration that the entity cannot perform one or more of its functions for an extended time b. resulting in major long-term harm to entity assets.
Australian financial and economic impacts	a. undermining the financial viability of, or causing substantial financial damage to, a number of major Australia-based or Australian-owned organisations or companies b. causing long-term damage to the Australian economy to an estimated total of $10 to $20 billion c. causing major, short-term damage to global trade or commerce, leading to short-term recession or hyperinflation in Australia.
Impacts on government policies	a. significantly disadvantaging Australia in international negotiations or strategy b. temporarily damaging the internal stability of Australia or friendly countries c. causing significant damage or disruption to diplomatic relations, including resulting in formal protest or retaliatory action.
Impacts on personal safety	endangering small groups of individuals – the compromise of information could lead to serious harm or potentially life-threatening injuries to a small group of individuals
Impacts on crime prevention	causing major, long-term impairment to the ability to investigate serious offences, ie offences resulting in two or more years imprisonment.
Impacts on defence operations	causing damage to the operational effectiveness or security of Australian or allied forces that could result in risk to life.
Impacts on intelligence operations	causing damage to Australian or allied intelligence capability.
Impacts on national infrastructure	damaging or disrupting significant national infrastructure.

The following information describes the minimum protections and handling for legacy CONFIDENTIAL information.

Annex E Table 3 Minimum protection and handling for CONFIDENTIAL information

BIL 3.5	CONFIDENTIAL—significant damage to the national interest, organisations or individuals
Protective marking	Maintain text-based protective marking **CONFIDENTIAL** to documents (including emails). If text-based markings were not used, maintain colour-based markings. For CONFIDENTIAL a green colour was used historically. If text or colour-based protective markings cannot be used, apply the entity's marking scheme for such scenarios. From October 2020, do not mark new information as CONFIDENTIAL. For new information that would previously have been marked CONFIDENTIAL, consider the harm and apply corresponding security classification marking under the current PSPF.
Access	The need-to-know principle applies to all CONFIDENTIAL information. Ongoing access to CONFIDENTIAL information requires a Negative Vetting 1 security clearance or above. Any temporary access must be supervised.
Use	CONFIDENTIAL information and mobile devices that process, store or communicate CONFIDENTIAL information can be used in security Zones 1-5. **Outside entity facilities (including at home)** CONFIDENTIAL information and mobile device that processes, stores or communicates CONFIDENTIAL information: a. **do not** use for regular ongoing home-based work

	a. occasional home-based work **not recommended**, but if required, obtain manager approval, apply entity procedures on need for a security assessment, and exercise judgement to assess environment risk b. **do not** use elsewhere (for example café).
Storage	**Do not** leave CONFIDENTIAL information or a mobile device that processes, stores or communicates CONFIDENTIAL information unattended, store securely when unattended. When storing physical CONFIDENTIAL information a. inside entity facilities (Zones 2-5 only): i. Zones 3-5, store in Class C container — Zone 2, store in Class B container. b. Outside entity facilities **not recommended**, if required for occasional home-based work (see use above): i. apply requirements for carrying outside entity facilities, and i. retain in personal custody (strongly preferred), or for brief absences from home, store in Class B or higher container (container must be approved as a proper place of custody by the Accountable Authority or their delegate), and return to entity facility as soon as practicable. When storing a mobile device that processes, stores or communicates CONFIDENTIAL information i. inside entity facilities (Zones 2-5 only): a. Zones 3-5: if in a secured or unsecured state, store in Class C container a. Zone 2: if in a secured state, Class B container, if unsecured state, store in a higher zone. b. Outside entity facilities **not recommended**, if required for occasional home-based work (see use above): a. apply requirements for carrying outside entity facilities, and ii. retain in personal custody (strongly preferred), or for brief absences from home, exercise judgement to store in a Class C container.
Carry	When carrying physical CONFIDENTIAL information a. inside entity facilities: i. Zones 2-5, retain in personal custody in an opaque envelope or folder that indicates Classification — Zones 1, retain in personal custody in an opaque envelope or folder that indicates classification and place in a security briefcase, pouch or satchel. b. outside entity facilities (including external meetings) and between entity facilities: i. retain in personal custody ii. place in a security briefcase, pouch or satchel, and iii. **recommend** tamper-evident packaging if aggregate information increases risk. When carrying a mobile device that processes, stores or communicates CONFIDENTIAL information i. inside entity facilities: i. Zone 5, if in a secured or unsecured state, apply entity procedures d. Zones 2-4, carry in secured state; if in an unsecured state, apply entity in procedures ii. Zone 1, carry in a secured state; if in an unsecured state, place inside a security briefcase, pouch or satchel. c. outside entity facilities (including external meetings) and between entity facilities: a. in a secured state, retain in personal custody e. in an unsecured state, carry inside a security briefcase, pouch or satchel and consider tamper evident seals.
Transfer	When transferring CONFIDENTIAL information a. inside entity facilities (Zones 1-5): transfer by hand or entity safe hand and apply requirements for carrying; can be uncovered if office environment presents very low risk of unauthorised viewing b. to another officer in a different facility a. apply requirements for carrying outside entity facilities, and iii. transfer by hand, entity safe hand, safe hand courier rated BIL 4, or DFAT courier (if transfer by courier, use tamper evident packaging). Any transfer requires a receipt.

Transmit	When transmitting electronically communicate over SECRET secure networks (or networks of higher classification). Use ASD's High Assurance Cryptographic Equipment to encrypt CONFIDENTIAL information for any communication that is not over a SECRET network (or network of higher classification).
Official travel	**Travel in Australia** When travelling with physical CONFIDENTIAL information: a. apply requirements for carrying outside entity facilities and any additional entity procedures b. for airline travel, retain as carry-on baggage and if airline requires to be checked at the gate, try to observe entering and exiting the cargo hold and reclaim ASAP c. **do not** leave CONFIDENTIAL information unattended, retain in personal custody, and d. **do not** store while travelling (eg in a hotel room), if storage required, store in an Australian entity facility. When travelling with a mobile device that processes, stores or communicates CONFIDENTIAL information: a. apply requirements for carrying outside entity facilities and any additional entity procedures b. **not recommended** for airline travel, if required, retain as carry-on baggage and if airline requires to be checked at the gate, try to observe entering and exiting the cargo hold and reclaim ASAP c. **do not** leave CONFIDENTIAL information unattended, retain in personal custody, and d. **do not** store while travelling, if storage required, store in an Australian entity facility. **Travel outside Australia** **Not recommended** to travel overseas with physical CONFIDENTIAL information. If required, follow entity procedures, and if required, consult DFAT. **Do not** travel overseas with a mobile device that processes, stores or communicates CONFIDENTIAL information. If required, see DFAT advice on options to access information at destination.
Disposal	Dispose of CONFIDENTIAL information using a Class A shredder or entity-assessed and approved or NAID AAA certified destruction service with specific endorsement and approved equipment and systems.

Annex F. Email protective marking standard

The Email protective marking standard provides guidance for applying protective markings (and, where relevant, information management markers) on emails exchanged in and between Australian Government entities.

Annex F - Email protective marking standard

Annex G. Sample case studies

The following case studies are examples that entities may wish to draw on or adapt in establishing their procedures and operational controls. These are examples of application of the policy only, and the Department of Home Affairs recommends that entities consider whether the examples provided meet entity-specific requirements and are suitable for use in conjunction with existing entity procedures.

Entity personnel should not rely on these examples for advice on how to apply the PSPF—consult a security advisor in your entity to ensure you are applying the PSPF in accordance with your entity's security plan and procedures.

Case study: Example of information declassification for increased sharing

The Productivity Commission Data Availability and Use report indicates that a wide range of government data can be shared. The availability and usefulness of data delivers benefits to the community, engenders community trust and confidence in how data is managed and used and preserves commercial incentives to collect, maintain and add value to data.

For example, there is potential for data about health service provider costs and performance, as well as de-identified linked data about health service recipients, that can be used for effective and targeted service interventions and improved health outcomes.

Identifying characteristics that appear predictive during data analysis can provide valuable insights into the effectiveness of various policies and interventions, allowing new services to emerge in response to community demand.

By de-identifying the health service recipients' data or redacting sensitive personal details, the information is no longer considered to be OFFICIAL: Sensitive (as it does not include sensitive information under the Privacy Act or other measures of harm) and can be shared. If desirable, the protection markings for OFFICIAL can be applied to the information.

Case study: Using TOP SECRET information in a Zone 3

An officer with NV2 clearance wants to read a TOP SECRET document in a Zone 3 within the entity. In accordance with the minimum protections outlined in **Annexure A**, the officer assesses their surroundings to judge whether the people and equipment within their proximity are likely to compromise the officer's ability to protect the information from unauthorised access.

The officer notes that several of the people around them are contractors without security clearances. The officer judges that there is a high probability that an unauthorised person may see the material and decides the information could be more easily secured from unauthorised viewing by moving to a nearby meeting room within the Zone 3 to read the material. Before moving to the meeting room, the officer puts the material in a folder with TOP SECRET indicated on the front.

Case study: Physical presence when at home in Australia

An officer is attending an early morning meeting tomorrow in another government building in the same city in Australia. The officer requires access to a PROTECTED document for use at the meeting. Given the meeting starts at 6:30am close to where the officer lives, the officer's manager has given approval for them to take the material home overnight providing the officer:

(i) confirms the external meeting will take place in a meeting room that is a security zone

(ii) secures the information from unauthorised access by using double-enveloping (in a sealed envelope inside a security briefcase)

(iii) does not open or use the information until the officer is in the secure meeting room, and

(iv) keeps the information in their personal custody/physical presence (ie keeps the secured information in the same room with them, including while asleep).

While the officer is at home, they remember a dinner engagement at the local restaurant. The officer judges that taking the security briefcase with them would draw attention and determines the information would be safer left at home. The officer stores the security briefcase in a lockable cabinet and heads to dinner. As soon as the officer returns home, they retrieve the briefcase, open it to confirm the information is still sealed within, and then keep the briefcase with them until returning to their entity's facility after the meeting.

Case study: Removing TOP SECRET information from entity facilities to use in a meeting

An officer with a NV2 security clearance needs to remove a TOP SECRET document from the entity facility to attend an external meeting.

The officer knows that this practice is not recommended but the meeting organisers have advised they are unable to make the material available to attendees and requested they bring a copy with them. The officer takes the following steps to ensure the protection of the information:

(i) confirms the external meeting will take place in a government meeting room that is at lease a Zone 3

(ii) seeks their manager's written approval to remove the material, and keeps a record of the approval

(iii) records the information is being removed with manager approval in the team's Classified Document Register

(iv) secures the information from unauthorised access by enclosing the TOP SECRET information in a tamper evident envelope, and placing it in a security satchel

(v) ensures the material remains unopened until the officer is in the Zone 3 meeting room.

When the meeting concludes, the officer secures the TOP SECRET information in a tamper evident envelope and places it in the security satchel, where it remains unopened until the officer is back in a Zone 3 or higher of the entity facility.

Once back in the office, the officer updates the Classified Document Register to confirm the material has been returned to the entity facility.

Case study: assessing unmarked information

An entity regularly receives information from members of the public. The information does not bear a protective marking.

Upon receiving the information, the entity, as the 'originator', applies Requirement 2 of PSPF policy 8 to assess the value, importance or sensitivity of official information by considering the potential damage to government, the national interest, organisations or individuals that would arise if the information's confidentiality was compromised.

This information is now part of Australian Government business and cannot be marked UNOFFICIAL. As the information does not constitute personal information, the entity's receiving officer sets the protective marking or security classification at the lowest reasonable level, in this case OFFICIAL.

Case study: classifying aggregated OFFICIAL: Sensitive information

An entity regularly receives information on a particular topic that contains identifiable information, for example a Tax File Number (TFN), from members of the public. The information does not bear a protective marking or classification.

Upon receiving the information the entity, as the 'originator', applies Requirement 2 of PSPF policy 8 to assess the value, importance or sensitivity of official information by considering the potential damage to government, the national interest, organisations or individuals that would arise if the information's confidentiality was compromised. The entity's receiving officer therefore sets the protective marking or security classification at the lowest reasonable level, in this case OFFICIAL: Sensitive.

It is a core requirement of this policy that entities implement operational controls to protect information holdings in proportion to their value, importance and sensitivity. During the entity's security planning process, the Chief Security Officer identifies that while these individual pieces of information are appropriately marked as OFFICIAL: Sensitive, in aggregate form, they are likely to be more attractive target to potentially malicious actors.

The Chief Security Officer tasks a security advisor to perform a business impact level assessment of this aggregated information using the advice provided in Annex I of PSPF policy 8 and the Business Impact Level Tool. The security advisor's assessment is that the collated information in aggregation should attract a PROTECTED security classification, because the information is more valuable in aggregation and it would reveal new and more sensitive information that if compromised would cause reputational damage to the entity. The aggregated information is transferred to a PROTECTED system which offers a higher level of security and access control to the information.

Annex H. Assessing aggregated or integrated information holdings

This guidance relates to the classification of electronic aggregated or integrated Australian Government information.

Aggregated information

Aggregated information is a compilation of information that may be assessed as requiring a higher security classification or additional security controls where the aggregated holding is significantly more valuable than its individual components. This is because the collated information reveals new and more sensitive information or intelligence than would be apparent from the main source records and would cause greater damage than individual documents. When viewed separately, the components of the information holding retain their individual classifications. The entity that aggregates the information becomes the 'originator' and is therefore responsible for assessing the classification of the aggregated information.

Integrated information

Integrated information is information that is combined from different sources into a single, unified view. While the value of integrated data can be high, it is also generally de-identified, cleansed and transformed to the extent that it provides limited information outside of the insights for which it was created to provide. Considering this, integrated data is of a single value and should only be classified according to the value, importance and sensitivity of the fully integrated data set. The entity that integrates the data becomes the 'originator' and must therefore assess the classification of the integrated data.

Assessing the classification

It is a core requirement of this policy that entities identify their information holdings, assess the classification of those information holdings, and implement operational controls to protect information holdings in proportion to their value, importance and sensitivity. This process applies equally when information is aggregated or integrated to form a new holding.

Table 1 outlines the suggested process for applying these requirements to aggregated or integrated holdings.

Annex G Table 2 Process for considering the security classification of aggregated or integrated holdings

Process steps	Things to consider
1. Identify aggregated or integrated holdings	Identify the aggregated or integrated holdings in your entity (**core requirement**), and give thought to the following: • Has the information been sanitised or declassified from the original source? • Where is the holding stored and on what type of ICT system? – Is the system authorised to operate and with sufficient access and security controls? – If stored on a legacy system, are there sufficient alternative mitigations in place to limit the compromise of this data? – If stored on an ICT system that connects to multiple other systems, are the access controls in place sufficient to prevent unauthorised access to the dataset? – Does the system have sufficient access controls? • What permissions are in place to hold, store or use the holding? Will you need to agree the appropriate classification and/or protections with another entity?
2. Assess the value, importance or sensitivity	Assess the security classification of the holding (**core requirement**), and decide the classification by considering the potential damage to the government, national interest, organisations or individuals, that would arise if the holding's confidentiality was compromised (**Requirement 2**). Give thought to the following: • What is the highest classification or marking present in the holding? • Does the collated information reveal new and more sensitive information or intelligence than would be apparent from the main source records that would cause greater damage than individual documents? • Does bringing this information together make it a more attractive target to a potentially malicious actor or trusted insider? For example, large amounts of OFFICIAL: Sensitive personal or corporate information that when aggregated reveal significant information about the entity's operations or personnel. • Does other information or data stored on the same system affect the value of the holding?

	• Does the holding include caveated[1] information or optional information management markers and will this affect or limit the options for aggregating or integrating this information?
3. Consider the options and constraints	Based on the information gathered in steps 1 and 2, consider the options available to your entity and any constraints that would affect the appropriate classification to apply. Give thought to the following: • If the aggregated holding's classification is required to be raised, will it remain on the same system, where the same users will be able to access the information? If so, consider whether additional access or security controls are required to protect the aggregated information holding. • Does your entity's risk environment make your information a more attractive target for compromise by a malicious actor, including a trusted insider? If so, does this affect the type of access or security controls you will implement to protect the holding or does the holding need to be moved to an ICT system that enforces additional access requirements? • What is your internal security environment? Will the holding only be accessed by security cleared personnel, including any contractors? • What are the classifications of the ICT systems you have available to store the holding? • Where the entity does not have access to an ICT system rated to the proposed classification of the holding, remedial action is required to ensure the commensurate requirements for that classification can be implemented. – This may mean removing or storing the highly classified components separately. For example, if the holding is assessed overall as SECRET but the entity only has access to a PROTECTED network, then action will be required to ensure the holding is assessed no higher than PROTECTED. This may mean removing the more highly classified components.
4. Decide and document	Decide which protective marking or security classification to apply and what, if any, additional access or security controls are required to protect the holding from compromise. In accordance with PSPF policy 3: *Security planning and risk management*, document the decision in the entity's security plan along with acceptance of any residual risk and period of review of the decision.

