



OFFICIAL

Records Management

Policy Statement

Document ID (PPN)	TI-1094
TRIM Record Number	ADD2021/1506316
BCS Function	Technology and Information Management
Document Owner	Group Manager Legal
Approval Date	19 April 2023
Document Contact	Records Management Section [REDACTED]@homeaffairs.gov.au

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

OFFICIAL**Table of Contents**

1. Purpose	3
2. Scope	3
2.1. In Scope	3
2.2. Out of Scope	3
3. Policy Statement	4
3.1. Create and capture	4
3.1.1. Electronic Document and Records Management Systems	4
3.1.2. Metadata	4
3.1.3. Naming conventions	4
3.1.4. Electronic records	4
3.1.5. Physical records	4
3.2. Maintain and protect	5
3.2.1. Record security	5
3.2.2. Record integrity	5
3.2.3. Electronic storage	5
3.2.4. Maintaining digital records	5
3.2.5. Physical records	5
3.2.6. Record custody	6
3.3. Disposal, destruction and transfer	6
3.3.1. Record authorities and retention periods	6
3.3.2. Normal Administrative Practice	6
3.3.3. Disposal freezes and retention notices	6
3.3.4. Machinery of Government changes	7
3.4. Acceptable Use of ICT resources	7
4. Accountabilities and Responsibilities	7
5. Version Control	8
Attachment A – Definitions	9
Attachment B – Related Documents	12
Attachment C – Related Legislation	13
Attachment D – Consultation	14
1.1 Internal Consultation	14

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

1. Purpose

This Policy Statement (PS) sets out the management of records throughout the information lifespan from create and capture, to maintain and protect, to disposal and destruction that all workers in the Department of Home Affairs (the Department), including the Australian Border Force (the ABF), must adhere to.

A record is all information created, sent and received in the course of carrying out the business of the Department. Records are a vital asset to the Department's corporate memory and quality records management is underpinned by the authenticity, reliability, integrity and usability of information.

All agencies must maintain accurate and reliable records as evidence to ensure that business activities and decisions are transparent and accountable. This is in accordance with the general principles and legislation in the *Archives Act 1983* (the Archives Act), the *Privacy Act 1988* (the Privacy Act), the *Freedom of Information Act 1982* (the FOI Act), the *Protective Security Policy Framework* (PSPF) and material issued by the National Archives of Australia (NAA), including Building Trust in the Public Record policy.

2. Scope

2.1. In Scope

This PS:

- applies to all business areas and business information created and received by the Department
- applies to records in all formats whether electronic or physical, including those created or captured via email, websites, social media applications, databases and business information systems
- applies to all persons carrying out work for the Department (referred to as 'workers' in this PS), including:
 - Immigration and Border Protection (IBP) workers (including all APS employees in the Department, including the ABF)
 - workers at overseas posts (including locally engaged workers)
 - ongoing, non-ongoing and casual workers
 - contractors and consultants
 - Senior Executive Services (SES)
 - personnel whose services are made available to the Department.

2.2. Out of Scope

This PS does not apply to Cabinet documents. Refer to the Department of Prime Minister and Cabinet Cabinet Handbook 15th Edition.

In addition to this PS, see the Handling Protectively Marked Material – Procedural Instruction (HR-6361) for information security obligations and responsibilities, and guidance on how to correctly handle and apply protective markings to official information.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

3. Policy Statement

3.1. Create and capture

3.1.1. Electronic Document and Records Management Systems

All records must be stored in an Electronic Document and Records Management System (EDRMS). EDRMS supports the creation, use and management of records and information in electronic and physical formats. All new business systems must be ISO 16175 compliant. If no dedicated business system exists specifically for the storage of particular records, the records must be stored in TRIM.

TRIM is the Department's EDRMS for records protectively marked and/or security classified up to and including PROTECTED and metadata for physical records up to and including TOP SECRET as long as the metadata is not security classified above PROTECTED. Records management systems for human resources, financial management, travel and core functions processing systems, which create, capture and collect data and records, are subject to the same records management legislative and statutory requirements as TRIM.

s. 47E(d)

3.1.3. Naming conventions

Naming conventions for record titles provide context and consistency and must describe the content of the record, so records can be found.

Key information must be provided in the record title including:

- **What** activity the content of the record relates to.
- **Where** the activity represented in the record took place. For example, as a state or region.
- **When** the content of the record took place or is for. For example, specify dates.
- **Who** the content of the record relates to. For example, an individual name, business area, or client's name.

3.1.4. Electronic records

Records created or received electronically should remain electronic and stored in an EDRMS. Digitising source records must be in accordance with the Digitising Physical Records – Procedural Instruction (TI-5396). Once a record is digitised and no requirement remains to retain the original, the physical record must be destroyed to reduce duplication and storage of physical records.

3.1.5. Physical records

s. 47E(d)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

3.2. Maintain and protect

3.2.1. Record security

All records must be handled in accordance with the Handling Protectively Marked Material – Procedural Instruction (HR-6361). This covers information security obligations and responsibilities as well as guidance on how to correctly handle and apply protective markings to official information.