[1] Refer to the Australian Government Security Caveat Guidelines for classification and handling requirements.

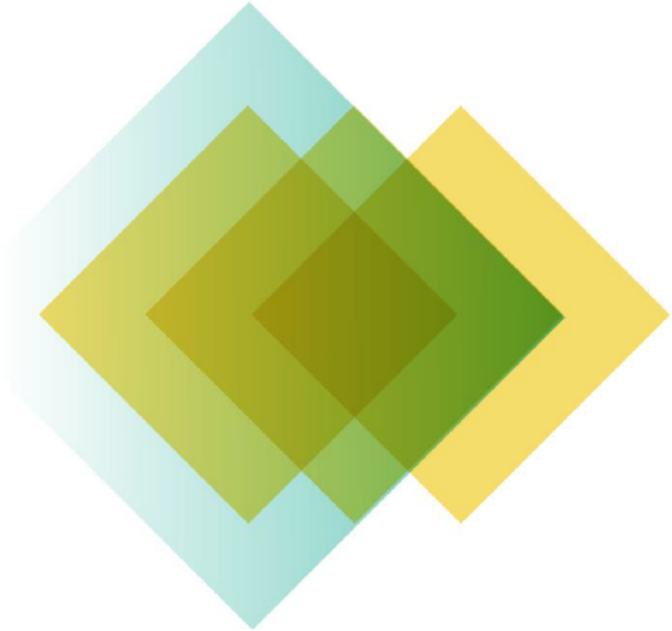
Australian Government

Office of the Australian Information Commissioner

OAIC PSPF Policy Statement and Framework

Incorporating the OAIC Security Policy Manual

Document ID:	**D2021/000285**
Version:	1.0
Approved:	8th January 2021



January 2021

OAIC

Document Control

Version	Review Date	Action	Authorised by
1	8 January 2021	Approved	Elizabeth Hampton (A/g Australian Information Commissioner)
1.1	7 September 2021	Updated numbering of policies and procedures to be 3 places (PSPF policy number: OAIC policy number for that PSPF policy: Procedure number for that OAIC policy).	

Table of Contents

OAIC Security Policy Statement

The Office of the Australian Information Commissioner (OAIC) is committed to ensuring the secure delivery of its services and continuing to build trust and confidence in its ability to engage with and manage protective security risks.

The OAIC will work towards meeting the following five principles of the Protective Security Policy Framework (PSPF):

1. Security is everyone's responsibility. Developing and fostering a positive security culture is essential to ensuring effective security outcomes.
2. Security enables the OAIC to deliver efficient and effective services.
3. Security measures protect the OAIC's people, information and assets and are complementary to their assessed risks.
4. The Australian Information Commissioner and Privacy Commissioner own the security risks of the OAIC and its impact on shared risks.
5. A cycle of action, evaluation and learning is expected at the OAIC in response to security incidents.

Additionally, the OAIC strives to achieve the following four security outcomes:

1. **Governance** – The OAIC manages security risks and supports a positive security culture ensuring:
   - clear lines of accountability, sound planning, investigation and response, assurance, and review processes, and
   - proportionate reporting.
2. **Information** – The OAIC maintains the confidentiality, integrity and availability of all official information.
3. **Personnel** - The OAIC ensures the suitability of its employees and contractors to access Australian Government resources and that they meet appropriate standards of integrity and honesty.
4. **Physical** - The OAIC provides a safe and secure physical environment for its people, information, and assets.

The security of the OAIC is a shared responsibility and therefore, I encourage the development and maintenance of a positive security culture throughout the organisation.

Elizabeth Hampton

A/g Australian Information Commissioner and Privacy Commissioner

8 January 2021

OAIC Security Framework

The OAIC's security framework is outlined in the diagram below:

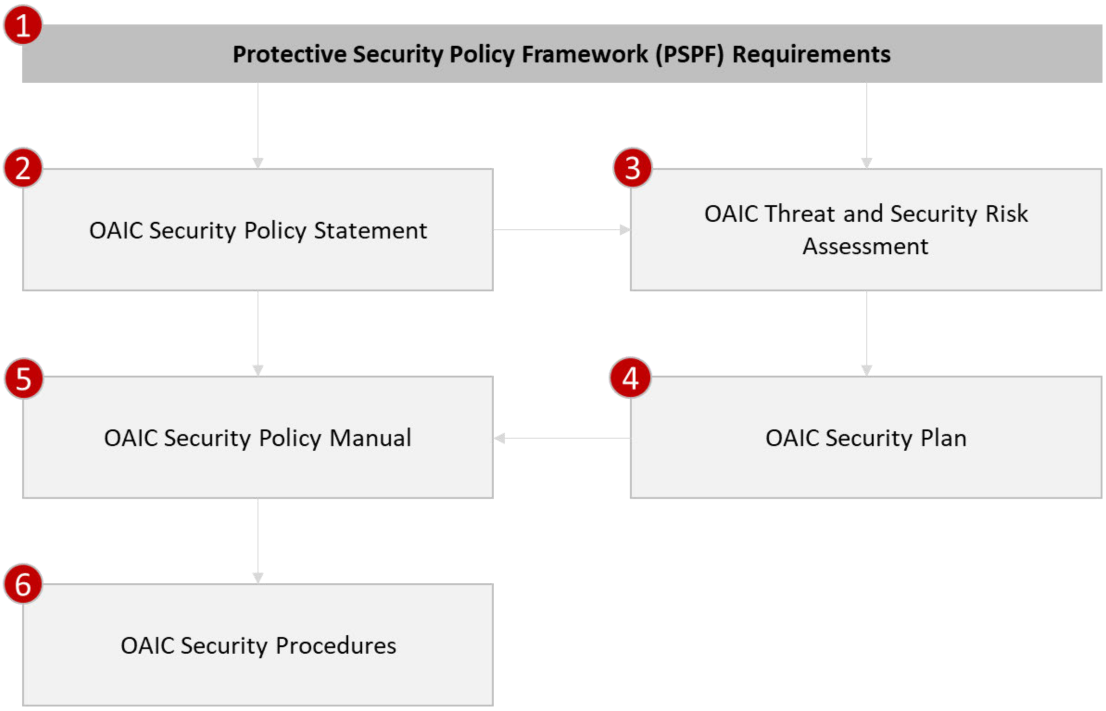

1
Protective Security Policy Framework (PSPF) Requirements
2
OAIC Security Policy Statement
3
OAIC Threat and Security Risk Assessment
5
OAIC Security Policy Manual
4
OAIC Security Plan
6
OAIC Security Procedures

Figure 1- OAIC Security Framework

The elements of the OAIC Security Framework and their interactions are outlined below:

1. **Protective Security Policy Framework (PSPF) Requirements** – The PSPF has been developed to assist Australian Government entities to protect their people, information and assets, at home and overseas. The PSPF articulates government protective security policy. It also provides guidance to entities to support the effective implementation of the policy across the areas of security governance, personnel security, physical security and information security. (PSPF requirements may be found at www.protectivesecurity.gov.au).

2. **OAIC Security Policy Statement** – This document is presented on the previous page and outlines the OAIC's commitment to the PSPF's:
    a. five principles that apply to every area of security. These are fundamental values that represent what is desirable for all entities – security principles guide decision making.
    b. four outcomes that outline the desired end-state results the government aims to achieve. Desired protective security outcomes relate to security governance, as well as information, personnel, and physical security.
    c. sixteen core requirements that articulate what entities must do to achieve the government's desired protective security outcomes.

3. **OAIC Threat and Security Risk Assessment** – This is an objective and stand-alone document that addresses PSPF 3 - security planning and risk management. It helps to ensure that the OAIC is aware of its security risk context, threat, and broader risk environment. It informs the development of a security plan (see 4 below). The OAIC Threat and Security Risk Assessment may be found at D2020/018345.

4. **OAIC Security Plan** - This is an objective and stand-alone document that addresses PSPF 3 - security planning and risk management. This document details how the OAIC plans to manage and address its security risks. It helps to ensure that appropriate controls are in place to manage security risks. It defines the extent to which the sixteen core requirements and supporting requirements are implemented at the OAIC through policies and procedures (see 5 and 6 below). The OAIC Security Plan may be found at D2020/019633.

5. **OAIC Security Policy Manual** – As presented in this document. The OAIC currently has 25 policies that map to the sixteen elements of the PSPF. These policies outline how the OAIC complies with the core and supporting requirements of the PSPF. They also provide a roadmap to relevant procedures (see 6 below) and guides that support the operational implementation of the PSPF.

6. **OAIC Security Procedures** – Are referenced under each policy and presented in Annex A. These procedures provide the detailed steps related to the implementation of OAIC security policies (see 5 above).

OIAC Security Policy Manual

Scope and Authority

Scope

These policies apply to the Office of the Australian Information Commissioner.

Review

Security policies will be reviewed:

a. annually to ensure that they remain fit-for-purpose; or
b. when there are any amendments to the Protective Security Policy Framework.

Selected policies will be reviewed and updated if they are impacted by:

a. a major security incident
b. a change to the National Terrorism Threat Advisory System; and
c. any changes made to the office environment including, but not limited to:

    i. relocation.
    ii. renovation; and
    iii. change in security zones.

Note

The processes and procedures associated with this document reflect the way the OAIC applies the PSPF in upholding all relevant requirements and ensuring existing protective apparatus are in place, aligned and will mature over time to respond to existing or emerging threats and risks.

Where the CSO (or security advisor on behalf of the CSO) implements an alternative mitigation measure or control to a PSPF requirement, they must document the decision and adjust the maturity level for the related PSPF requirement.

Authority

These policies have been endorsed by the Australian Information Commissioner and Privacy Commissioner.

Elizabeth Hampton
A/g Australian Information Commissioner and Privacy Commissioner
8 January 2020

Governance Outcome

Policy 1 - 1: Role of Accountable Authority

PSPF 1 – Core Requirement

The accountable authority is answerable to their minister and the government for the security of their entity.

The accountable authority of each entity must:

a. determine their entity's tolerance for security risks
b. manage the security risks of their entity
c. consider the implications their risk management decisions have for other entities, and share information on risks where appropriate

The accountable authority of a lead security entity must:

a. provide other entities with advice, guidance and services related to government security
b. ensure that the security support it provides helps relevant entities achieve and maintain an acceptable level of security
c. establish and document responsibilities and accountabilities for partnerships or security service arrangements with other entities.

Purpose

The purpose of this Policy is to set out role and responsibilities of the Office of the Australian Information Commissioner's (OAIC) accountable authority.

Policy

It is the policy of the OAIC that the accountable authority for the OAIC is the Australian Information Commissioner and Privacy Commissioner and that the accountable authority is answerable to the Attorney-General and the government for the security of the OAIC.

The accountable authority is responsible for:

a. implementing the PSPF core and supporting requirements
b. appointing an SES Chief Security Officer who is responsible for oversight of protective security and authorised to make security decisions (see PSPF policy: Management structures and responsibilities)
c. providing security awareness training for personnel (including contractors) about their security responsibilities (see PSPF policy: Management structures and responsibilities)
d. approving an appropriate security plan to manage security risks and ensure personnel understand how to manage those risks (see PSPF policy: Security planning and risk management)
e. ensuring appropriate accreditation processes are in place for ICT systems, including accepting any residual security risks to the system or the information the system processes, stores or communicates (see PSPF policy: Robust ICT systems)
f. fostering a positive security culture with clearly defined expectations and priorities (see PSPF policy: Security planning and risk management)
g. monitoring the entity's security maturity (see PSPF policy: Security maturity monitoring)

h. accurately recording in the annual report of the entity's security maturity (see PSPF policy: Reporting on security)
i. approving citizenship waivers and uncheckable background waivers (see PSPF policy: Eligibility and suitability of personnel)
j. embedding effective security risk management
k. ensuring variances to PSPF implementation (as a result of exceptional circumstances) are defendable, considered in light of the entity's risk tolerances and are for a limited time period.

The accountable authority responsibilities are addressed through the plans, policies and procedures incorporated in the OAIC Security Policy Suite.

OAIC is the lead security entity with responsibility for whole of government information management policy and practice, including freedom of information and privacy. The accountable authority will provide advice, guidance and services related to government security, ensure appropriate security support is provided to assist relevant entities to achieve and maintain an acceptable level of security and establish and document responsibilities and accountabilities for partnerships or security service arrangements with other entities as necessary.

Tolerance for security risks

Security risk tolerance is addressed through the OAIC Risk Appetite Statement. This is found at D2021/002782.

In its approach to risk management, the OAIC has a low tolerance for security risks and uses the As Low As Reasonably Practical (ALARP) approach to determine whether specific risks are acceptable, acceptable when treated, or not acceptable.

References and associated Policies/Procedures

All security policies and procedures supporting the PSPF documented or referenced in this Policy Statement and Framework.

s22

Policy 2-1: Security appointments and responsibilities

PSPF 2 - The accountable authority is answerable to their minister and the government for the security of their entity.

The accountable authority must:

a. **appoint a Chief Security Officer (CSO) at the Senior Executive Service level 1 to be responsible for security in the entity.**

b. empower the CSO to make decisions about:

- **i. appointing security advisors within the entity**
- **ii. the entity's protective security planning**
- **iii. the entity's protective security practices and procedures**
- **iv.** investigating, responding to, and reporting on security incidents

c. ensure personnel and contractors are aware of their collective responsibility to foster a positive security culture and are provided sufficient information and training to support this.

And

	Supporting requirements
Requirement 1. Security advisors	**The CSO must be responsible for directing all areas of security to protect the entity's people, information (including ICT) and assets. This includes appointing security advisors to support them in the day-to-day delivery of protective security and, to perform specialist services.**
Requirement 2. Security procedures	**Entities must develop and use procedures that ensure:** **a. all elements of the entity's security plan are achieved** **b. security incidents are investigated, responded to, and reported** **c. relevant security policy or legislative obligations are met.**
Requirement 3. Security training	Entities **must** provide all personnel, including contractors, with security awareness training at engagement and annually thereafter.
Requirement 4. Specific training	Entities **must** provide personnel in specialist and high-risk positions (including contractors and security incident investigators) with specific security awareness training targeted to the scope and nature of the position.
Requirement 5.	**Entities must maintain a monitored email address as the central**

General email	**conduit for all security-related matters across governance, personnel, information (including ICT) and physical security.**

- Bolded elements addressed in this policy.

Purpose

The purpose of this Policy is to set out the Protective Security Policy Framework (PSPF) requirements for security appointments for the Office of the Australian Information Commissioner (OAIC).

Policy

It is the policy of the OAIC that the security roles and responsibilities of the accountable authority and others with security responsibilities are clearly defined and that there are clear lines of accountability. The OAIC will ensure, when appointing personnel to a security role, their responsibilities are clearly defined and explained, and that they receive appropriate training to enable them to fulfil their roles.

Appointment of Chief Security Officer

The PSPF mandates that a Chief Security Officer (CSO) must be appointed at the Senior Executive Service (SES) level and be empowered to oversee security across the OAIC and make security-related decisions. The CSO supports the accountable authority to protect the OAIC's people, information and assets and achieve the requirements outlined in PSPF policy. The accountable authority has appointed the Deputy Commissioner as the CSO.

Appointment and responsibilities of the Agency Security Adviser

The OAIC has an Agency Security Adviser (ASA) and Information Technology Security Adviser (ITSA). These positions are appointed by the CSO and manage security functions and implement and monitor the PSPF requirements. The ITSA is an officer of the Australian Human Rights Commission given shared service arrangements.

The ASA is responsible for developing and using procedures that ensure:

a. all elements of the entity's security plan are achieved
b. security incidents are investigated, responded to, and reported
c. relevant security policy or legislative obligations are met.
d. OAIC maintains a monitored email address as the central conduit for all security-related matters across governance, personnel, information (including ICT) and physical security.

All OAIC personnel and contractors

All positions are responsible for:

a. being aware of and adhering to OAIC ICT Security Policies and Procedures
b. being aware of and adhering to specific SOPs for their position.
c. accessing only information/systems to which they are appropriately approved, and in accordance with the Need-to-Know principle
d. reporting any security incident (suspected or actual) as per OAIC Incident Response Procedures
e. ensuring security is integrated into their own procedures as standard practice.

Delegations

All responsibilities and powers delegated to each security position will be assumed by any person appointed to act in that role in the absence of the incumbent.

Procedures

Procedure 2-1-1: Security Appointments – D2020/019569

References and associated policies/procedures

PSPF 1: Role of accountable authority

PSPF 2: Management structures and responsibilities

PSPF 13: Ongoing assessment of personnel

Procedure 3-1-1: Security Risk Management - D2020/019568

s22

s22

Policy 2 - 3: Security awareness training

PSPF 2 - The accountable authority must:

a. appoint a Chief Security Officer (CSO) at the Senior Executive Service level to be responsible for security in the entity

b. empower the CSO to make decisions about:
   I. appointing security advisors within the entity
   II. the entity's protective security planning
   III. the entity's protective security practices and procedures
   IV. investigating, responding to, and reporting on security incidents

c. ensure personnel and contractors are aware of their collective responsibility to foster a positive security culture, and are provided sufficient information and training to support this

And

	Supporting requirements
Requirement 3. Security Training	Entities **must** provide all personnel, including contractors, with security awareness training at engagement and annually thereafter.

Purpose

The purpose of this Policy is to set out the Protective Security Policy Framework (PSPF) requirements for security awareness training at the Office of the Australian Information Commissioner (OAIC).

Policy

It is the policy of the OAIC that security awareness training will be provided to all employees and contractors undertaking work for the OAIC on induction, and thereafter:

- annually
- in the event of a significant security breach
- if/when any legislative changes affect the responsibilities of the OAIC
- If/when there are any significant changes to ICT systems of procedures
- if, in the opinion of the CSO, ASA or ITSA, that there is a need for further training.

Training

The OAIC will present training as set out in the supporting material and will be delivered through either face-to-face or online training. This training will be augmented by:

a. campaigns that address the ongoing needs of the entity and the specific needs of sensitive areas, activities, or periods of time

b. security instructions and reminders via publications, electronic bulletins, and visual displays such as posters

c. protective security-related questions in personnel selection interviews

d. drills and exercises; and

e. inclusion of security awareness and attitudes in the entity performance management program.

References and associated policies

PSPF 2: Management structures and responsibilities

Supporting material

Content of security awareness training[2]

Audience	Suggested content
Content for all personnel	The Attorney General's Department recommends that security awareness training programs or briefings include: a. an overview of protective security requirements, procedures and security culture in the entity. b. personal safety and security measures in entity facilities and in the field. c. individual and line manager security responsibilities. d. confidentiality, integrity and availability requirements for information and assets, including intellectual property. e. understanding entity-specific security risks and threats: i. the protective security policies and procedures for their area. ii. the risks the policies and procedures are designed to mitigate against. iii. the roles and responsibilities of personnel in relation to the policies and procedures. f. information control measures (need-to-know principle). g. overseas travel safety and security. h. unusual and suspicious behaviour. i. asset protection. j. reporting requirements, including but not limited to: i. reporting security incidents (including compromise of information, breach of entity procedures, data spills. ii. contact reporting, including the Contact Reporting Scheme. iii. reporting concerns about other personnel, including their suitability to access Australian Government resources. iv. any other entity-specific reporting requirements including public interest disclosure (whistleblowing) under the *Public Interest Disclosure Act 2013*. Previously reported or investigated security incidents can be used in security awareness training to demonstrate what could happen, how to respond to incidents, and how to minimise them in the future. The Attorney-General's Department recommends that information be redacted to maintain appropriate confidentiality.

[2] PSPF 2: Management structures and responsibilities

Audience	Suggested content
Additional content for security-cleared personnel	The Attorney-General's Department recommends that, as a minimum, security awareness training programs or briefings for security-cleared personnel: a. ensure that people who have access to security classified resources, understand and accept their day-to-day security responsibilities and reporting obligations (e.g. changes of circumstances, and suspicious, ongoing, unusual or persistent contacts). b. provide clearance holders with briefing and training reminding them of their clearance responsibilities at regular intervals. c. include training and briefings from or in consultation with compartment owners, for personnel with access to Sensitive Compartmented Information.
High-risk positions	Requirement 4 mandates that entities must provide personnel in specialist and high-risk positions (including contractors and security incident investigators) with specific security awareness training to address risks related to the nature and scope of their work or specialisations. Specialist or high-risk positions may include: a. sensitive or priority negotiations or policy work. b. responsibility for or access to valuable or attractive assets. c. working remotely or in dangerous conditions. d. being required to liaise with foreign officials, or regularly share information with foreign officials.

s22

s22

s22

s22

s22

[redacted]

s22

s22

[redacted]

s22

s22

[redacted]

s22

s22

Policy 6-1: Contract and procurement security

PSPF 6 - Each entity is accountable for the security risks arising from procuring goods and services and must ensure contracted providers comply with relevant PSPF requirements.

And

	Supporting requirements
Requirement 1. Assessing and managing security risks of procurement	When procuring goods or services, entities **must** put in place proportionate protective security measures by identifying and documenting: a. specific security risks to its people, information and assets b. mitigations for identified risks.
Requirement 2. Establishing protective security terms and conditions in contracts	Entities **must** ensure that contracts for goods and services include relevant security terms and conditions for the provider to: a. apply appropriate information, physical and personnel security requirements of the PSPF b. manage identified security risks relevant to the procurement c. implement governance arrangements to manage ongoing protective security requirements, including to notify the entity of any actual or suspected security incidents and follow reasonable direction from the entity arising from incident investigations.
Requirement 3. Ongoing management of protective security in contracts	When managing contracts, entities **must** put in place the following measures over the life of a contract: a. ensure that security controls included in the contract are implemented, operated and maintained by the contracted provider and associated subcontractor b. manage any changes to the provision of goods or services, and reassess security risks.
Requirement 4. Completion or termination of a contract	Entities **must** implement appropriate security arrangements at completion or termination of a contract.

Purpose

The purpose of this Policy is to ensure that the Office of the Australian Information Commissioner (OAIC) assesses and manages security risks arising from procuring goods and services and to reduce the likelihood of additional financial and non-financial costs to government.

Policy

It is the policy of the OAIC that when procuring goods or services, proportionate protective security measures will be determined, documented and managed throughout the term of the contract.

Procedures

OAIC Procurement Policy and Procedures - D2021/000849

References and associated policies and procedures

PSPF 6: Security governance for contracted goods and service providers

PSPF 3: Security planning and risk management

Procedure 3-1-1: Security Risk Management - D2020/019568

s22

[redacted]

s22

Information Security Outcome

Policy 8-1: Information security classification

PSPF 8 - Each entity must:

a. identify information holdings

b. assess the sensitivity and security classification of information holdings

c. implement operational controls for these information holdings proportional to their value, importance, and sensitivity.

The supporting requirements help Australian Government entities maintain the confidentiality, integrity and availability of official information—including where the entity is the originator of information (the entity that initially generated or received the information). The OAIC's address of PSPF 8 supporting requirements are detailed in OAIC Policy and Procedures for Information Management - D2020/019571.

Purpose

The purpose of this Policy is to describe the way the Office of the Australian Information Commissioner (OAIC) identifies its information holdings and assesses the sensitivity or security classification of its information. The policy also ensures that the OAIC's information is correctly marked, handled, stored, and declassified and/or disposed of to ensure information is not compromised.

Policy

All of the OAIC's information holdings are identified, appropriately classified, and controlled in accordance with the requirements of the Protective Security Policy Framework.

Procedures

OAIC Information Management Policy - D2020/019571

References and associated policies

PSPF 8: Sensitive and classified information

Policy 9-1: Access to information

PSPF 9 - Each entity must enable appropriate access to official information. This includes:

a. sharing information within the entity, as well as with other relevant stakeholders

b. ensuring that those who access sensitive or security classified information have an appropriate security clearance and need to know that information

controlling access (including remote access) to supporting ICT systems, networks, infrastructure, and applications.

And

	Supporting requirements
Requirement 1. Formalised agreements for sharing information and resources	When disclosing security classified information or resources to a person or organisation outside of government, entities must have in place an agreement or arrangement, such as a contract or deed, governing how the information is used and protected.
Requirement 2. Limiting access to sensitive and classified information and resources	To reduce the risk of unauthorised disclosure, entities must ensure access to sensitive and security classified information or resources is only provided to people with a need-to-know.
Requirement 3. **Ongoing access security classified information and resources**	Entities must ensure that people requiring ongoing access to security classified information or resources are security cleared to the appropriate level: a. For ongoing access to PROTECTED information—Baseline security clearance or above b. For ongoing access to SECRET information—Negative Vetting 1 security clearance or above c. For ongoing access to TOP SECRET information—Negative Vetting 2 security clearance or above Note: Some Australian office holders are not required to hold a security clearance. In addition, entities must ensure that people requiring access to caveated information meet all clearance and suitability requirements imposed by the originator and caveat owner.

	Note: Access to caveated material that involves a codeword requires a briefing and may require a Negative Vetting 1, Negative Vetting 2 level or Positive Vetting level security clearance as well as other additional requirements. For guidance, see the PSPF policy: Sensitive and classified information and the supporting Security Caveats Guidelines available for security advisors only on GovTEAMS or by request.
Requirement 4. Temporary access to classified information and resources	Entities may provide a person with temporary access to security classified information or resources on the basis of a risk assessment for each case. In such cases, entities must: a. limit the duration of access to security classified information or resources: i. to the period in which an application for a security clearance is being processed for the particular person ii. up to a maximum of three months in a 12-month period b. conduct recommended employment screening checks (see the PSPF policy: Eligibility and suitability of personnel) c. supervise all temporary access d. for access to TOP SECRET information, ensure the person has an existing Negative Vetting 1 security clearance e. deny temporary access to classified caveated information (other than in exceptional circumstances, and only with approval of the caveat owner).
Requirement 5. Managing access to information systems	To manage access to information systems holding sensitive or security classified information, entities must implement unique user identification, authentication and authorisation practices on each occasion where system access is granted.

Purpose

The purpose of this Policy is to ensure that access controls to information held by the Office of the Australian Information Commissioner (OAIC) are sufficient to enable staff to access that information in a timely, traceable and secure manner while providing appropriate security and privacy protections to that information.

Policy

It is the policy of the OAIC that appropriate access control measures are applied to physical and electronic information, both within the OAIC and wider Australian government systems, to allow the sharing of information within the OAIC and relevant stakeholders; ensuring that those who access sensitive or security classified information have an appropriate security clearance and need to know that information; and appropriate controls are implemented in line with shared service agreements to control access (including remote access) to supporting Information and Communications Technology (ICT) systems, networks, infrastructure, devices and applications.

OAIC information is not to be released into the public domain unless it has been approved by a member of the executive team.

Procedures

Procedure 9-1-1: Transporting classified material and secure fax management (via AGS) - D2020/019554

Proactive Information Access Audit Policy D2020/011546

References and associated policies and procedures

OAIC Policy and Procedures for Information Management - D2020/019571
PSPF 7: Security governance for international sharing

PSPF 8: Sensitive and classified information

PSPF 9: Access to information

PSPF 10: Safeguarding information from cyber threats

PSPF 11: Robust ICT systems

Policy 9-2: Clean desk

> PSPF 9 - Each entity must enable appropriate access to official information. This includes:
>
> a. sharing information within the entity, as well as with other relevant stakeholders
> b. ensuring that those who access sensitive or security classified information have an appropriate security clearance and need to know that information
> c. controlling access (including remote access) to supporting ICT systems, networks, infrastructure and applications.

And

	Supporting requirements
Requirement 2. Limiting access to sensitive and classified information and resources	To reduce the risk of unauthorised disclosure, entities must ensure access to sensitive and security classified information or resources is only provided to people with a need-to-know.

Purpose

The purpose of this Policy is to establish the minimum requirements for maintaining a "clean desk", where sensitive/critical information about our employees, our intellectual property, our stakeholders and our vendors is secure in locked areas and out of sight.

Policy

It is the policy of the OAIC that employees are required to ensure that all sensitive and security classified information in hardcopy or electronic form is secure in their work area at the end of the day and when they are away from their desk for an extended period.

Procedures

Procedure 9-2-1: Clean Desks - D2020/019555

References and associated policies

PSPF 8: Sensitive and classified information

PSPF 9: Access to information

PSPF 16: Entity facilities

Policy 10-1: Safeguarding information from cyber threats

PSPF 10 - Each entity must mitigate common and emerging cyber threats by:

a. implementing the following mitigation strategies from the Strategies to Mitigate Cyber Security Incidents:
   I. application control
   II. patching applications
   III. restricting administrative privileges
   IV. patching operating systems

b. considering which of the remaining mitigation strategies from the Strategies to Mitigate Cyber Security Incidents you need to implement to protect your entity.

And

	Supporting requirements
Requirement 1. Transacting online with the public	Entities **must** not expose the public to unnecessary cyber security risks when they transact online with government.

Purpose

This Policy describes the arrangements for the protection of information from cyber threats for the Office of the Australian Information Commissioner (OAIC).

Policy

It is the policy of the OAIC that appropriate measures are in place to mitigate common and emerging cyber threats. These measures include liaison with the OAIC's shared service provider for ICT services and ensuring all personnel and contractors are aware of their responsibility to protect information when transacting online with the public.

The OAIC will ensure that the public will not be exposed to unnecessary cyber security risks when they transact online with government.

Procedures / Plans

OAIC System Security Plan D2020/019556

OAIC Security Risk Management Plan D2017/003896

References and associated policies and procedures

Procedure 10-1-1: Information Security Assurance - D2020/019557

PSPF 10: Safeguarding information from cyber threats

Policy 11-1: Information and communication technology security

PSPF 11- Each entity must have in place security measures during all stages of ICT systems development. This includes certifying and accrediting ICT systems in accordance with the Information Security Manual when implemented into the operational environment.

And

	Supporting requirements
Requirement **Authorisation of ICT systems to operate**	Entities **must** only process, store or communicate information on ICT systems that the determining authority (or their delegate) has authorised to operate based on the acceptance of the residual security risks associated with its operation. When establishing new ICT systems, or implementing improvements to existing systems, the decision to authorise (or reauthorise) an ICT system to operate **must** be based on the *Australian Government Information Security Manual*'s six step risk-based approach for cyber security.
Requirement **Secure internet gateways**	Entities **must** protect internet-connected ICT systems, and the information they process, store or communicate, by implementing a secure internet gateway that meets Australian Signals Directorate requirements.

Purpose

This Policy describes the arrangements for the management and protection of Information and Communications Technology (ICT) for the Office of the Australian Information Commissioner (OAIC).

Policy

It is the policy of the OAIC that appropriate cyber security measures are in place to protect OAIC information and other data, commensurate with the assessed business impact level of its potential compromise.

Shared ICT Services

Under the terms of the Memorandum of Understanding between the OAIC and the Australian Human Rights Commission (AHRC), signed on 18 November 2019, the AHRC is responsible for all aspects of managing and protecting the OAIC's Information and Communications Technology System including:

- Providing guidance to staff in accessing and using the network

- set up and maintenance of accounts
- provision of remote access facilities
- high level advice to the OAIC on addressing its ICT needs
- provision of network/cloud resources
- provision of Virus/Malware protection, including maintenance of application whitelisting; and maintaining the security of the network
- provision of Information and Technology Security Adviser Services

While maintaining the network and equipment, the AHRC does not and will not have access to OAIC information stored on the network or the cloud.

Assurance

The OAIC seeks assurance from the AHRC that it is complying with all relevant IT security framework and policies and is accurately measuring and reporting its maturity against the Protective Security Policy Framework (PSPF) policies: 10 - Safeguarding information from cyber threats; and 11-Robust ICT systems.

The OAIC will meet with the AHRC ITSA, and Chief Information Security Officer regularly to discuss and review the security arrangements in place for protecting security classified and sensitive information. The AHRC ITSA will provide updates and reports to the OAIC as outlined in the AHRC ICT Security Management Plan and OAIC Information Security Assurances Procedures, which will involve reporting to the OAIC on the outcomes of all ICT Security Risk Assessments, the implementation of any mitigation implemented that are in line with the agreed Agencies Risk and Control Register, System Security Plan (SSP) and Standard Operating Procedures (SOP) that full under the AHRC ICT Security Risk Assessment and Management Plan (SRMP). These assurances are measures put in place under the shared services agreement under which the AHRC provides the ICT infrastructure and is the ICT service provider to OAIC, ensuring the OAIC follows both Commonwealth and industry best practice in ICT Security Management, including:

- Commonwealth Protective Security Policy Framework (PSPF), V 1.2, January 2011.
- Defence Signals Directorate (DSD) Information Security Manual (ISM), June 2011.
- ISO/AS/NZS 31000: 2009 – Risk Management – Principles and Guidelines.

Procedures

Procedure 10-1-1: Information Security Assurance - D2020/019557

References and associated policies and procedures

OAIC System Security Plan D2020/019556

OAIC Security Risk Management Plan D2017/003896

PSPF 7: Security governance for international sharing

PSPF 8: Sensitive and classified information

PSPF 9: Access to information

PSPF 10: Safeguarding information from cyber threats

PSPF 11: Robust ICT systems

s22

[redacted]

s22

s22

s22

[redacted]

s22

s22

[redacted]

s22

[redacted]

s22

s22

[redacted]

s22

s22

[redacted]

s22

Physical Security Outcome

Policy 15-1: Physical security for resources

PSPF 15 - Each entity must implement physical security measures that minimise or remove the risk of:

a. harm to people, and
b. information and physical asset resources being made inoperable or inaccessible, or being accessed, used or removed without appropriate authorisation.