3.2.2. Record integrity

To maintain record integrity, record content must remain complete, accurate, authentic, and accessible to those who have the appropriate security clearance and on a need-to-know basis. Unauthorised damage or alteration of a Commonwealth record (other than in accordance with subsection 24(2) of the Archives Act) with the purpose of changing the intent or context, jeopardises integrity, contravenes the Archives Act and may constitute a breach of the Australian Public Service Code of Conduct. Business areas are responsible for applying and maintaining record access control. Workers are responsible for only accessing records that are necessary to fulfil their role and with the appropriate level of security clearance.

3.2.3. Electronic storage

Records must be stored in ISO 16175 compliant systems. The following are not ISO 16175 compliant, and must not be used unless an exemption is approved by the Director Records Management as outlined in Correct use of the Department's Information Storage Systems and Network Drives – Policy Statement (TI-5981):

- Network Attached Storage (NAS) devices;
- shared drives;
- SharePoint;
- Microsoft Teams;
- email systems;
- temporary storage solutions, such as Universal Serial Buses (USBs); and
- external drives.

3.2.4. Maintaining digital records

Electronic records must be managed to maintain authenticity, reliability and integrity as stipulated in NAA's Building Trust in the Public Record Policy. If a record is created digitally, the record should remain digital and should not be reproduced in physical form, for example, by printing. Keeping the record digital in an EDRMS allows for audit events to be tracked, versions controlled and reduces the burden of physical storage.

3.2.5. Physical records

Records must only be kept in physical form when a legal or administrative requirement exists. Digitising Physical Records – Procedural Instruction (TI-5396) provides further information. Physical records storage, whether in-house or with an external provider, must be within a facility that ensures records are protected, accessible, traceable, and managed in a secure manner. Further information on security zoning of a work area and the appropriate containers or secure rooms required for storage can be found in Handling Protectively Marked Material – Procedural Instruction (HR-6361).

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

3.2.6. Record custody

Commonwealth records are the property of the Commonwealth. Business areas are responsible for the maintenance of records created or owned by the business area for which their business function relates. For example, during a machinery of government change, records may move to or from another department based on the incoming or outgoing business function being transferred. As such, business areas are responsible for maintaining these records. All workers are accountable for the correct management of records. This includes service providers who manage records on behalf of the Department. Commonwealth records that are managed by service providers remain Commonwealth records and must be returned to the Department at the end of the contract. General Records Authority (GRA) 40 provides further information.

3.3. Disposal, destruction and transfer

3.3.1. Record authorities and retention periods

A Record Authority (RA) is a legal instrument that allows agencies to make decisions about keeping, destroying or transferring Commonwealth records. RAs are issued by the NAA and are used to determine how long to keep records and provide permission to destroy records once this time has elapsed. General RAs are used to authorise the disposal of records that contain administrative business activities and responsibilities common to all Commonwealth agencies. Agency specific RAs are used for specific business activities and functions. The disposal and destruction of Commonwealth records must be in accordance with the Archives Act. Disposal cannot take place unless:

- an RA is assigned to the record that permits the destruction once the retention period has elapsed, or
- if a disposal freeze or retention notice does not apply, or
- the record is eligible to be disposed under Normal Administrative Practice (NAP) (see section 3.3.2 below).

See Destroying Low Value Information - Normal Administrative Practice - Procedural Instruction (TI-5393).

The Privacy and Information Disclosure Section must be contacted if a business area seeks to retain official information that contains personal information, for a business purpose, beyond the minimum retention period specified in the relevant RA. Email [s.22\(1\)\(a\)\(ii\)@homeaffairs.gov.au](mailto:s.22(1)(a)(ii)@homeaffairs.gov.au).

Contact [s.22\(1\)\(a\)@homeaffairs.gov.au](mailto:s.22(1)(a)@homeaffairs.gov.au) for further assistance on record authority and retention periods if needed.

3.3.2. Normal Administrative Practice

NAP is an exception to the prohibition on the destruction of Commonwealth records under section 24 of the Archives Act, which permits the destruction of information under certain circumstances without formal permission from the NAA (see paragraph 24(2)(c) of the Archives Act). NAP cannot be used to dispose of records that are, or should be, covered by an RA. The application of NAP is outlined in Destroying Low Value Information – Normal Administrative Practice – Procedural Instruction (TI-5393).

3.3.3. Disposal freezes and retention notices

Disposal freezes may be imposed on Commonwealth agencies by the NAA to prevent the destruction of records that relate to significant events, issues or judicial proceedings. Retention notices apply to records related to the core business activities of specific Commonwealth agencies. Agency specific records cannot be destroyed or disposed of when the NAA applies a retention notice. A list of current disposal freezes and retention notices is available at the NAA's website.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

3.3.4. Machinery of Government changes

Records may be transferred to or received from other agencies when a Machinery of Government (MOG) change occurs through Administrative Arrangements Orders (AAO). The NAA's website, [Transferring information following administrative change](#), provides further information.

3.4. Acceptable Use of ICT resources

In accordance with the [Acceptable Use of Departmental ICT Systems and Information - Procedural Instruction \(HR-3320\)](#), all departmental workers have obligations under legislation, including (but not limited to) the *Australian Border Force Act 2015*, the *Migration Act 1958*, the *Australian Citizenship Act 2007*, the Privacy Act, the *Criminal Code Act 1995*, the *Public Service Act 1999* and departmental policies and procedures to protect the security and confidentiality of information, including that which is held within the Department's Information Communications Technology (ICT) resources, and to use these resources in a proper manner and for a proper purpose.