And

	Supporting requirements
Requirement 1. Physical security measures	Physical security measures Entities must put in place appropriate physical security measures to protect entity resources, commensurate with the assessed business impact level of their compromise, Note i loss or damage.
Requirement 2. Security containers, cabinets and rooms Entities must assess security risks and select the appropriate containers, cabinets, secure rooms and strong rooms to protect entity information and assets.	Requirement 2. Security containers, cabinets and rooms Entities must assess security risks and select the appropriate containers, cabinets, secure rooms and strong rooms to protect entity information and assets.
Requirement 3. Disposal Entities must dispose of physical assets securely.	Requirement 3. Disposal Entities must dispose of physical assets securely.

Purpose

The purpose of this Policy is to detail the physical security measures the Office of the Australian Information Commissioner (OAIC) has in place to safeguard its people, information and assets.

Policy

It is the policy of the OAIC that appropriate physical security measures are implemented to minimise or remove the risk to its resources, commensurate with the assessed value of their compromise, loss or damage. Security risks will be assessed to ensure that the appropriate containers, cabinets, secure rooms and strong rooms are utilised to protect OAIC information and assets. The OAIC will ensure that prior to the disposal of any physical assets they are thoroughly inspected and if necessary, disposed of securely.

Procedures

Procedure 15-1-1: OAIC Asset Management Policy and Procedures - D2020/019572

References and associated policies

PSPF 15: Physical security for entity resources

Policy 15-2: Access control and identification cards

PSPF 15-2- Each entity must implement physical security measures that minimise or remove the risk of:

a. harm to people, and
b. information and physical asset resources being made inoperable or inaccessible, or being accessed, used or removed without appropriate authorisation.

And

	Supporting requirements
Requirement 1. Physical security measures	Physical security measures Entities must put in place appropriate physical security measures to protect entity resources, commensurate with the assessed business impact level of their compromise, Note loss or damage.
Requirement 2. Security containers, cabinets and rooms Entities must assess security risks and select the appropriate containers, cabinets, secure rooms and strong rooms to protect entity information and assets.	Requirement 2. Security containers, cabinets and rooms Entities must assess security risks and select the appropriate containers, cabinets, secure rooms and strong rooms to protect entity information and assets.
Requirement 3. Disposal Entities must dispose of physical assets securely.	Requirement 3. Disposal Entities must dispose of physical assets securely.

Purpose

This Policy sets out controls on access to the Office of the Australian Information Office (OAIC) and the use of keys, access cards, safe combinations by staff, contractors or visitors.

Policy

It is the policy of the OAIC that appropriate access control and identification measures to protect the OAIC resources, commensurate with the assessed business impact level of their compromise, are implemented.

Chief Security Officer (CSO) responsibility

The CSO has overall responsibility to ensure appropriate physical security measures to protect OAIC resources, commensurate with the assessed business impact level of its compromise.

This responsibility includes the adequacy of OAIC access, ID and Visitor ID processes. Consequently, the CSO is responsible for the authorisation of access for employees to areas within OAIC, including determining the level of employee access and the times they are authorised access to the premises and systems.

This includes:

- arrangements for the locking and alarming of OAIC facilities and property when not in use, including the issue of keys, access control cards and alarm Personal Identification Numbers (PINs), safe and cabinet combinations
- reprogramming alarm systems every six months or following the loss of alarm PINs, in the event of a breach or on advice from ASIO
- changing safe combinations every six months or in the event of a breach or on advice from ASIO
- security related clocks when a key is lost or in the event of a breach or on advice from ASIO
- authorising the replacement of lost access control cards and keys
- ensuring staff have the correct identification media (ID Card) for the OAIC
- the destruction of all returned identification media
- revoking the rights for returned access cards from the access control system
- revoking the rights for staff who have been transferred from the access control system
- providing access control logs of personnel to authorised personnel or organisations
- implementing Visitor processes including the issuing of Visitor ID
- auditing compliance.

The CSO may delegate responsibility for some or all of these actions to other suitable qualified and experienced officers.

Staff responsibility

All staff are responsible for wearing and displaying the appropriate ID and ensuring that visitors to the OAIC are issued with an appropriate ID and escorted at all times while on the OAIC premises.

Holders of keys (including access control cards), PINs and safe combinations will:

- sign for the item when it is issued or changed
- sign to acknowledge the return of the item when transferred to another department or if/when their employment is terminated

- immediately notify the CSO in case of loss (temporary or otherwise) or theft
- immediately notify the CSO in case of a compromised PIN or safe combination.

Procedures

Procedures 15-2-1: Access Control - D2020/019562

Procedure 15-2-2: Identity Cards - D2020/019573

References and associated policies

PSPF 3: Security planning and risk management

PSPF 8: Sensitive and classified information

PSPF 9: Access to information

PSPF 10: Safeguarding information from cyber threats

PSPF 11. Robust ICT systems

PSPF 14: Separating personnel

PSPF 15: Physical security for entity resources

PSPF 16: Entity facilities

Policy 15-3: Working remotely

PSPF 15 - Each entity must implement physical security measures that minimise or remove the risk of:

a. harm to people, and
b. information and physical asset resources being made inoperable or inaccessible, or being accessed, used or removed without appropriate authorisation.

Purpose

This Policy provides standards and guidance on good personnel security practice for remote working by staff of the Office of the Australian Information Commissioner (OAIC).

Definition

For this policy "remote working" is considered:

- **home working** - where the staff member works mainly in their own home, or in different places using their home as a base
- **mobile working** - working from any location including in hotels, work hubs or in transit
- **agile working** – dividing time, working from a main office and another location other than an Australian government place of work
- **teleworking or telecommuting** - working in a location that is separate from the OAIC by using telecommunication technologies

Policy

It is the policy of the OAIC that all personnel working remotely will apply security measures to assets, IT systems or information in their possession that are commensurate to those applied when working in the OAIC office. It is their responsibility to ensure that OAIC security culture and all procedures applied in the office of the OAIC are adhered to when working away from the office.

Procedures

Procedure 15-3-1: Working Remotely - D2020/019563

Chief Security Officer (CSO) responsibility

The CSO will ensure that staff undertaking remote working are aware of the security procedures relevant to the remote work and will ensure that appropriate security measures are implemented or modified to ensure the protection OAIC resources and information, commensurate with the assessed business impact level of their compromise.

The CSO will ensure the protection of OAIC staff and contractors by ensuring appropriate physical resources are available to staff who are working remotely.

References and associated policies

PSPF 3: Security planning and risk management

PSPF 14: Separating personnel

PSPF 15: Physical security for entity resources

PSPF 16: Entity facilities

Policy 16-1: Physical Security

PSPF 16 - Each entity must:

a. ensure it fully integrates protective security in the process of planning, selecting, designing and modifying its facilities for the protection of people, information and physical assets
b. in areas where sensitive or security classified information and assets are used, transmitted, stored or discussed, certify its facility's physical security zones in accordance with the applicable ASIO Technical Notes, and
c. accredit its security zones.

Purpose

This Policy describes the physical protections required to safeguard people, information, and assets (including ICT equipment) to minimise or remove security risk.

Policy

It is the policy of the OAIC that appropriate physical security measures are in place to protect OAIC resources, commensurate with the assessed business impact level of their compromise. When planning, selecting or designing and modifying its premises, the OAIC will ensure that where sensitive or security classified information and assets are used, transmitted, stored or discussed, those physical security zones will be certified in accordance with the applicable ASIO Technical Notes.

Procedures

Procedure 16-1-1: Duress Alarm - D2020/019564

Procedure 15-2-1: Access Control - D2020/019562

Procedure 3 - 1-1: Security Risk Management - D2020/019568

Prensa Lockdown Procedures - D2020/019565

Dexus Emergency Plan - D2020/019566

External links

ASIO T4 Protective Security Handbook

ASIO Technical Notes 1-15 Physical Security Zones- - Table 3 Physical protections for security zones - D2020/019627

Chief Security Officer (CSO) responsibility

The CSO has an overall responsibility to ensure the identification and implementation of appropriate physical security measures to protect OAIC resources commensurate with the assessed business impact level of their compromise. This is accomplished by:

- assessing security risks and select the appropriate containers, cabinets, secure rooms and strong rooms to protect entity information and assets
- ensuring that physical assets are disposed of securely
- identifying the people, information and assets that are critical to the ongoing operation of the entity and the national interest and apply appropriate protections to support core government business
- ensuring the protection of OAIC staff, contractors and visitors by ensuring compliance with the protective security elements of the Protective Security Policy Framework, the Work Health and Safety Act framework and other appropriate legislative requirements including:
  - identifying, protecting, and supporting employees under threat of violence, based on a threat and risk assessment of specific situations
  - reporting incidents to management, human resources, security, and law enforcement authorities is encouraged, as appropriate
  - providing information, training, and counselling to employees
  - maintaining thorough records and statements on reported incidents
- ensuring the protection of OAIC staff, contractors and visitors by implementing appropriate physical resources, such as successive layers or combinations of procedural and physical security measures.

References and associated policies

PSPF 3: Security planning and risk management

PSPF 14: Separating personnel

PSPF 15: Physical security for entity resources

PSPF 16: Entity facilities

Appendix A – Document Reference List

Governance Outcome procedures

s22 [redacted]

Procedure 2-1-1: Security Appointments – D2020/019569

Procedure 2-2-1: Security and Security Incident Reporting - D2020/019549

Procedure 3-1-1: Security Risk Management - D2020/019568

s22 [redacted]

Information Security Outcome procedures

s22 [redacted]

Procedure 9-2-1: Clean Desks - D2020/019555

Procedure 10-1-1: Information Security Assurance - D2020/019557

s22 [redacted]

Physical Security Procedures

Procedure 15-1-1: OAIC Asset Management Policy and Procedures - D2020/019572

Procedures 15-2-1: Access Control - D2020/019562

Procedure 15-2-2: Identity Cards - D2020/019573

Procedure 15-3-1: Working Remotely - D2020/019563

s22 [redacted]

Procedures including PSPF procedures.

Procurement Policy and Procedures (D2021/000849)

OAIC Information Management Policy (D2020/019571)

PSPF related plans and procedures

OAIC System Security Plan D2020/019556

OAIC Security Risk Management Plan D2017/003896

s22 [redacted]

Appendix B - External links

1. Australian Government Investigations Standards 2011
2. ASIO Outreach

Glossary

A glossary of common and complex terms used in this Policy Manual is presented below.

Term	Meaning
Accountable authority	The accountable authority of a Commonwealth entity is the person or group of persons responsible for, and with control over the entity's operations. This is set out in Section 12 of the *Public Governance, Performance and Accountability Act 2013* (Cth).
Alternative mitigation	Alternative security measures or controls that provide at least the same level of protection as the PSPF requirement and may exceed the required level of protection.
Authorised vetting agency	An Australian Government entity that is authorised to undertake security vetting and issue personnel security clearances. The Australian Government Security Vetting Agency (AGSVA) is the central vetting agency for the Australian Government. AGSVA can issue security clearances that are sponsored by any Australian Government entity There are six (6) non-corporate Commonwealth entities that are authorised to issue security clearances for their own personnel: • (AFP) • (ASIO) • (ASIS) • (ONI) • (DFAT) is authorised to issue security clearances at the Baseline, Negative Vetting 1 and Negative 2 levels • (ASIC) is authorised to issue security clearances at the Baseline level only.
Caveat owner	The entity that creates official records with special handling requirements that are in addition to the security classification. For more information see the *Sensitive Material Security Management Protocol (SMSMP).*
Chief Security Officer (CSO)	The Senior Executive Service (SES) level officer appointed by the accountable authority to be responsible for oversight of entity security arrangements across governance, information, personnel and physical security. Provisions for appointing a CSO in an entity with fewer than 100 employees are outlined in PSPF policy: Role of accountable authority.
Core requirement	The requirements that entities must meet to achieve the government's desired protective security outcomes. There are 16 policies, each of which includes a core requirement and supporting requirements.
Eligibility waiver	An accountable authority's decision to waive the citizenship or checkable background eligibility requirement of a candidate to hold a security clearance where there is an exceptional business requirement and after conducting a risk assessment.
Entity	Any Commonwealth entity listed under paragraph 10(1) of the *Public Governance, Performance and Accountability Act 2013 (Cth)*

Term	Meaning
Lead protective security entity	A Commonwealth entity with additional responsibilities as: a) lead entity in their portfolio. b) provider of government protective security advice, policy, technical standards or intelligence services, or c) provider of shared services arrangements.
Negative vetting	As part of the process for obtaining certain security clearances, this is an evaluation process that relies on the absence of information to the contrary in order to assess the subject's suitability for that security clearance.
Originator	The entity responsible for creating and classifying an official record where a record is as defined in the *Archives Act 1983(Cth)*. The entity remains the sole and permanent owner of the classification.
Outcomes	The protective security aims of the government relating to governance, people, information, and physical assets. The PSPF has four security outcomes for entities to achieve as part of the PSPF implementation.
Personal security file	A record of the checks undertaken, decisions undertaken, risk assessments, mitigations, conditions imposed and all other information relevant to a security clearance.
Personnel	Employees and contractors, including secondees and service providers engaged by the entity, and anyone given access to Australian government resources held by the entity as part of entity sharing initiatives.
Positive vetting	As part of the process for obtaining certain security clearances, this is a system of security checking that attempts to examine and independently verify all relevant aspects of a subject's suitability for a security clearance—positive vetting requires more extensive checks than negative vetting.
Protective security	The protection of information, people, and physical assets.
Principles	Fundamental values that guide decision-making. There are five principles that inform protective security settings (refer to Securing government business: Protective security guidance for executives).
PSPF maturity rating	The level to which an entity has addressed and implemented the core and supporting requirements as outlined in the PSPF. There are four levels of PSPF maturity.
Risk appetite	The risk an entity is willing to accept or retain within its tolerance levels in order to achieve its objectives, as defined in the *Department of Finance Risk Management Policy.*
Risk tolerance	An entity's tolerated levels of risk taking to achieve a specific objective or manage a category of risk, as defined in the *Department of Finance Risk Management Policy.*
Security advisors	Personnel appointed to perform security functions or specialist services related to security within an entity. These personnel support the work of

Term	Meaning
	the Chief Security Officer.
Security caveat	Indications of special handling requirements additional to those indicated by security classification. See *Australian Government Security Caveat Guidelines* for more detail.
Security culture	The characteristics, attitudes and habits within an organisation that establish and maintain security. Security culture is critical to supporting an entity to appropriately manage security risks.
Security Governance Committee	A senior committee that supports an accountable authority and CSO in achieving protective security objectives and monitoring performance against those objectives. This is especially valuable to entities with large or complex arrangements.
Security plan	Central document detailing how the entity plans to manage and address their security risks. For further detail see PSPF policy 3: Security planning and risk management.
Security maturity	The entity's capability to holistically and appropriately manage their security risks by effectively implementing and managing the PSPF core and supporting requirements in the context of the entity's specific risk environment and risk tolerances.
Security risk	Something that could result in compromise, loss, unavailability or damage to information or physical assets, and/or cause harm to people.
Security risk management	Managing risks related to an entity's information, people, and physical assets.
Security incident	A security incident is defined as an: a) **action**, whether deliberate, reckless, negligent or accidental that fails to meet protective security requirements or entity-specific protective security practices and procedures that results, or may result in the loss, damage, corruption or disclosure of official information or resources (see PSPF policy 2: Management structures and responsibilities C.7.1 Security incidents); b) **approach** from anybody seeking unauthorised access to official resources. c) observable **occurrence or event** (including natural disaster events, terrorist attacks etc) that can harm Australian Government people, information or assets. For further detail, see PSPF policy 2: Management structures and responsibilities. This also provides details about reporting channels for particular security incidents.
Security vetting	An assessment by an authorised vetting agency of a clearance subject's suitability to hold a security clearance.

Term	Meaning
Sponsoring entity	The Australian Government entity that sponsors an individual's security clearance.
Supporting requirement	The necessary actions to implement core requirements and attain the government's desired protective security outcomes. There are 16 policies which each include supporting requirements to support implementation of the policy's core requirement.
T4 Protective Security (T4 or ASIO T4)	ASIO's protective security capability (T4) provides expert protective security advice and training to the Australian Government, state and territory governments and business. This includes physical security certification advice (as defined in the PSPF), technical surveillance countermeasures, and resources for security managers to assist in the protection of their information, people, and assets via the ASIO Business and Government Liaison website. T4 evaluates protective security products (such as locks, alarms, and detection devices) to determine their suitability for use in government facilities. T4 provides protective security advice for Australian Government agencies. With the written approval of the Attorney-General, T4 can provide such services to, state and territory governments, business enterprises and critical infrastructure owners, provided that a Commonwealth interest can be shown.
Vetting	The evaluation of a person's suitability to obtain and maintain a security clearance and access sensitive and classified Australian Government resources.
Vetting entity	An authorised entity responsible for assessing a person's suitability to obtain and maintain a security clearance.
Vetting personnel	Vetting officers and delegates who assess a clearance subject and identify any vulnerabilities that may compromise Australian Government resources.

Acronyms

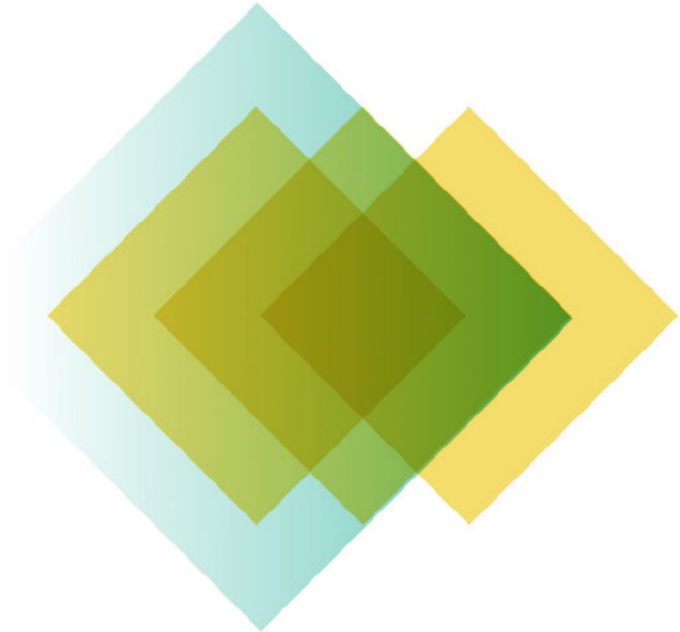
A list of acronyms used in this Policy Manual is presented below.

Acronym	Meaning
ACSC	Australian Cyber Security Centre
AFP	Australian Federal Police
AGSVA	Australian Government Security Vetting Agency
APS	Australian Public Service
APSC	Australian Public Service Commission
ASD	Australian Signals Directorate
ASIC	Australian Securities and Investments Commission
ASIO	Australian Security and Intelligence Organisation
ASIS	Australian Secret Intelligence Service
CSO	Chief Security Officer
DFAT	Department of Foreign Affairs and Trade
EACS	Electronic Access Control Systems
ISM	Information Security Manual
IRAP	Information Security Registered Assessor
OAIC	Office of the Australian Information Commissioner
ONI	Office of National Intelligence
PGPA Act	*Public Governance, Performance and Accountability Act 2013* (Cth)
PSPF	Protective Security Policy Framework
SCEC	Security Construction and Equipment Committee
SES	Senior Executive Service
SMSMP	Sensitive Material Security Management Protocol
TSCMs	Technical Surveillance Countermeasures

Australian Government

Office of the Australian Information Commissioner

Public Interest Disclosure Procedures



May 2024

Contents

I, Angelene Falk, Australian Information Commissioner, under s 59(3) of the *Public Interest Disclosure Act 2013* (Cth), establish these procedures for facilitating and dealing with public interest disclosures relating to the Office of the Australian Information Commissioner.

These procedures commence on: [Date][1]

[Signature]

Angelene Falk
Australian Information Commissioner

[Date]

[1] These procedures replace the OAIC's 2021 *Public Interest Disclosure Procedures*.

Version	Reviewer	Comments	Approved	Date
1.0		Version 1	Yes	November 2018
2.0				April 2021
3.0	A/g Chief Operating Officer	Amendments required by enactment of the *National Anti-Corruption Commission Act 2022* and the *PID Amendment (Review) Act 2023*		April 2024

1. Introduction

The Office of the Australian Information Commissioner (OAIC) is committed to a culture that encourages reporting of wrongdoing and inefficiency.

The OAIC's *Public Interest Disclosure Procedures* (Procedures) outline the OAIC's approach to managing matters which arise under the *Public Interest Disclosure Act 2013* (PID Act). This includes support and protection for public officials who report suspected wrongdoing. These procedures are established in accordance with section 59(3) of the PID Act for the OAIC.

The purpose of the PID Act is to provide a legislative scheme for the making of disclosures about serious wrongdoing in the Commonwealth public sector, investigating those disclosures, and protecting persons who make those disclosures (known as 'disclosers') and others from legal action and reprisals for disclosing.

These procedures:

- deal with the assessment of risks that reprisals may be taken in relation to disclosures under the PID Act (see section 5 below)
- provide for confidentiality of investigative processes (see section 3.4 below), and
- comply with standards in force under section 74(1) of the PID Act (*Public Interest Disclosure Standard 2013* [PID Standard]).

The OAIC is committed to the highest standards of ethical and accountable conduct. The OAIC encourages the reporting of wrongdoing under the PID Act, and will act on disclosures where appropriate and protect disclosers and others from any reprisals or threats of reprisals as a result of making a disclosure.

The operation of these procedures will be reviewed regularly to ensure their continued effectiveness.

2. What is a public interest disclosure?

Not all disclosures of information made to the OAIC will be public interest disclosures (PIDs) for the purposes of the PID Act. A disclosure of information will only be a PID if:

- it is made by a discloser – a current, former or deemed public official (see section 2.1 below)
- it is made to a supervisor of the discloser or to an authorised internal recipient (see section 2.2 below)
- the information tends to show, or the discloser believes on reasonable grounds that the information tends to show, one or more instances of disclosable conduct (see section 2.3 below), and
- the disclosure is not made in the course of performing the discloser's ordinary functions as a public official.

Only if each of the above requirements has been met will the disclosure be covered by the PID Act and the discloser have the benefit of the protections that it confers.

Accordingly, it is important that persons contemplating making a disclosure of information carefully review the contents of the PID Act and seek legal advice where appropriate in order to determine whether the disclosure can be made in a way that attracts the protections of the PID Act.

There are 5 kinds of PID:

1. internal, a PID made by a current or former public official to their supervisor or an authorised internal recipient, providing information that they believe tends to show, on reasonable grounds, disclosable conduct within an Australian Government agency or by a public official
2. external, a PID made by a current or former official to any person other than a foreign public official, providing information that they believe tends to show, on reasonable grounds, disclosable conduct within an Australian Government agency or by a public official. Further requirements apply in order for a disclosure to be considered an external PID, including that on a previous occasion, the discloser made an internal disclosure of information that consisted of, or included, the information now disclosed, the disclosure is not, on balance, contrary to public interest and no more information is publicly disclosed than is reasonably necessary to identify one or more instances of disclosable conduct. All requirements are set out in section 26 of the PID Act
3. emergency, a PID made by a current or former official to any person other than a foreign public official, providing information the discloser believes, on reasonable grounds, concerns a substantial and imminent danger to the health and safety of one or more persons or to the environment. Further requirements apply in order for a disclosure to be considered an emergency PID. All requirements are set out in section 26 of the PID Act
4. legal practitioner, a PID made by a current or former official to an Australian legal practitioner, made for the purpose of obtaining legal advice, or professional assistance, from the recipient in relation to the discloser having made, or proposing to make, a PID. Further requirements apply in order for a disclosure to be considered a legal practitioner PID. All requirements are set out in section 26 of the PID Act
5. National Anti-Corruption Commission (NACC) disclosures, a disclosure to the NACC which provides information about a corruption issue. See section 23 of the *National Anti-Corruption Commission Act 2022* (NACC Act).

These procedures focus on internal disclosures under the PID Act. Further information on other types of disclosures is available on the Commonwealth Ombudsman's website: Public interest disclosure (whistleblowing) | Commonwealth Ombudsman.

The full definition of 'public interest disclosure' is in section 26 of the PID Act.

2.1. Who is a public official?

A person must be a current, former or deemed public official to make a PID.

The term ‘public official’ is broadly defined in the PID Act and includes (but is not limited to):

- the principal officer of an agency (i.e. in the case of the OAIC, the Australian Information Commissioner (AIC))
- a member of staff of an agency (including an APS employee in the agency)
- a service provider under a Commonwealth contract, along with their officers and employees who provide services directly or indirectly for the purposes of the Commonwealth contract
- a statutory officeholder
- a person employed under the *Parliamentary Service Act 1999*
- a member of the Australian Defence Force
- an appointee of the Australian Federal Police (AFP), and
- a person deemed to be a public official by an authorised officer under section 70 of the PID Act.

Judicial officers, members of a Royal Commission, members of Parliament and persons employed or engaged under the *Members of Parliament (Staff) Act 1984* **are not** public officials for the purposes of the PID Act.

The full definition of ‘public official’ is in section 69 of the PID Act and the full definition of ‘principal officer’ is in section 73(1) (see item 10).

2.2. Who can a PID be made to?

A public official (or former public official) can make a PID to their supervisor (or manager) or to an ‘authorised internal recipient’ (an authorised officer at the agency to which the conduct relates, or an authorised officer at the agency to which the discloser belongs, or the Commonwealth Ombudsman [there are different requirements in relation to intelligence agencies and functions]).

A discloser’s ’supervisor’ is a public official who supervises or manages the person making the disclosure.

An ‘authorised officer’ is the principal officer of the agency (in the OAIC’s case, the AIC), or a public official who belongs to the agency and is appointed in writing by the principal officer of the agency.

The OAIC’s authorised officers are listed on the OAIC website, accessible at this link. Disclosures may be made by email to PID@oaic.gov.au or by post to GPO Box 5288, Sydney NSW 2001 marked ‘Confidential – PID’. The OAIC uses the above email address for PID matters only and restricts access to it to authorised officers.

If the PID relates to the conduct of another agency, it may be appropriate to make the PID to an authorised officer of that agency.

The principal officer of an agency is also an 'authorised officer' for the purposes of the PID Act, so a public official may also make a PID to the AIC.

If the discloser believes, on reasonable grounds, that it would be appropriate for the PID to be investigated by the Commonwealth Ombudsman – or if the PID is about the Ombudsman – then the PID should be made to the Ombudsman.

There are additional obligations for supervisors who receive PIDs (see section,4below).

For PIDs relating to intelligence agencies or agency's intelligence functions – the PID **must** be made to an authorised officer of the intelligence agency in question, the Inspector-General of Intelligence and Security ('IGIS') or to an investigative agency.

The full definition of 'authorised internal recipient' is in section 34 of the PID Act and the full definition of 'authorised officer' is in section 36.

2.3. What is disclosable conduct?

Disclosable conduct is conduct by:

- an agency (a Commonwealth entity or a prescribed authority)
- a public official in connection with their position (see section 2.1 above), or
- a contracted service provider for a Commonwealth contract (in connection with that contract)

if that conduct involves:

- illegal conduct
- corruption (including corrupt conduct)
- maladministration
- abuse of public trust
- fabrication, falsification, plagiarism or deception relating to scientific research
- wastage of public money or public property
- unreasonable danger, or increased risk of danger, to health and safety
- danger, or an increased risk of danger, to the environment
- a public official abusing their position
- conduct that could (if proved) give reasonable grounds for disciplinary action resulting in the termination of the public official's engagement or appointment, or
- any conduct prescribed by the PID Rules.

The full definition of ‘disclosable conduct’ is in section 29 of the PID Act.

Contracted service provider for a Commonwealth contract

A ‘contracted service provider for a Commonwealth contract’ is:

- a person who is a party to a Commonwealth contract, and is responsible for the provision of goods or services under that contract, or
- a subcontractor who is responsible under a subcontract for the provision of goods or services for the purposes (whether direct or indirect) of the Commonwealth contract.

A ‘Commonwealth contract’ does not include a grant covered by an instrument made under section 105C of the *Public Governance, Performance and Accountability Act 2013* (instruments relating to grants).

The full definition of ‘contracted service provider for a Commonwealth contract’ is set out in section 30 of the PID Act.

Corrupt conduct

A person can make a disclosure directly to the NACC providing information about a corruption issue which will be called a ‘NACC disclosure’ (the full definition of NACC disclosure is set out in section 23 of the NACC Act). A NACC disclosure is a PID (see section 26(1A)(c) of the PID Act).

Authorised officers (and PID investigators) must refer a PID which raises a corruption issue to the NACC if they received the PID in the course of their functions under the PID Act, the corruption issue concerns conduct of a person who is or was a staff member of the agency while that person is or was a staff member of that agency, and the authorised officer (or PID investigator) suspects the issue could involve serious or systemic corrupt conduct. More detail can be found in Part 5.4 of these Procedures.

Section 8(1) of the NACC Act states that each of the following is ‘corrupt conduct’:

- any conduct of any person (whether or not a public official) that adversely affects, or that could adversely affect, either directly or indirectly:
  - the honest or impartial exercise of any public official’s powers as a public official
  - the honest or impartial performance of any public official’s functions or duties as a public official
- any conduct of a public official that constitutes or involves a breach of public trust
- any conduct of a public official that constitutes, involves or is engaged in for the purpose of abuse of the person’s office as a public official, or

- any conduct of a public official, or former public official, that constitutes or involves the misuse of information or documents acquired in the person's capacity as a public official.

Conduct involving a public official may be corrupt conduct even if the conduct is not for the person's personal benefit.

2.4. What is not disclosable conduct?

The following **is not** disclosable conduct:

- disagreement with government policies or government action or expenditure
- certain conduct connected with courts, Commonwealth tribunals and intelligence agencies, or
- personal work-related conduct (subject to the exceptions set out below).

Personal work-related conduct

Personal work-related conduct is conduct (by act or omission) engaged in by a public official (the first official) in relation to another public official (the second official) that:

- occurs in relation to, or in the course of, either or both of the following:
  - the second official's engagement or appointment as a public official
  - the second official's employment, or exercise of functions and powers, and
- has, or would tend to have, personal implications for the second official.

The following are some examples of personal work-related conduct:

- conduct relating to an interpersonal conflict between the first official and the second official (including, but not limited to, bullying or harassment)
- conduct relating to the transfer or promotion of the second official
- conduct relating to the terms and conditions of engagement or appointment of the second official
- disciplinary action taken in relation to the second official
- the suspension or termination of the second official's employment or appointment as a public official, or
- conduct in relation to which the second official is, or would have been, entitled to review under section 33 of the *Public Service Act 1999* (Public Service Act).

Personal work-related conduct will be disclosable conduct if the conduct:

- would constitute taking a reprisal against another person
- would constitute an offence against section 19 of the PID Act, or

- is of such a significant nature that it would undermine public confidence in an agency (or agencies) or has other significant implications for an agency (or agencies).

The full definition of 'personal work-related conduct' is in section 29A of the PID Act. Sections 31, 32 and 33 of the PID Act provide more detail about conduct that **is not** disclosable conduct.

Other mechanisms to report and resolve issues relating to conduct

The OAIC has other mechanisms for public officials to report and resolve some of the above types of conduct. For example, in relation to grievances relating to an employee's own employment there are:

- Suspected Breaches of the APS Code of Conduct Procedures
- Work Health and Safety Policy
- Talking about performance (TAP): forms and templates
- Appropriate Workplace Behaviours policy

3. Making an internal disclosure under the PID Act

3.1. How do you make an internal disclosure under the PID Act?

Where a public official is considering making a PID they may wish to, in the first instance, contact an authorised officer to get information about making a disclosure under the PID Act.

A PID may be made by a public official to their supervisor or to an authorised internal recipient (see section 2.2 above):

- orally or in writing
- anonymously or openly, and
- with or without the discloser asserting that the disclosure is made for the purposes of the PID Act – a PID may be made even without the discloser knowing about the PID Act.

Where possible, OAIC officials are encouraged to make a PID to an authorised officer rather than to their supervisor (or manager) because of the additional training given to authorised officers in the OAIC. This paragraph does not prevent an OAIC official from making a PID to their supervisor or manager.

To make a PID in writing, OAIC officials have the option of emailing PID@oaic.gov.au. The OAIC also maintains a list of current authorised officers which can be accessed here. OAIC officials or former officials can make a PID directly to one of the authorised officers.

Once a PID has been made it cannot be withdrawn, but a discloser may tell the authorised officer that they do not want the PID to be investigated. This will be a relevant consideration in the investigator deciding whether or not to investigate the PID.

A person who is considering making a PID should be aware that making a PID does not entitle them to protection from the consequences of their own wrongdoing.

A disclosure made in the course of performing the discloser's ordinary functions as a public official is not a PID.

3.2. What information should be provided when making a PID?

The information contained in a PID should be clear and factual, and should, as far as possible, avoid speculation, personal attacks and emotive language. It should contain supporting evidence where available to the discloser and should, where possible, identify any witnesses to the disclosable conduct.

A public official making a PID may wish to include the following details:

- their name and contact details (but they do not have to do this, and they can use a pseudonym instead of their real name)
- the details of the suspected wrongdoing
- the name of the person or entity who they believe committed the suspected wrongdoing
- the place, time and date of the suspected wrongdoing
- whether the suspected wrongdoing has been reported to anyone else
- whether there were any witnesses to the wrongdoing, and if so, who the witnesses are, and
- whether they have any concerns that anyone might take reprisal action against them for having made the PID.