All information and data moving through the Department's ICT environment must be appropriately protected according to the degree of sensitivity, confidentiality and criticality in accordance with the [Protective Security Policy Framework \(PSPF\)](#), the [Information Security Manual \(ISM\)](#), the ABF Act, the Privacy Act, and any other applicable legislation.

4. Accountabilities and Responsibilities

Role	Description
National Archives of Australia (NAA)	Established under the Archives Act, the NAA have overall responsibility for managing, maintaining and preserving Commonwealth records.
Assistant Secretary FOI and Records Management	Responsible for: • promoting a culture that supports best practice records and information management • maintaining and monitoring the records and information management policy framework for the Department, including implementing systems and practices to ensure the Department meets its regulatory obligations • updating and providing advice on the content of this PS, Procedural Instruction(s) and Supporting Material • arranging the approval of disposal activities for all departmental records
Chief Information Officer	Responsible for: • maintaining information technology (IT) platforms to support records and information management systems and processes, consistent with this PS and Procedural Instruction(s) • integrating records and information management requirements in the Department's IT systems and strategic plans

 Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

Role	Description
	implementing an integrated EDRMS for the Department and providing required system enhancements
All Senior Executive Service (SES) and Executive Level (EL) staff	Responsible for arranging processes to ensure that records and information management practices for their business areas are implemented and consistent with this PS and Procedural Instruction(s), including business functions onshore, offshore and services provided by third parties.
Enterprise Operations Committee	Has oversight of records and information management functions within the Department including the <u><i>Building Trust in the Public Record: Managing Information and Data for Government and Community</i></u> policy.
Records Management Section	The Records Management Section is responsible for: - providing advice and support - updating records management policies and procedures - determining record retention - reporting unauthorised destruction of records to the Archives
Connected Services / TRIM Help Desk	Provides TRIM support to workers.
All workers, including: - ABF Officers - Contractors - Consultants Workers at overseas posts, including locally engaged workers.	Responsible for: - understanding their records and information management obligations and responsibilities that relate to their position - adhering to this PS and related Procedural Instruction(s) in creating and maintaining records and information related to their daily work - accessing supporting material to ensure that they follow policy and procedures correctly - undertaking the mandatory Records Essentials training every two (2) years
New employees	New employees must complete the <i>Essentials Suite</i> and <i>TRIM Essentials</i> mandatory online learning courses within 90 days of commencement.

5. Version Control

Version number	Date of issue	Author(s)	Brief description of change
1.0	11 July 2016	Records Management Section	First version.

OFFICIAL

Version number	Date of issue	Author(s)	Brief description of change
2.0	19 April 2023	Records Management Section	Review.

Attachment A – Definitions

Term	Acronym (if applicable)	Definition
Access	-	The ability to create, receive, edit or share records, and apply control to restrict access.
Building Trust in the Public Record Policy	-	A Whole-of-Government policy led by the National Archives of Australia (NAA) that identifies requirements for agencies to address capability gaps and improve information management by: - managing information assets strategically with appropriate governance and reporting; - implementing fit-for-purpose information management processes, practices and systems; - reducing areas of information management inefficiency and risk
Capture	-	The process of storing a record in an EDRMS and assigning metadata to describe the record and its context.
Commonwealth record	-	As defined in subsection 3(1) of the <i>Archives Act 1983</i> (the <i>Archives Act</i>), to mean: - a record that is the property of the Commonwealth or of a Commonwealth institution; or - a record that is to be deemed to be a Commonwealth record by virtue of a regulation under subsection 3(6) or by virtue of section 22; but does not include a record that is exempt material.
Electronic Document and Records Management System	EDRMS	An EDRMS is a software application that manages a range of digital information, including word-processed documents, spreadsheets, emails, images and scanned documents. An EDRMS can combine both document management and records management functionality.
Information	-	Knowledge communicated or received; the result of processing, gathering, manipulating and organising data in a way that adds to the knowledge of the receiver.

Released by Department of Home Affairs under the Freedom of Information Act 1982

OFFICIAL

Term	Acronym (if applicable)	Definition
Information Security Manual	ISM	Outlines a cyber security framework that organisations can apply, using their risk management framework, to protect their information and systems from cyber threats.
ISO 16175 - Principles and functional requirements for records in electronic office environments	ISO 16175	ISO 16175 provides internationally agreed principles and functional requirements for software used to create and manage digital information in office environments.
Metadata	-	Data or information about data that assists to help understand the structure, nature and context of the data. For example, the record number, title, creator and owner are metadata fields in TRIM.
Naming conventions	-	To apply approved terms to record titles and names to assist retrieval and traceability.
National Archives of Australia	NAA	Under the authority of the Archives Act, the NAA have overall responsibility for managing, maintaining and preserving Commonwealth records.
Normal Administrative Practice	NAP	A process that allows agencies to destroy certain types of low value and short-term information in the normal course of business.
Protective marking	-	Protective markings are text-based marking applied to documents and emails. A protective marking indicates the required level of protection for the information to all users at a quick glance. Protective markings available for use are UNOFFICIAL, OFFICIAL, OFFICIAL: Sensitive, PROTECTED, SECRET, TOP SECRET and Caveats which are applied to documents and indicate access and handling requirements for the information.
Protective Security Policy Framework	PSPF	Sets out government protective security policy that Australian Government entities must apply to protect their people, information and assets.
Records Authority	RA	A records authority is a legal instrument that allows agencies to make decisions about keeping, destroying or transferring Commonwealth records. Records authorities are used to determine how long to keep records and provide permission for the destruction of records once this time has passed.
Record sentencing	-	Sentencing is the process of matching information to a relevant RA to establish the value of information and for how long it must be kept.

 Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

Term	Acronym (if applicable)	Definition
Source record	-	The physical record from which a digitised version is made.
TRIM (also known as Content Manager)	-	The Department's electronic document and records management system (EDRMS).

Released by Department of Home Affairs
under the *Freedom of Information Act 1982*

OFFICIAL

Attachment B – Related Documents

- [Australian Government Digital Service Standard](#)
- [Australian Government Information Security Manual](#)
- [Australia Government Recordkeeping Metadata Standard](#)
- [Building Trust in the Public Record: Managing Information and Data for Government and Community Policy](#)
- [Cabinet Handbook 15th Edition](#)
- [ISO 15489 - Australian Standard for Records Management](#)
- [ISO 16175 - Principles and Functional Requirements for Records in Electronic Office Environments](#)
- [Protective Security Policy Framework](#)
- [Business Systems for Records Management Compliance – Policy Statement \(TI-6632\)](#)
- [Correct use of the Department's Information Storage Systems and Network Drives – Policy Statement \(TI-5981\)](#)
- [Department's Privacy Policy – Policy Statement \(TI-1149\)](#)
- [Email, Instant Messaging and Social Media – Policy Statement \(TI-5397\)](#)
- [Acceptable use of Departmental ICT Systems and Information – Procedural Instruction \(HR-3320\)](#)
- [Access Examination – Procedural Instruction \(TI-5395\)](#)
- [Audiovisual Records – Procedural Instruction \(TI-7057\)](#)
- [Destroying Low Value Information – Normal Administrative Practice – Procedural Instruction \(TI-5393\)](#)
- [Digitising Physical Records – Procedural Instruction \(TI-5396\)](#)
- [Handling Protectively Marked Material – Procedural Instruction \(HR-6361\)](#)
- [Information and Communication Technology Access Control – Procedural Instruction \(TI-1618\)](#)
- [Overseas Records Management – Procedural Instruction \(TI-6359\)](#)
- [Records Management for Disturbing Material – Procedural Instruction \(TI-6977\)](#)
- [Records Management for Machinery of Government Changes – Procedural Instruction \(TI-7049\)](#)
- [Roles and Responsibilities of Business and Technical System Owners - Policy Statement \(TI-6262\)](#)
- [Guide to Good Records Management – Supporting Material \(TI-6069\)](#)
- [Records Management Reference Guide for Contract Managers – For Internal Use Only – Supporting Material \(TI-7053\)](#)
- [Records Management Guide for Service Providers – For External Use – Supporting Material \(TI-7054\)](#)
- [Records Management Plan – Supporting Material \(TI-7067\)](#)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

Attachment C – Related Legislation

- Administrative Decisions (Judicial Review) Act 1977
- Archives Act 1983
- Auditor-General Act 1997
- Australian Border Force Act 2015
- Australian Citizenship Act 2007
- Crimes Act 1914
- Electronic Transactions Act 1999
- Evidence Act 1995
- Freedom of Information Act 1982
- Migration Act 1958
- Public Governance, Performance and Accountability Act 2013
- Privacy Act 1988
- Public Order (Protection of Person and Property) Act 1971
- Public Service Act 1999

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

Attachment D – Consultation

1.1 Internal Consultation

- Privacy and Information Disclosure Section - s. 22(1)(a)(ii) @homeaffairs.gov.au
- Performance and Communication - s. 22(1)(a)(ii) @homeaffairs.gov.au
- Cyber and Information Security - s. 22(1)(a)(ii) @homeaffairs.gov.au
- ICT - s. 22(1)(a)(ii) @homeaffairs.gov.au
- Security Policy, Communications and Skilling - s. 22(1)(a)(ii) @homeaffairs.gov.au
- Integrity and Professional Standards Branch - s. 22(1)(a)(ii) @homeaffairs.gov.au
- Legal Group - s. 22(1)(a)(ii) @homeaffairs.gov.au

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL



OFFICIAL

Email, Instant Messaging and Social Media

Policy Statement

Document ID (PPN)	TI-5397
TRIM Record Number	ADD2022/6212454
BCS Function	Technology and Information Management
Document Owner	Group Manager Legal
Approval Date	19 April 2023
Document Contact	Records Management Section  @homeaffairs.gov.au

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

OFFICIAL**Table of Contents**

1. Purpose	3
2. Scope	3
2.1. In Scope	3
2.2. Out of Scope	3
3. Policy Statement	4
3.1. General principles	4
3.2. Access to instant messaging and social media	4
3.3. Management of emails, instant messages and social media as Commonwealth records	5
3.4. Deleting emails, instant messages and social media	5
3.5. Emailing attachments	5
3.6. Information security	5
3.7. Management of group mailboxes	5
3.8. Mobile messaging applications	6
3.9. Acceptable use of ICT resources	6
3.10. Consequences of non-compliance	Error! Bookmark not defined.
4. Accountabilities and Responsibilities	6
5. Version Control	8
Attachment A – Definitions	9
Attachment B – Related Documents	11
Attachment C – Related Legislation	12
Attachment D – Consultation	13
1.1 Internal Consultation	13

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

1. Purpose

Workers are responsible for the records management of information created or received as part of Australian Government business. This Policy Statement (PS) provides workers of the Department of Home Affairs (the Department), including the Australian Border Force (the ABF), guidance on the records management of official information transmitted through email, instant messaging, social media and similar platforms and services.