A discloser who knowingly makes a false or misleading statement or knowingly contravenes a designated publication restriction without reasonable excuse in a PID **will not** have immunity from civil, criminal or administrative liability under the PID Act (see section 3.6 below for further information on disclosers' immunity from liability).

3.3. How are anonymous disclosures dealt with?

A discloser may wish to make an anonymous disclosure. A disclosure is anonymous if the identity of the discloser is not revealed and if no contact details for the discloser are provided. It is also anonymous if the discloser does not disclose their name but provides anonymous contact details. Providing a de-identified email address for correspondence will allow the authorised officer or AIC (or delegate) to contact the discloser anonymously where required.

Receiving an anonymous disclosure does not mean that it cannot be treated as a disclosure for the purposes of the PID Act. However, the disclosure will only be a PID if the discloser is a public official (see section 2.1 above).

Where a supervisor (or manager) receives an anonymous disclosure for the purposes of the PID Act they **must** refer it to an authorised officer as soon as reasonably practicable.

3.4. What are the confidentiality obligations under the PID Act?

The OAIC's authorised officers and the AIC (or delegate), and any other persons who are aware of a PID, should take all reasonable steps to protect the identity of a public official who has made a PID for the purposes of the PID Act.

Only individuals directly involved in dealing with the PID (such as the authorised officer and the AIC, and any persons assisting them) may be advised of the details of the PID. These individuals **must** not disclose the identity of the discloser or any information which is likely to reveal the identity of the discloser (identifying information) without the consent of the discloser or where permitted under the PID Act.

Any interviews conducted for the purpose of an investigation under the PID Act should be conducted in private and avoid the identification of the discloser by other staff of the OAIC.

A person commits an offence if they disclose or use identifying information about a discloser, **unless** one or more of the following applies:

- the disclosure or use is for the purposes of the PID Act – that is for the purpose of providing assistance in relation to a PID, providing legal advice, or other professional assistance in relation to a PID, or in the performance or exercise (or purported performance or exercise) of a function or power conferred by the PID Act
- the disclosure or use is in connection with the performance of the Commonwealth Ombudsman's functions or the IGIS's functions
- the disclosure or use is for the purposes of a law of the Commonwealth of Australia or a prescribed law of an Australian State or a Territory
- the person likely to be identified by the information has consented to the disclosure or use of the information, or acted in a way that is inconsistent with keeping that person's identity confidential, or
- the information has previously been lawfully published.

Identifying information about a discloser is not required to be disclosed to a court or tribunal except where it is necessary to do so for the purposes of giving effect to the PID Act.

The offences regarding the use or disclosure of identifying information are set out in sections 20 and 21 of the PID Act.

3.5. What are the recordkeeping obligations?

Where an authorised officer or the AIC (or delegate) is required to keep a record under these procedures, the record **must** be kept in hard copy or electronic form or both. Access to these records **must** be restricted to only those officers who require access in order to perform some function under the PID Act or for the purposes of another law of the Commonwealth (for example, under the *Work Health and Safety Act 2011* or the Public Service Act).

Appropriate written records **must** be kept of the allocation decision (see section 5 below) and of the investigation (see section 6.3 below).

3.6. What protections and support are available under the PID Act?

Protection against reprisals

The PID Act provides a range of protections for persons who make a PID and others who may be affected. Chief among these is that reprisal action cannot be taken or threatened against a discloser or any other person (for example, a witness) because of a PID.

Reprisal occurs when someone causes, by an act or omission, detriment to another person because they believe or suspect that person, or anyone else, may have made, intends to make, or could make a PID. This could include an action or omission (or threat of action or omission), or detriment, that results in:

- disadvantage to a person, including dismissal, injury in their employment, discrimination between them and other employees or alteration of their position to their disadvantage
- a physical or psychological injury, including a stress-related injury
- intimidation, harassment or victimisation
- loss or damage to property, or
- disadvantage to a person’s career (for example, denying them a reference or a promotion without appropriate reasons).

It is a criminal offence to take or threaten to take a reprisal action against anyone in relation to a PID and the penalty is up to two years imprisonment. An OAIC official who commits a reprisal action may also be subject to disciplinary procedures, for example for breaching the Australian Public Service Code of Conduct.

The AIC **must** take reasonable steps to protect public officials against reprisals that have been, or may be, taken in relation to PIDs that have been made, may have been made, are proposed to be made or could be made to an authorised officer or supervisor belonging to the OAIC. This firstly requires that the authorised officers or Commissioner undertake an assessment of the risk of reprisals against the discloser or anyone related to a PID.

Following the reprisal risk assessment, a strategy for providing an appropriate level of support will be developed by the authorised officer (see section 5.2 below).

A person **does not** take a reprisal against another person to the extent that the person takes administrative action that is reasonable to protect the other person from detriment.

What constitutes 'taking a reprisal' is set out in section 13 of the PID Act.

Disclosers' immunity from liability

If an individual makes a PID they are not subject to any civil, criminal or administrative liability (including disciplinary action) for making the PID and no contractual or other remedy may be enforced, and no contractual or other right may be exercised, against the individual on the basis of the PID (it should be noted that this immunity applies where an individual makes any of the 5 types of PID – see section 2 above).

The discloser has absolute privilege in proceedings for defamation in respect of the PID, and a contract to which the discloser is a party **must not** be terminated on the basis that the PID constitutes a breach of the contract.

However, these immunities do not apply if the discloser:

- makes a statement which they know is false or misleading
- commits an offence under specific sections of the Criminal Code by:
  - providing false or misleading information
  - giving false or misleading documents
  - making a false document
  - using a forged document, or
- contravenes a 'designated publication restriction' (for example, a court or Tribunal order to protect the identity of people) if they know the PID contravenes that restriction and do not have a reasonable excuse for that contravention (see the definition of 'designated publication restriction' in section 8).

If a discloser provides information that relates to their own conduct, their liability for that conduct **is not** affected.

The details of the immunity from liability for disclosers are set out in sections 10, 11, 11A and 12 of the PID Act.

Witnesses' immunity from liability

An individual is a 'witness' if they provide assistance in relation to a PID, if they give information or produce a document or other thing, or answer a question, that they consider on reasonable grounds to be relevant to:

- the making of a decision in relation to the allocation of a PID
- a PID investigation or a proposed PID investigation, or
- a review or proposed review by the Commonwealth Ombudsman or the IGIS.

A witness is not subject to any civil, criminal or administrative liability (including disciplinary action) because of the assistance provided. No contractual or other remedy may be enforced, and no contractual or other right may be exercised, against the witness on the basis of the assistance provided.

A witness has absolute privilege in proceedings for defamation in respect of the assistance provided, and a contract to which the witness is a party **must not** be terminated on the basis that the assistance provided constitutes a breach of the contract.

However, these immunities **do not apply** if the witness:

- makes a statement which they know is false or misleading
- commits an offence under specific sections of the *Criminal Code* by:
  - providing false or misleading information
  - giving false or misleading documents
  - making a false document
  - using a forged document, or
- contravenes a designated publication restriction (see the definition of ‘designated publication restriction’ in section 8).

If a witness provides information that relates to their own conduct, their liability for that conduct **is not** affected.

The details of the immunity from liability for witnesses are set out in sections 12A and 12B of the PID Act.

Good faith exemption for officers involved in PID processes

The AIC (or delegate), an authorised officer, a supervisor (or manager) of a person who makes a PID, or a person assisting the AIC (or delegate) is not liable to any criminal or civil proceedings, or any disciplinary action (including any action that involves imposing any detriment), for or in relation to an act or matter done, or omitted to be done, in good faith:

- in the performance, or purported performance, of any function conferred on the person by the PID Act
- in the exercise, or purported exercise, of any power conferred on the person by the PID Act, or
- in the case of a person assisting the AIC (or delegate) — in assisting the AIC (or delegate) in performing any function or exercising any power under the PID Act.

This exemption does not apply to a breach of a designated publication restriction (see the definition of ‘designated publication restriction’ in section 8).

The details of this good faith exemption are in section 78 of the PID Act.

Support for public disclosers

The OAIC has a number of support mechanisms available to disclosers, including but not limited to the Employee Assistance Program, the OAIC People and Culture team and the OAIC’s Harassment Contact Officers.

Regardless of the outcome of any risk reprisal assessment, the authorised officer, investigator, manager or supervisor will take all reasonable steps to protect public officials who have made a disclosure from detriment or threats of detriment.

This may include taking one or more of the following actions:

- if the discloser wishes, appointing a support person to assist the discloser who is responsible for checking on the wellbeing of the discloser regularly
- informing the discloser of the progress of the investigation
- advising the discloser of the availability of the Employee Assistance Program
- advising the discloser of the role and responsibilities of the OAIC's Harassment Contact Officers, whose job it is to provide support and information to people who believe they are being harassed.
- where there are any concerns about the health and wellbeing of the discloser, liaising with the OAIC's People and Culture team
- transferring the discloser to a different area within the workplace.

4. Procedures for supervisors receiving a disclosure

A 'supervisor' is a public official who supervises or manages the public official making the disclosure. This can be the discloser's direct supervisor or another person up the line of reporting. A supervisor (or manager) who receives a disclosure of disclosable conduct (see section 2.3 above) from a public official is required under the PID Act to take the following steps.

Where a public official discloses information to their supervisor or manager (who is not an authorised officer) and the supervisor (or manager) has reasonable grounds to believe that the information concerns, or could concern, disclosable conduct they **must**:

- inform the discloser that the disclosure could be treated as a PID
- explain to the discloser that the procedures under the PID Act require:
  - the supervisor (or manager) to give the disclosure to an authorised officer
  - the authorised officer to decide whether to allocate the disclosure to the AIC or to another agency, and
  - if the PID is allocated, the principal officer (or delegate) must investigate it
- advise the discloser about the circumstances (if any are applicable) in which a disclosure must be referred to another agency or person under another law of the Commonwealth
- explain to the discloser the protections under the PID Act (see section 3.6 above), and
- as soon as reasonably practicable after the disclosure is made, give the information to an authorised officer.

The supervisor (or manager) should also seek the discloser's consent to provide the authorised officer with the discloser's identity. If the discloser declines, the supervisor (or manager) will need provide the authorised officer with as much information as possible, without revealing the discloser's identity and will need to conduct the reprisal risk assessment (see section 5.2 below).

If the disclosure is not in writing, the supervisor or manager must make a written record of the substance of the disclosure and of the time and date of the disclosure, and ask the discloser to sign the written record of the disclosure (where this is practicable).

The obligations of supervisors are set out in section 60A of the PID Act.

5. Procedures for authorised officers receiving and allocating a disclosure

An authorised officer who receives a disclosure of disclosable conduct (see section 2.3 above) from a public official must deal with the disclosure in accordance with the PID Act, PID Standard and these procedures.

5.1. Receiving a disclosure

Where:

- an individual discloses, or proposes to disclose, information to an authorised officer, which the authorised officer has reasonable grounds to believe may be disclosable conduct (see section 2.3 above), and
- the authorised officer has reasonable grounds to believe that the person may be unaware of the consequences of making the disclosure,

the authorised officer **must**:

- inform the individual that the disclosure could be treated as an internal disclosure for the purposes of the PID Act
- explain what the PID Act requires in order for the disclosure to be an internal disclosure (see section 2 above)
- advise the individual about the circumstances (if any) in which a PID must be referred to an agency, or other person or body, under another law of the Commonwealth, and
- advise the individual of any orders or directions of which the authorised officer is aware that are designated publication restrictions that may affect disclosure of the information.

If the disclosure is not in writing, the authorised officer must make a written record of the substance of the disclosure and of the time and date of the disclosure, and ask the discloser to sign the written record of the disclosure (where this is practicable).

The authorised officer should ensure that they do not have an actual or perceived conflict of interest in making any decisions about the disclosure including whether or not to allocate the disclosure. A conflict of interest could arise, for example, where information suggests they or a family member of the discloser or persons against whom allegations are made or are implicated in the alleged wrongdoing the subject of the disclosure.

5.2. Conducting a reprisal risk assessment

An authorised officer must conduct a risk assessment of the risk of reprisals being taken against the discloser (and other public officials who belong to the OAIC, if applicable) as a result of the PID. This should be conducted as soon as possible after a potential PID is received by an authorised officer.

If the disclosure is first made to a supervisor (or manager) then the authorised officer may ask the supervisor (or manager) for further assistance in carrying out the risk assessment.

Reprisal risk **must** be assessed in all cases however the way in which a risk assessment is conducted may vary depending on the circumstances. The risk assessment can include the risk of direct reprisal against the discloser and the risk of related workplace conflict or difficulties.

Early and open communication with the discloser is critical. Sensitivity needs to be applied in talking about the risks with the discloser. The authorised officer conducting the risk assessment should be alert to the possibility that the discloser may feel that the discussion of reprisal risk is intended to discourage them from proceeding with their disclosure. As part of the risk assessment, any concerns of the discloser about the reprisal risks should be discussed with them and addressed, taking into account all of the circumstances. The discloser should also be informed of the protections afforded to them under the PID Act (see section 3.6 above).

The following framework may be used for assessing the risk of reprisals being taken:

- **Identifying the risks** – the authorised officer should identify the risk factors relating to the particular disclosure, taking into account the individual and organisational circumstances. Some risk factors may include (but are not limited to) those listed in the first column of the table below. Considerations for the risk assessment are listed in the second column:

Threats or past experience	• Has a specific threat against the discloser been received? • Is there a history of conflict between the discloser and the subjects of the disclosure, management, supervisors or colleagues? • Is there a history of reprisals or other conflict in the workplace?

	• Is it likely that the disclosure will exacerbate this?
Confidentiality unlikely to be maintained	• Who knows that the disclosure has been made or was going to be made? • Has the discloser already raised the substance of the disclosure or revealed in the workplace their disclosure or intention to make a disclosure? • Who in the workplace is aware of the actual or intended disclosure and/or the discloser's identity? • Is the discloser's immediate work unit small? • Are there circumstances, such as the discloser's stress level, that will make it difficult for them to not discuss the matter with people in their workplace? • Will the discloser become identified or suspected when the existence or substance of the disclosure is made known or investigated? • Can the disclosure be investigated while maintaining confidentiality?
Significant reported wrongdoing	• Are there allegations about individuals in the disclosure? • Who are those individuals' close professional and social associates within the workplace? • Is there more than one wrongdoer involved in the matter? • Is the reported wrongdoing serious? • Is the disclosure particularly sensitive or embarrassing for any

	subjects of the disclosure, senior management, the agency or the Government? • Do these people have the intent to take reprisals—for example, because they have a lot to lose? • Do these people have the opportunity to take reprisals—for example, because they have power over the discloser?
Vulnerable discloser	• Is or was the reported wrongdoing directed at the discloser? • Are there multiple subjects of the disclosure? • Is the disclosure about a more senior officer? • Is the discloser employed part time or on a casual basis? • Is the discloser isolated—for example, geographically or because of shift work? • Are the allegations unlikely to be substantiated—for example, because there is a lack of evidence? • Is the disclosure being investigated outside your organisation?

- **Assessing the risks** – the authorised officer should consider the likelihood and consequence of reprisal or related workplace conflict occurring. For example, the likelihood of a risk may be high where threats have been made, there is already conflict in the workplace or the discloser's identity would be obvious because of the nature of the disclosure.
- **Controlling the risks** – the authorised officer should identify strategies to be put in place to prevent or contain reprisals or related workplace conflict. Any decision affecting the discloser should be made in consultation with them and should be reasonable and appropriate in all of the circumstances.

- **Monitoring and reviewing the risk management process** – the risk assessment should be monitored, reviewed and updated as circumstances change throughout the course of the investigation.

Regardless of the outcome of the risk assessment, if it has been determined that a discloser will require support, the authorised officer should develop a strategy for providing an appropriate level of support. This may include taking one or more of the following actions:

- with the discloser's consent, appointing a support person to assist the discloser, who is responsible for checking on the wellbeing of the discloser regularly
- informing the discloser of the progress of the investigation
- advising the discloser of the availability of the Employee Assistance Program and access to workplace Harassment Contact Officers, and
- where there are any concerns about the health and wellbeing of the discloser, liaising with officers responsible for health and safety in the OAIC.

If the situation is serious enough, protecting the discloser may require significant action such as a transfer, relocation, a leave of absence, physical protection or an injunction.

For further information on carrying out reprisal risk assessments, see the Commonwealth Ombudsman's *Agency Guide to the Public Interest Disclosure Act 2013*: www.ombudsman.gov.au.

5.3. Allocating a disclosure

An authorised officer who receives a disclosure (either directly from the discloser or from the discloser's supervisor) **must** either:

- allocate the disclosure to one or more agencies, or
- decide not to allocate the disclosure to any agency if they are satisfied, on reasonable grounds, that:
  - there is no reasonable basis on which the disclosure could be considered an internal disclosure (see section 2 above), or
  - the conduct disclosed would be more appropriately investigated under another Commonwealth law or power.