All official information exchanged through the Department's communication systems remains the property of the Department and must be managed as Commonwealth records in accordance with the *Archives Act 1983* (Archives Act), *Freedom of Information Act 1982*, *Privacy Act 1988* (Privacy Act), this PS, the Records Management – Policy Statement (TI-1094), Protective Security Policy Framework and Handling Protectively Marked Material – Procedural Instruction (HR-6361).

2. Scope

2.1. In Scope

This PS:

- applies to all business areas and business information created and received by the Department through email, instant messaging, social media and similar platforms and services.
- applies to all persons carrying out work for the Department, including:
 - all Immigration and Border Protection (IBP) workers
 - workers at overseas posts (including locally engaged workers)
 - ongoing, non-ongoing and casual workers
 - contractors and consultants
 - Senior Executive Services (SES)
 - personnel from other Australian Government agencies undertaking duties on behalf of the Department.

2.2. Out of Scope

This PS **does not**:

- replace internal communication guidelines;
- replace policies on the use and management of emails transferred to other systems; or
- apply to the personal use of email, instant messaging and social media. See Use of Social Media and Other Online Services - Procedural Instruction (SM-1560).

Email, instant messaging and social media for official business must comply with this PS, the Acceptable use of Departmental ICT Systems and Information - Procedural Instruction (HR-3320) and other applicable policies.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

3. Policy Statement

3.1. General principles

Official information created, collected and shared through email, instant messaging services and social media records must be stored in accordance with relevant legislative requirements and the Records Management – Policy Statement (TI-1094).

Use of the Department's communication systems must be managed in accordance with the APS Values and Code of Conduct, and the Acceptable Use of Departmental ICT Systems and Information – Procedural Instruction (HR-3320).

Workers must not:

- transmit or store inappropriate material;
- use the Department's communication systems to comment on, or distribute inappropriate content, that is:
 - unlawful;
 - harmful;
 - threatening;
 - false;
 - obscene;
 - defamatory;
 - libellous;
 - hateful;
 - vilifying; or
 - of a similar nature to the above
- forward departmental emails or instant messages to recipients outside of the Department including third parties (except where there is a genuine business need to do so). To do so may result in the recipients inappropriately obtaining privileged information, or personal, sensitive or classified information that is not intended for external recipients; or
- send 'all staff' emails without clearance. See the Internal Communication intranet page for further information.

3.2. Access to instant messaging and social media

S. 47E(d)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL**3.3. Management of emails, instant messages and social media as Commonwealth records**

s. 47E(d)

3.4. Deleting emails, instant messages and social media

s. 47E(d)

3.5. Emailing attachments

s. 47E(d)

3.6. Information security

s. 47E(d)

3.7. Management of group mailboxes

s. 47E(d)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

s. 47E(d)

3.8. Mobile messaging applications

Messaging applications on mobile devices are not appropriate for recording or storing records. Workers must extract, take a screenshot, or take note of any official business conducted on a mobile messaging application and record it in an EDRMS, such as TRIM. See the Smart Mobile Device Security – Procedural Instruction (TI-6664) for mobile applications suitable for conducting departmental communications. Workers are responsible for ensuring that the settings used on devices do not erase records automatically before workers can save the records to an EDRMS.

3.9. Acceptable use of ICT resources

In accordance with the Acceptable Use of Departmental ICT Systems and Information - Procedural Instruction (HR-3320), workers have obligations under legislation, including (but not limited to) the *Australian Border Force Act 2015* (the ABF Act), the *Migration Act 1958*, the *Australian Citizenship Act 2007*, the *Privacy Act*, *Criminal Code Act 1995*, the *Public Service Act 1999* (the Public Service Act) and departmental policies and procedures to protect the security and confidentiality of information, including that which is held within the Department's Information Communications Technology (ICT) resources, and to use these resources in a proper manner and for a proper purpose.

All information and data moving through the Department's ICT environment must be marked appropriately and protected according to the degree of sensitivity, confidentiality and criticality in accordance with the Protective Security Policy Framework (PSPF), the Information Security Manual (ISM), the ABF Act, the Privacy Act, and any other applicable legislation.