The authorised officer **must** use their best endeavours to make a decision about the allocation of the disclosure **within 14 days** of the disclosure being made or given to the officer. This 14-day period is subject to any stop action direction issued under the NACC Act to stop taking action in relation to a corruption issue.

Deciding whether or not to allocate the disclosure

An authorised officer who receives a disclosure must allocate the disclosure to the AIC or a principal officer of another agency **unless**:

- they are satisfied, on reasonable grounds, that there is no reasonable basis on which the disclosure could be considered an internal disclosure – the grounds on which an authorised officer could be satisfied of this include that:
  - the disclosure has not been made by a person who is, or was, a public official (see section 2.1 above)
  - the disclosure was not made to an authorised internal recipient or supervisor (see section 2.2 above)
  - the disclosure does not include disclosable conduct (see section 2.3 above)
  - the person who is alleged to have carried out the disclosable conduct was not a public official at the time that they are alleged to have carried out that conduct, or
  - the disclosure is not otherwise a PID within the meaning of the PID Act, or
- the conduct would be more appropriately investigated under another Commonwealth law or power.

In making a decision about allocation, the authorised officer **must** have regard to the following considerations:

- generally, an agency should not handle a PID unless some or all of the conduct disclosed relates to that agency (i.e. generally the OAIC should not handle the PID if it does not relate to the OAIC)
- any other matters the authorised officer considers relevant, including:

if another agency in the same portfolio would be better able to handle the PID (for example, the Attorney-General's Department),the authorised officer may allocate the PID to another agency in the same portfolio as the recipient agency if they consider that the other agency would be better able to handle the PID. However, the allocation may not be made to another agency unless an authorised officer in that agency consents to the allocation

  - any recommendation made by the Commonwealth Ombudsman or the IGIS about the allocation of the PID, and

- whether the obligations in section 60(1) of the PID Act (Additional obligations of authorised officers) has been satisfied in relation to the PID.

The authorised officer may obtain information from such persons, and make such inquiries, as the authorised officer thinks fit, in order to make a decision about the allocation of the disclosure.

A disclosure that includes information relating to a number of instances of conduct, some of which may be considered disclosable conduct, and some of which may not (for example, because that conduct is personal work-related conduct) must still be allocated.

If the information disclosed concerns conduct alleged to be related to an intelligence agency, Australian Criminal Intelligence Commission (ACIC) or the Australian

Federal Police (in respect of their intelligence functions) then the IGIS must be notified and the process in section 45A of the PID Act **must** be followed.

The requirements for making a decision about allocating a disclosure are set out in section 43 of the PID Act.

Decision not to allocate

Where an authorised officer decides **not to allocate** a disclosure to any agency, they **must**, as soon as reasonably practicable, give written notice to:

- the discloser (if reasonably practicable) of:
  - the decision
  - the reasons for the decision
  - any action the authorised officer has taken or proposes to take to refer the conduct for investigation under another Commonwealth law or power (if any), and
  - any courses of action that might be available to the discloser under another Commonwealth law or power (if any), and
- the Commonwealth Ombudsman (unless the conduct disclosed relates to an intelligence agency, or ACIC or the AFP in relation to that agency's intelligence functions) of:
  - the decision
  - the reasons for the decision, and
  - any action the authorised officer has taken or proposes to take to refer the conduct for investigation under another Commonwealth law or power (if any).

If the conduct disclosed relates to an intelligence agency, or ACIC or the AFP in relation to that agency's intelligence functions, the authorised officer **must** also give written notice to the IGIS.

The authorised officer must keep an appropriate written record of the following:

- the decision
- the reasons for the decision
- whether the notice (or a copy of the notice) of the decision not to allocate was given to the discloser, and if not, why not, and
- if the notice (or a copy of the notice) of the decision not to allocate was given to the discloser – the following matters:
  - the day and time the notice (or copy) was given to the discloser
  - the means by which the notice (or copy) was given to the discloser, and
  - the matters included in the notice.

The requirements for the notice of a decision to not allocate a disclosure are set out in section 44A of the PID Act. The requirements for written records are set out in section 6 of the PID Standard.

Decision to allocate

Where an authorised officer decides **to allocate** a disclosure (to the AIC or to another agency) they **must**, as soon as reasonably practicable, give written notice to:

- the principal officer of each agency to which the PID is allocated (so where an authorised officer decides to allocate an internal public interest disclosure to the OAIC for handling, the authorised officer must give notice of the allocation to the Information Commissioner), and
- the Commonwealth Ombudsman (or to the IGIS if the PID is allocated to an intelligence agency or ACIC or the AFP, in relation to their intelligence functions).

The notice **must** include the following matters:

- the allocation to the agency
- the information that was disclosed
- the conduct disclosed, and
- the discloser's name and contact details (if these are known to the authorised officer and the discloser consents to these details being provided).

If reasonably practicable, the authorised officer must give a copy of the notice to the discloser as soon as reasonably practicable.

The authorised officer should also ask the discloser whether they consent to the officer giving the discloser's name and contact details to the AIC (or to the principal officer of another agency if the PID is allocated to another agency).

The IGIS must also be notified if the PID is allocated to an intelligence agency, ACIC or the AFP in relation to that agency's intelligence functions.

The authorised officer **must** keep an appropriate written record of the following:

- the decision (including the name of each agency to which the PID is to be allocated)
- the reasons for the decision
- if the PID has been allocated to another agency — the consent given by an authorised officer in the agency to which the PID is allocated
- whether the notice (or a copy of the notice) of the decision to allocate was given to the discloser, and if not, why not and
- if the notice (or a copy of the notice) of the decision to allocate was given to the discloser – the following matters:

  - the day and time the notice (or copy) was given to the discloser
  - the means by which the notice (or copy) was given to the discloser, and
  - the matters included in the notice.

The requirements for the notice of a decision to allocate a PID are set out in section 44 of the PID Act. The requirements for written records are set out in section 6 of the PID Standard.

Reallocation of PIDs

The authorised officer may, after making a decision to allocate a PID, decide to reallocate the PID to one or more agencies (which may include an agency to which the PID had formerly been allocated). The processes set out above must be followed if a decision is made to reallocate the PID.

5.4. Mandatory referral to the NACC

In addition to considering whether or not to allocate the disclosure, the authorised officer **must** consider whether the PID involves a 'corruption issue', as defined in s 9 of the NACC Act. A 'corruption issue' involves 'corrupt conduct', as defined in s 8 of the NACC Act and set out above in Part 2.3.

A staff member includes an agency head, employees, contracted service providers for Commonwealth contracts and their employees and officers, secondees, statutory officeholders, and others performing functions under a Commonwealth law (see section 12 of the NACC Act).

If the authorised officer, in the course of dealing with a PID, becomes aware of a corruption issue that:

- concerns the conduct of a person who is, or was, a staff member of the OAIC while that person is, or was a staff member, and
- the authorised officer suspects it could involve corrupt conduct that is serious or systemic,

they **must** refer the PID to the National Anti-Corruption Commissioner (the NACC Commissioner) as soon as reasonably practicable. The authorised officer must inform the discloser of the referral as soon as reasonably practicable after the referral.

An authorised officer is not required to provide information to the NACC Commissioner if:

- the authorised officer has reasonable grounds to believe that the NACC Commissioner is already aware of the information, or
- the NACC Commissioner has advised the authorised officer that the provision of information about the corruption issue is not required.

The NACC Commissioner may direct an agency head (including the AIC) to stop the agency taking specified action, including allocating the PID.

If the authorised officer does not allocate the PID because of a stop action direction under the NACC Act, the authorised officer must, as soon as reasonably practicable:

- give written notice to the Commonwealth Ombudsman (or the IGIS regarding intelligence agencies and functions) of:
  - the information that was disclosed
  - the conduct disclosed
  - if the discloser's name and contact details are known to the authorised officer, and the discloser consents to the Commonwealth Ombudsman (or IGIS) being informed—the discloser's name and contact details, and
  - the stop action direction under the NACC Act that prevents allocation of some or all of the PID, and
- inform the discloser and give the discloser a copy of the notice if the AIC (or delegate) considers that it is reasonably practicable or appropriate to do so.

The authorised officer **must** keep an appropriate written record of the following:

- details of the direction, including when the direction was made and when the stop action direction no longer applies, and
- whether the AIC (or delegate) considers that it is reasonably practicable or appropriate for the discloser to be given a copy of the notice (and whether the discloser was given a copy of the notice).

The above requirements for written records are set out in section 6 of the PID Standard.

Even where a referral is made to the NACC, the authorised officer (or PID investigator) should continue to handle a disclosure in line with obligations under the PID Act, unless a stop action direction has been issued under section 43(1) of the NACC Act. If a stop action direction is issued but subsequently revoked, the timeframes stipulated under the PID Act recommence from the date the authorised officer (or PID investigator) becomes aware that a stop action direction no longer applies.

The NACC Act and the PID Act offer different protections to disclosers. The NACC Act protections are available to any person who provides information or evidence related to a corruption issue to the Commission. Importantly, a public official will be able to access protections under both schemes where the information or evidence disclosed to the Commission also constitutes disclosable conduct under the PID Act.

6. Procedures for investigating an internal disclosure

The AIC (or delegate) must, as soon as reasonably practicable, after being allocated a PID decide whether to:

- investigate the PID
- not investigate the PID further, or

- investigate the PID under another Commonwealth law or power.

If the NACC Commissioner issues a stop action direction under the NACC Act, which prevents the investigation of some or all of the PID, the AIC must inform the Commonwealth Ombudsman of the stop action direction (or the IGIS, if the PID concerns conduct relating to an intelligence agency, the IGIS, or ACIC or the AFP in relation to those agencies' intelligence functions).

The AIC (or delegate) **must**, as soon as reasonably practicable, give written notice to the discloser stating:

- information about the AIC's powers to:
  - decide not to investigate the PID
  - decide not to investigate the PID further, or
  - decide to investigate the PID under a separate investigative power.

The AIC (or delegate) must ensure that, where it is reasonably practicable to do so, the discloser is given the above information **within 14 days** after the PID is allocated to the agency.

6.1. Deciding whether or not to investigate

The AIC (or delegate) **may decide not to investigate** the PID, or (if the investigation has started) not to investigate further if one of the following considerations apply:

- the discloser is not, and has not been, a public official (see section 2.1 above)
- the information does not, to any extent, concern serious disclosable conduct (see section 2.3 above)
- the PID is frivolous or vexatious
- the information is the same, or substantially the same, as information previously disclosed under the PID Act, and:
  - a decision was previously made not to investigate the earlier PID further or at all, or
  - the earlier PID has been, or is being, investigated as a PID investigation
- the conduct disclosed, or substantially the same conduct, is being investigated under another Commonwealth law or power, and the AIC (or delegate) is satisfied, on reasonable grounds, that it would be inappropriate to conduct an investigation under the PID Act at the same time
- the conduct disclosed, or substantially the same conduct, has been investigated under another Commonwealth law or power, and the AIC (or delegate) is satisfied, on reasonable grounds, that there are no further matters concerning the conduct that warrant investigation

- the AIC (or delegate) is satisfied, on reasonable grounds, that the conduct disclosed would be more appropriately investigated under another Commonwealth law or power (that the conduct disclosed raises a corruption issue is not sufficient alone for this)
- the AIC (or delegate) has been informed that the discloser does not wish the investigation of the PID to be pursued and the AIC (or delegate) is satisfied, on reasonable grounds, that there are no matters concerning the PID that warrant investigation, or
- it is impracticable for the PID to be investigated because:
  - the discloser's name and contact details have not been disclosed
  - the discloser refuses or fails, or is unable, to give, for the purposes of the investigation, such information or assistance as the person who is or will be conducting the investigation asks the discloser to give, or
  - of the age of the information.

The circumstances where the principal officer may decide not to investigate a PID are set out in section 48 of the PID Act.

6.2. Decision not to investigate

Discloser and Commonwealth Ombudsman must be notified

If the AIC (or delegate) has decided not to investigate the PID (or not to investigate the PID further) they must, as soon as reasonably practicable, give written notice to the discloser (if contacting the discloser is reasonably practicable) and to the Commonwealth Ombudsman stating that:

- the AIC (or delegate) has decided not to investigate the PID (or not to investigate the PID further)
- the reasons for that decision, and
- if the AIC (or delegate) has taken action, or proposes to take action, in relation to the referral of the conduct disclosed for investigation under another Commonwealth law or power, details of:
  - the other Commonwealth law or power
  - the agency or other person or body to which the conduct has been, or is to be, referred, and
  - the steps taken, or proposed to be taken, for the conduct to be referred or to facilitate its referral.

The AIC (or delegate) may delete from the copy of the reasons given to the discloser anything that would cause the document to:

- be exempt for the purposes of Part IV of the *Freedom of Information Act 1982* (FOI Act)

- have, or be required to have, a national security or other protective security classification, or
- contain intelligence information.

The notification requirements are set out in sections 50 and 50A of the PID Act.

Referral for investigation under another Commonwealth law or power

The AIC (or delegate) must, as soon as reasonably practicable, take reasonable steps to refer the conduct disclosed, or to facilitate its referral, for investigation under another Commonwealth law or power, if the AIC (or delegate):

- decides not to investigate the PID, or not to investigate the PID further
- does not decide to investigate the PID under a separate investigative power, and
- is satisfied, on reasonable grounds, that the conduct disclosed would be more appropriately investigated under another Commonwealth law or power (other than a separate investigative power).

The requirements for referral of a PID for investigation under another Commonwealth law or power are set out in section 50AA of the PID Act.

6.3. Decision to investigate

The investigation must be completed within 90 days

An investigation must be completed within **90 days** after the day when the PID was initially allocated.

If the PID was reallocated, the investigation must be completed 90 days after the day when the PID was reallocated. In the case of a reinvestigation, the investigation must be completed 90 days after the day when the AIC (or delegate) decided to reinvestigate the relevant PID.

The Commonwealth Ombudsman may extend the 90-day period by an additional period that the Ombudsman considers appropriate on the Ombudsman’s own initiative or on application made by the AIC (or delegate) or the discloser. If an extension is granted, the AIC (or delegate) must, as soon as reasonably practicable, inform the discloser (if contacting the discloser is reasonably practicable).

Failure to complete the investigation within the 90-day time limit does not affect the validity of the investigation.

Time limit requirements for investigations are in section 52 of the PID Act.

Conduct of the investigation

An investigation is to be conducted as the AIC (or delegate) thinks fit and they may, for the purposes of the investigation, obtain information from such persons, and make such inquiries, as they think fit. If it is reasonably practicable to contact the discloser, the investigator should keep them updated as to the progress of the investigation.

The steps that should be undertaken for conducting investigations are outlined in the OAIC's *Investigation steps under the Public Interest Disclosure Act 2013* and should be followed unless contrary to any requirement of the PID Act or PID Standard, or an alternative direction is provided by the NACC Commissioner, or the AIC; in relation to any or all of the steps.

When conducting an investigation, the AIC (or delegate) **must**:

- ensure that a PID is investigated on the basis that a decision whether evidence is sufficient to prove a fact must be determined on the balance of probabilities
- ensure that a finding of fact is based on logically probative evidence
- ensure that the evidence relied on in an investigation is relevant
- act in accordance with any rules relating to fraud that are made for the purposes of the *Public Governance, Performance and Accountability Act 2013*, to the extent that the investigation relates to one or more instances of fraud, and those rules are not inconsistent with the PID Act, and
- comply with any standards in force under the PID Act (i.e. the PID Standard).

Subject to restrictions imposed by any other law of the Commonwealth, the AIC (or delegate) (PID investigator) must ensure that, if a person is interviewed as part of the investigation of a PID, the interviewee is informed of the following:

- the identity and function of each individual conducting the interview
- the process of conducting an investigation
- the authority of the AIC (or delegate) under the PID Act to conduct the investigation, and
- the protections provided by Part 2 (Protection of disclosers and witnesses) of the PID Act (see section 3.6 above).

The AIC (or delegate) **must** ensure that:

- an audio or visual recording of the interview is not made without the interviewee's knowledge
- when an interview ends, the interviewee is given an opportunity to make a final statement or comment, or express a position, and
- any final statement, comment or position by the interviewee is included in the record of the interview.

The AIC (or delegate) conducting an investigation may adopt a finding set out in the report of an investigation or inquiry under another Commonwealth law or power, another investigation under Division 2 of Part 3 of the PID Act.

The requirements for conducting investigations are in sections 53, 54, and 56 of the PID Act and in Part 3 of the PID Standard.