4. Accountabilities and Responsibilities

Role	Description
All IBP workers and workers at overseas posts, including locally engaged workers.	Responsible for: • understanding records and information management obligations and responsibilities that relate to their position; • adhering to this PS and related Procedural Instruction(s) in creating and maintaining records and information related to their daily work; • accessing supporting material to ensure policy and procedures are followed correctly; and • using systems in a way that: ○ does not breach the APS Values and Code of Conduct; ○ ensures business information is managed in an appropriate and secure manner that protects Commonwealth records from loss, destruction, privacy or security breaches or information leaks; ○ ensures the application of DLMs complies with the Protective Security Policy Framework; and

OFFICIAL

Role	Description
	ensures email signature blocks and properties are accurate and up to date.
All Senior Executive Service (SES) and Executive Level (EL) staff	Responsible for arranging processes to ensure that records and information management practices for business areas are implemented and consistent with this PS and Procedural Instruction(s), including business functions onshore, offshore and services provided by third parties.
Chief Information Officer	Responsible for: - maintaining Information Technology platforms to support records and information management systems and processes, consistent with this PS and Procedural Instruction(s); - the integration of records and information management requirements in the Department's Information Technology systems and strategic plans; and - implementing an integrated EDRMS for the Department and providing required system enhancements.
Connected Services / TRIM Help Desk	Provides TRIM support to workers.
Director Collaboration Infrastructure Services	Responsible for the technical management of email and instant messaging systems.
Assistant Secretary FOI and Records Management	Is responsible for: - promoting a culture that supports best practice records and information management; - maintaining and monitoring the records and information management policy framework for the Department, including implementing systems and practices to ensure the Department meets its regulatory obligations; - preparing and updating content for the Policy Statement, Procedural Instruction(s) and Supporting Material; - providing advice on the Policy Statement, Procedural Instruction(s) and Supporting Material; and - arranging the approval of disposal activities for all departmental records.
National Archives of Australia (NAA)	Under the authority of the Archives Act, the NAA have overall responsibility for managing, maintaining and preserving Commonwealth records.
Records Management Section	The Records Management Section is responsible for: providing advice and support;

 Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

Role	Description
	• updating records management policies and procedures; • determining record retention; and • reporting unauthorised destruction of records to the Archives.

5. Version Control

Version number	Date of issue	Author(s)	Brief description of change
1.0	2018	Records Management Section	First version.
1.1	2019	Records Management Section	Addition of mobile messaging applications, minor edits to 4.10 Emailing attachments.
2.0	19 April 2023	Records Management Section	Review.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

Attachment A – Definitions

Term	Acronym (if applicable)	Definition
Commonwealth record	-	As defined in subsection 3(1) of the <i>Archives Act 1983</i> (the <i>Archives Act</i>), to mean: - a record that is the property of the Commonwealth or of a Commonwealth institution; or - a record that is to be deemed to be a Commonwealth record by virtue of a regulation under subsection 3(6) or by virtue of section 22; but does not include a record that is exempt material.
Communication systems	-	Includes email, instant messaging, social media and similar platforms and services.
Electronic Document and Records Management System	EDRMS	An EDRMS is a software application that manages a range of digital information, including word-processed documents, spreadsheets, emails, images and scanned documents. An EDRMS can combine both document management and records management functionality.
Email	-	Electronic mail transmitted as messages over computer networks.
Enterprise Vault	EV	Repository for storage of email and messaging business information.
Freedom of Information	FOI	Under the <i>Freedom of Information Act 1982</i> (FOI Act), the public has a legal right (subject to some exceptions) to see documents held by Commonwealth agencies (departments and authorities) and to get copies of those documents. Members of the public can also see most manuals, rules and guidelines that Commonwealth agencies use to make decisions about the legislation they administer.
Information	-	Knowledge communicated or received; the result of processing, gathering, manipulating and organising data in a way that adds to the knowledge of the receiver.
Information Security Manual	ISM	Outlines a cyber-security framework that organisations can apply, using their risk management framework, to protect their information and systems from cyber threats.
Instant Messaging (Skype for Business, Microsoft Teams, WebEx)	IM	Telecommunications application software products that provides video chat and voice calls between electronic devices via the internet and telephones. Users may transmit both text, voice and video messages, and may exchange digital documents such as images, text and video.

OFFICIAL

Term	Acronym (if applicable)	Definition
ISO 16175 - Principles and functional requirements for records in electronic office environments	ISO 16175	ISO 16175 provides internationally agreed principles and functional requirements for software used to create and manage digital information in office environments.
Microsoft Outlook	-	The Department's email system.
National Archives of Australia	NAA	Under the authority of the Archives Act, the NAA have overall responsibility for managing, maintaining and preserving Commonwealth records.
Normal Administrative Practice	NAP	A process that allows agencies to destroy certain types of low value and short-term information in the normal course of business.
Official information	-	Official information is all information created, sent or received as part of work for the Australian Government.
Protective Security Policy Framework	PSPF	Assists Australian Government entities to protect their people, information and assets, both at home and overseas.
Record	-	A record is all information created, sent and received in the course of carrying out the business of the Department.
Social media records	-	Information on social media which contains evidence of an agency's business activities, including, but not limited to, posts and comments.
TRIM (also known as Content Manager)	-	The Department's electronic document and records management system (EDRMS).

 Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

Attachment B – Related Documents

- [Australian Government Digital Service Standard](#)
- [Australian Government Information Security Manual](#)
- [Australia Government Recordkeeping Metadata Standard](#)
- [Building Trust in the Public Record: Managing Information and Data for Government and Community Policy](#)
- [Cabinet Handbook 15th Edition](#)
- [ISO 15489 - Australian Standard for Records Management](#)
- [ISO 16175 - Principles and Functional Requirements for Records in Electronic Office Environments](#)
- [Protective Security Policy Framework](#)
- [Business Systems for Records Management Compliance – Policy Statement \(TI-6632\)](#)
- [Correct use of the Department's Information Storage Systems and Network Drives – Policy Statement \(TI-5981\)](#)
- [Department's Privacy Policy – Policy Statement \(TI-1149\)](#)
- [Freedom of Information – Policy Statement \(SM-3357\)](#)
- [Records Management – Policy Statement \(TI-1094\)](#)
- [Acceptable use of Departmental ICT Systems and Information – Procedural Instruction \(HR-3320\)](#)
- [Access Examination – Procedural Instruction \(TI-5395\)](#)
- [Audiovisual Records – Procedural Instruction \(TI-7057\)](#)
- [Destroying Low Value Information – Normal Administrative Practice – Procedural Instruction \(TI-5393\)](#)
- [Digitising Physical Records – Procedural Instruction \(TI-5396\)](#)
- [Handling Protectively Marked Material – Procedural Instruction \(HR-6361\)](#)
- [Information and Communication Technology Access Control – Procedural Instruction \(TI-1618\)](#)
- [Overseas Records Management – Procedural Instruction \(TI-6359\)](#)
- [Records Management for Disturbing Material – Procedural Instruction \(TI-6977\)](#)
- [Records Management for Machinery of Government Changes – Procedural Instruction \(TI-7049\)](#)
- [Roles and Responsibilities of Business and Technical System Owners - Policy Statement \(TI-6262\)](#)
- [Smart Mobile Device Security – Procedural Instruction \(TI-6664\)](#)
- [Guide to Good Records Management – Supporting Material \(TI-6069\)](#)
- [Records Management Reference Guide for Contract Managers – For Internal Use Only – Supporting Material \(TI-7053\)](#)
- [Records Management Guide for Service Providers – For External Use – Supporting Material \(TI-7054\)](#)
- [Records Management Plan – Supporting Material \(TI-7067\)](#)

 Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

Attachment C – Related Legislation

- Administrative Decisions (Judicial Review) Act 1977
- Archives Act 1983
- Auditor-General Act 1997
- Australian Border Force Act 2015
- Australian Citizenship Act 2007
- Crimes Act 1914
- Electronic Transactions Act 1999
- Evidence Act 1995
- Freedom of Information Act 1982
- Migration Act 1958
- Public Governance, Performance and Accountability Act 2013
- Privacy Act 1988
- Public Order (Protection of Person and Property) Act 1971
- Public Service Act 1999

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

Attachment D – Consultation

1.1 Internal Consultation

- Privacy and Information Disclosure Section - s. 22(1)(a)(ii) @homeaffairs.gov.au
- Performance and Communication - s. 22(1)(a)(ii) @homeaffairs.gov.au
- Cyber and Information Security - s. 22(1)(a)(ii) @homeaffairs.gov.au
- ICT - s. 22(1)(a)(ii) @homeaffairs.gov.au
- Freedom of Information - s. 22(1)(a) @homeaffairs.gov.au
- Media and Engagement Branch - s. 22(1)(a)(ii) @homeaffairs.gov.au
- Internal Communications - s. 22(1)(a)(ii) @homeaffairs.gov.au
- Policy Communications and Skilling, Security Branch - s. 22(1)(a)(ii) @homeaffairs.gov.au
- Collaboration Infrastructure Services - s. 22(1)(a)(ii) @homeaffairs.gov.au
- Integrity and Professional Standards - s. 22(1)(a)(ii) @homeaffairs.gov.au
- Legal Group - s. 22(1)(a)(ii) @homeaffairs.gov.au

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL



OFFICIAL

Acceptable use of Departmental ICT Systems and Information

Procedural Instruction

Document ID (PPN)	HR-3320
TRIM record number	ADD2024/102859984
BCS Function	Technology and Information Management
Document owner	Assistant Secretary, Cyber Risk Services Branch
Approval date	27/01/2023
Document Contact	Cyber Risk Management Section, s. 22(1)(a)(ii)@homeaffairs.gov.au

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

OFFICIAL

Table of Contents

1. Purpose	4
2. Scope	4
3. Procedural Instruction	4
3.1. Overview and context	4
3.2. Specific terms	5
3.3. IBP workers' responsibilities	6
3.3.1. IBP workers' responsibilities when using ICT resources	6
3.3.2. Unacceptable use of ICT resources	6
3.4. External information	7
3.5. Special exemptions for professional use	8
3.6. Personal use/reasonable access	8
3.7. Securing the ICT environment	9
3.7.1. Protecting the security and confidentiality of information	9
3.7.2. Unauthorised Access	10
3.7.3. Mandatory training	10
3.8. Security measures	11
3.8.1. Network threats	11
3.8.2. Access is subject to audit	11
3.9. Logging on	11
3.9.1. Logon banner	11
3.9.2. Passphrase requirements	11
3.10. Email and collaboration tools	11
3.10.1. Email use	11
3.10.2. Internal departmental email	12
3.10.3. Government email (other Australian government entities)	12
3.10.4. Non-government email	12
3.10.5. Using departmental email addresses for personal use	12
3.10.6. Personal email accounts	12
3.10.7. Receiving suspect email	13
3.10.8. Email classification and security	13
3.10.9. Govlink	13
3.10.10. Shared email accounts	14
3.10.11. Collaboration tools	14
3.11. Telephony	14
3.11.1. Standard desktop phones	14
3.11.2. Mobility and personally owned devices	15
3.11.3. Accessing public networks/Wi-Fi	15
3.12. Hardware and software	15
3.12.1. Connecting unapproved devices	15
3.12.2. Virus protection	15
3.12.3. Changes to departmental systems	16
3.12.4. Home drive access and use	16
3.12.5. Shared network drive usage and SharePoint	16
3.13. Reporting events	16