Mandatory reporting during the investigation – corruption issues (see section 5.4)

At any time during the course of the investigation, if the AIC (or delegate) becomes aware of a corruption issue that:

- concerns the conduct of a person who is, or was, a staff member of the agency while that person is, or was, a staff member (see section 5.4 above for the meaning of staff member), and
- the officer suspects could involve corrupt conduct that is serious and systemic,

they **must** refer the corruption issue to the NACC Commissioner, or in the case of an intelligence agency, to the IGIS.

The AIC (or delegate) **must** notify the discloser that the PID has been referred to the NACC Commissioner, as soon as reasonably practicable, after the referral.

Mandatory reporting during the investigation – criminal conduct

At any time during the course of the investigation, if the AIC (or delegate) suspects on reasonable grounds that the information in the PID or any other information obtained in the course of the investigation is evidence of the commission of an offence against a law of the Commonwealth of Australia, State or Territory:

- they may give the information to a member of an Australian police force responsible for the investigation of the offence, and
- they **must** give the information to a member of an Australian police force responsible for the investigation of the offence if the offence is punishable by imprisonment for life or by imprisonment for a period of at least 2 years, unless (relevantly) the information raises a corruption issue that has already been referred or which the NACC Commissioner/IGIS is already aware.

Report of investigation

In preparing a report of an investigation under the PID Act, the AIC (or delegate) must comply with the PID Act, the PID Standard and these procedures.

On completing an investigation, the AIC (or delegate) **must** prepare a report that sets out:

- whether there have been one or more instances of disclosable conduct
- any regulations, rules, administrative requirements or similar matters to which the disclosable conduct relates
- the steps taken to gather evidence and a summary of the evidence
- the matters considered in the course of the investigation
- the AIC’s findings (if any) based on the evidence

- the duration of the investigation
- the action (if any) that has been, is being, or is recommended to be, taken, and
- claims of any reprisal taken against the discloser, or any other person, that relates to the matters considered in the course of the investigation, together with any related evidence, and the agency's response to any claims or evidence.

Where the AIC (or delegate) in preparing the report proposes to make a finding of fact or express an opinion that is adverse to a person, the AIC (or delegate) must give that person a copy of the evidence that is relevant to the proposed finding or opinion and must give the person a reasonable opportunity to comment on it.

The investigation is 'completed' when the AIC (or delegate) has prepared the above report.

The AIC (or delegate) **must**, within a reasonable time after preparing the report, give written notice of the completion of the investigation, together with a copy of the report, to:

- the discloser, if reasonably practicable, and
- the Commonwealth Ombudsman.

The AIC (or delegate) may delete from the copy given to the discloser any material:

- that is likely to enable the identification of the discloser or another person
- the inclusion of which would:
  - result in the copy being an exempt document under Part IV of the FOI Act
  - result in the copy being a document having, or being required to have, a national security or other protective security classification
  - result in the copy containing intelligence information, or
  - result in contravene a designated publication restriction.

The AIC (or delegate) may delete from a copy of the report given to the Commonwealth Ombudsman any material:

- that is likely to enable the identification of the discloser or another person, or
- the inclusion of which would contravene a designated publication restriction.

The AIC must, as soon as reasonably practicable, ensure that appropriate action in relation to the agency is taken in response to any recommendations in the report.

Requirements for the investigation report are in section 51 of the PID Act.

7. Additional obligations of authorised officers

7.1. Protecting officials against reprisals

An authorised officer **must** take reasonable steps to protect public officials who belong to the OAIC against reprisals that have been, or may be, taken in relation to PIDs that the authorised officer suspects on reasonable grounds:

- have been made or given to the officer
- may have been made or given to the officer
- are proposed to be made or given to the officer
- could be made or given to the officer.

The obligations of authorised officers set out above are in section 60 of the PID Act.

8. Additional obligations of principal officers

8.1. Facilitating PIDs

The AIC **must** take reasonable steps to ensure that:

- the number of authorised officers of the agency is sufficient to ensure that they are readily accessible by public officials who belong to the agency
- public officials who belong to the agency are aware of the identity of each authorised officer of the agency, and
- there is an effective means for potential disclosers to find out how to contact authorised officers (i.e. a means for both current and former officials of the agency to find effectively contact authorised officers).

The AIC must take reasonable steps to encourage and support:

- public officials who make, or are considering making, PIDs relating to the agency, and
- any other persons who provide, or are considering providing, assistance in relation to such PIDs.

For further guidance, see the Commonwealth Ombudsman's *Agency Guide to the Public Interest Disclosure Act 2013*: www.ombudsman.gov.au.

8.2. Providing training and education for officials

The AIC **must** take reasonable steps to provide ongoing training and education to OAIC officials about the PID Act including, without limitation, training and education about the following:

- integrity and accountability
- how to make a PID
- the protections available under the PID Act
- the performance by those officials of their functions under the PID Act, and
- the circumstances (if any) in which a PID must be referred to an agency, or other person or body, under another law of the Commonwealth.

The AIC **must** take reasonable steps to ensure that OAIC officials who are appointed to positions that require, or could require, them to perform the functions or duties, or exercise the powers, of an authorised officer or supervisor under the PID Act are given training and education appropriate for the position within a reasonable time after that appointment.

The additional obligations of principal officers are in section 59 of the PID Act.

8.3. Protecting officials against reprisals

The AIC **must** take reasonable steps to protect public officials who belong to the OAIC against reprisals that have been, or may be, taken in relation to PIDs that:

- have been made
- may have been made
- are proposed to be made
- could be made.

The obligations set out above are in section 59(9) of the PID Act.

8.4. Providing information to the Commonwealth Ombudsman

The AIC (or delegate) **must** provide the following information to the Commonwealth Ombudsman, on request by the Ombudsman, for the purpose of the Ombudsman preparing a report under the PID Act:

- the number of PIDs received by authorised officers of the agency during the period covered by the report
- the kinds of disclosable conduct to which those PIDs related
- the number of PIDs allocated to the agency during the period covered by the report
- the number of PID investigations that the AIC (or delegate) conducted during the period covered by the report
- the time taken to conduct those investigations
- the actions that the AIC (or delegate) has taken during the period covered by the report in response to recommendations in reports relating to those PID investigations, and
- any other information requested by the Ombudsman.

The AIC (or delegate) **must** provide the information within a time requested by the Ombudsman or as otherwise agreed with the Ombudsman.

The requirements for giving information and assistance for Ombudsman reports are set out in Part 5 of the PID Standard.

9. Obligations of all OAIC officials

All public officials who belong to the OAIC **must** use their best endeavours to assist:

- the AIC (or delegate) in the conduct of an investigation under the PID Act
- the Commonwealth Ombudsman and the IGIS (where relevant) in the performance of their functions under the PID Act, and
- any other public official to exercise a right, or perform a duty or function, under the PID Act.

Beyond these specific responsibilities, all OAIC officials share the responsibility of ensuring the PID Act works effectively, this includes:

- reporting matters where there is evidence that shows or tends to show disclosable conduct
- identifying areas where there may be opportunities for wrongdoing to occur because of inadequate systems or procedures and proactively raising these with management
- supporting public officials who have made PIDs, and
- keeping confidential the identity of disclosers and witnesses, where that is known.

The additional obligations of public officials are in section 61 of the PID Act.

10. What if the discloser is not satisfied with the agency's actions?

A discloser may make a complaint to the Commonwealth Ombudsman about the OAIC's handling of a PID. The Ombudsman may review the handling of the PID by any or all of the supervisor, authorised officer, AIC, or any other public official involved. As a result of the review, the Ombudsman may make written recommendations, including recommendations about allocation, reallocation, investigation, reinvestigation, or any other action. The AIC (or delegate) must consider and respond to any recommendation made by the Commonwealth Ombudsman in accordance with section 55 of the PID Act.

If a person who has made a PID believes, on reasonable grounds, that the investigation conducted by the OAIC was inadequate, the response to the investigation was inadequate, or the investigation was not completed within the time limit, it may be open to the person to make an external disclosure under the PID Act.

For more information on when an external disclosure may be made and how to make one, please refer to the Commonwealth Ombudsman's website: https://www.ombudsman.gov.au/.

11. Freedom of information requests

Documents associated with a PID are not exempt from the operation of the FOI Act. Requests for access to documents under the FOI Act must be considered on a case-by-case basis. A range of exemptions may apply to individual documents or parts of documents, particularly in relation to material received in confidence, personal information, agencies' operations, and law enforcement.

12. Further information

Further information can be found on the OAIC website accessible at this link. The OAIC also has a mailbox accessed only by the Chief Operating Officer, Assistant Commissioner Corporate and Director Governance and Risk where staff, including authorised officers, can seek advice on integrity matters, including anything in relation to the PID Act. The mailbox is integrity@oaic.gov.au.

Australian Government

Office of the Australian Information Commissioner

Public Interest Disclosure Act 2013 (PID Act)

What behaviour can be reported

Who can make a disclosure

How to make a public interest disclosure

Melanie Drayton

Chief Operating Officer

Melanie.Drayton@oaic.gov.au

02 9942 4216

s47E(d)

Annamie Hale

Assistant Commissioner Corporate

Annamie.Hale@oaic.gov.au

02 9942 4097

s47E(d)

Andre Castaldi

Assistant Commissioner Regulation & Strategy

Andre.Castaldi@oaic.gov.au

02 9942 4124

s47E(d)

Pennie Snowden

Assistant Commissioner
Dispute Resolution

Pennie.Snowden@oaic.gov.au

02 9942 4220

David Moore

Director Legal

David.Moore@oaic.gov.au

02 9942 4131

For more information or to submit a PID that is not directed to a particular Authorised Officer:

Email: PID@oaic.gov.au

Please note this email address is only used for public interest disclosure matters and access is restricted to the OAIC's Authorised Officers.

If your disclosure relates to one of the OAIC's Authorised Officers, please email one of the alternative Authorised Officers.

While undertaking their duties, if an Authorised Officer becomes aware of corrupt conduct that is 'serious or systemic', they are required to report the matter to the National Anti-Corruption Commission.

A discloser's identify and contact details, as well as the content of your public interest disclosure, will be protected in accordance with the PID Act. If you wish to remain anonymous and do not wish to have your identity or contact details provided to the Principal Officer or investigator, clearly state this in your correspondence.

Protections for people who make a disclosure

The PID Act offers protection to disclosers and witnesses from reprisal action. The OAIC will not tolerate any reprisal action against a person who makes a disclosure in accordance with the Act.

OAIC Policies and Procedures relating to public interest disclosures

More information regarding how the OAIC deals with public interest disclosures, including the steps an investigator should take where there has been a disclosure, can be found in:

- OAIC Public Interest Disclosure Procedures – D2018/015607

- OAIC Investigation steps under the Public Interest Disclosure Act 2013 - D2018/015608

Privacy notice

Your personal information is protected by Australian law, including the *Privacy Act 1988*, and is collected by the Office of the Australian Information Commissioner (OAIC) for the purpose of responding to and/or investigating a public interest disclosure.

Your information may be disclosed to other parties if required by any Australian law.

More information about how the OAIC manages your personal information and how to make a privacy complaint about how the OAIC has handled your information, can be found in the OAIC Privacy Policy.

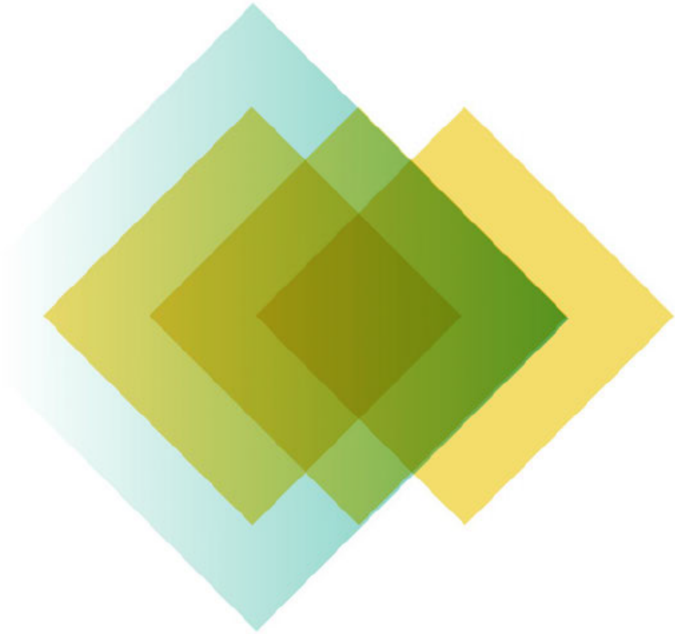
Further information

For more information:

- Public Interest Disclosure (Commonwealth Ombudsman)
- Assessing and managing the risk of reprisal (Commonwealth Ombudsman)

Procurement Policy and Procedures

June 2022



1 June 2022

OAIC

Audience: Internal

Location: Intranet

Review date: December 2023

Version	Name	Changes	Date
1.0	Lorraine Nurney	Original draft prepared	January 2018
2.0	Lorraine Nurney	Incorporate CPR changes commencing 1 January 2019	January 2019
2.1	Lorraine Nurney	Incorporate CPR changes commencing 20 April 2019	May 2019
2.2	Brenton Attard	Approved policy	June 2019
2.3	Ruth Mackay	Incorporating new PSPF policies (D2021/002255)	January 2021
2.4	Elizabeth Hampton	Approved	8 January 2021
2.5	Lorraine Nurney	Incorporate CPR changes commencing 14 December 2020	February 2021
2.6	Operations Committee	Approved policy	15 February 2021
2.7	Ruth Mackay	Draft PSPF additions	October 2021
2.8	Lorraine Nurney	Incorporate PSPF additions as per Security Governance Committee agreement 5 November	December 2021
2.9	Lorraine Nurney	Update for change from AHRC shared services to SDO	June 2022
3.0	Lorraine Nurney	Requirement for confidentiality deeds for contractors	July 2022
3.0	Brenton Attard	Review of updates version 2.9 and 3.0	August 2022

Contents

s22

[redacted]

[redacted]

s22

[redacted]

s22

[redacted]

s22

[redacted]

s22 [redacted]

Risk assessment

Risk management is built into the OAIC's procurement processes, and the extent of risk management required will vary from following routine procurement processes, to a significant undertaking involving the highest level of planning, analysis and documentation where the procurement is of a significance to warrant a full risk analysis. The effort directed to risk assessment and management should be commensurate with the scale, scope and risk of the procurement.

A requirement of any procurement is to conduct a risk assessment using the Risk Evaluation Guide. The level of risk will determine the procurement method that must be used. The assessed risk of the procurement will include consideration of the complexity and value of the procurement, the requirement, the circumstances and the market.

Procurements assessed as having a medium or high risk require a formal contract (refer to the procurement method section below). The following low risk procurements do not require a formal contract:

- petty cash purchases
- purchases using the corporate credit card
- issue of an invoice by the supplier before or after the delivery of the goods or services
- by issue of a purchase order.

Security risk management

When procuring goods or services, the OAIC will implement proportionate protective security measures by identifying and documenting:

a. specific security risks to its people, information and assets
b. mitigations for identified risks.

The OAIC will ensure that contracts for goods and services include relevant security terms and conditions for the provider to:

a. apply appropriate information, physical and personnel security requirements of the PSPF
b. manage identified security risks relevant to the procurement
c. implement governance arrangements to manage ongoing protective security requirements, including to notify the entity of any actual or suspected security incidents and follow reasonable direction from the entity arising from incident investigations.

When managing contracts, entities **must** put in place the following measures over the life of a contract:

a. ensure that security controls included in the contract are implemented, operated and maintained by the contracted provider and associated subcontractor
b. manage any changes to the provision of goods or services and reassess security risks.

Security risks will be assessed through the Risk Evaluation Guide. Guidance on assessing security risks and considering security arrangements during and at the conclusion of the contract are also included.

The procurement Risk Evaluation Guide requires prospective contract managers to identify the officer responsible for managing security risks through the life of and at the conclusion of the contract. The Agency Security Adviser (ASA) will keep a register of these arrangements and will monitor and report on their implementation.

Where there are changes to the contract the contract owner will arrange this with the assistance of the Governance and Procurement Manager who will subsequently provide the contract variation to the ASA to assess whether there are implications for managed security arrangements.

Confidentiality Deeds for contractors accessing sensitive information

The OAIC requires a Confidentiality Deed to be executed by contractors of suppliers where a procurement involves providing access to sensitive information. Sensitive information is any information, including personal information and security classified information, that is contained within the OAIC's computer systems/databases, including information provided to the OAIC as part of a privacy or freedom of information application process, or any records that contain, refer to or are based on any Confidential Information or any analysis of it.

Requests for quotation, approaches to markets, Commonwealth contracts or official work orders under panel arrangements should include a 'Disclosure of information' clause and contain a clause specifically stating the requirement for the supplier to arrange for its employees, agents or subcontractors to provide a written undertaking of non-disclosure by way of an executed confidentiality deed.

s22
[redacted]

s22

[redacted]

s22

[redacted]

s22

[redacted]

s22

[redacted]

s22

[redacted]

[redacted]

[2] Current as at 25 October 2021