OFFICIAL

OFFICIAL

4. Statement of expectation	17
5. Accountabilities and Responsibilities	17
6. Version Control	18
Attachment A – Definitions	20
Attachment B – Assurance and Control Matrix	24
Powers and Obligations	24
Controls and Assurance	24
Attachment C – Consultation	25
Internal Consultation	25
External Consultation	25

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

1. Purpose

This Procedural Instruction (PI) describes the acceptable use of ICT systems and information for the Department of Home Affairs (the Department), which includes the Australian Border Force (the ABF), and directs Immigration and Border Protection workers (IBP workers) whilst using departmental systems. This PI is a key component of, and should be read in conjunction with, the Department's Agency Security Plan – Policy Statement (HR-5535).

This PI incorporates the Australian Government's regulatory requirements for information security under the Protective Security Policy Framework (PSPF), the Information Security Manual (ISM) and the Department's Security Risk Management Framework – Policy Statement (HR-6224).

2. Scope

This PI establishes the acceptable use of the Department's ICT systems and applies to all IBP workers (as defined in subsection 4(1) of the *Australian Border Force Act 2015* (the ABF Act)) who have access to the Department's ICT environment (including remotely) in the course of performing their services for the Department.

For the purpose of this PI, the Department's ICT environment includes, but is not limited to, any IBP worker using a computer, phone, mobile phone, laptop, tablet, printer, fax, smart whiteboard, approved storage device, camera, scanner, server, personal electronic device, electronic peripheral, email, internet, or any service that operates on or is accessed via any device that contains or has ever contained official government information.

3. Procedural Instruction

3.1. Overview and context

The Department is responsible under the PSPF and the ISM for creating and maintaining an environment which achieves and maintains the confidentiality, integrity and availability of all official information.

In the context of the PSPF information security requirements, there are four core information security requirements that the Department **must** apply to achieve the information security outcome:

Policy title	Core requirement
Classification system	Each entity must: - identify information holdings; - assess the security classification of information holdings; and - implement operational controls for these information holdings proportional to their value, importance and sensitivity.

 Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

Policy title	Core requirement
Access to information	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 security classified information have an appropriate security clearance and need-to-know that information; and c. controlling access (including remote access) to supporting ICT systems, networks, infrastructure, devices and applications.
Safeguarding information from cyber threats	Each entity must mitigate common cyber threats by: a. implementing the following mitigation strategies from the <u>Strategies to Mitigate Cyber Security Incidents</u>: i. application control ii. patch applications iii. configure Microsoft Office macro settings iv. user application hardening v. restrict administrative privileges vi. patch operating systems vii. multi-factor authentication viii. regular backups. b. considering which of the remaining mitigation strategies from the <u>Strategies to Mitigate Cyber Security Incidents</u> need to be implemented to achieve an acceptable level of residual risk for their entity.
Robust ICT systems	Each entity must ensure the secure operation of their ICT systems to safeguard information and the continuous delivery of government business by applying the Australian Government Information Security Manual's <u>Cyber Security Principles</u> during all stages of the lifecycle of each system.

s. 47E(d)

3.2. Specific terms

In this PI the following terms require the following actions:

- 'must' or 'needs to' refers to requirements or actions that **have to be** implemented
- 'must not' refers to requirements or actions that **are not to be** implemented

OFFICIAL

- ‘**can, may, or could**’ refers to requirements that if implemented ***will benefit*** the Department
- ‘**are to**’ or ‘**is to**’ are controls that support compliance with the ***mandatory requirements*** of this PI
- ‘**should**’ refers to ***better practice***—agencies are expected to apply *better practice* unless the agency’s risk assessment has identified reasons to apply other controls.

3.3. IBP workers’ responsibilities

3.3.1. IBP workers’ responsibilities when using ICT resources

When using the Department’s ICT environment, IBP workers **must**:

- ensure that information is protectively marked in accordance with the *Handling Protectively Marked Material Procedural Instruction (HR-6361)* and only stored on systems and equipment that are accredited to store or process that level of material;
- handle information in accordance with the *Records Management – Policy Statement (TI-1094)*;

S. 47E(d)

- use an application approved for the relevant protective marking to access, discuss or share official information;

S. 47E(d)

3.3.2. Unacceptable use of ICT resources

When using the Department’s ICT environment, IBP workers **must not**:

- breach any applicable Australian laws, departmental or government policy;

S. 47E(d)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

- disclose or allow the disclosure of any official information without the appropriate authority;
- transmit any OFFICIAL or OFFICIAL: *Sensitive* information to recipients with unauthorised email accounts (including their own and other IBP workers' personal email accounts) without a valid business reason and never to individuals who do not have the need-to-know (noting exceptions in section 3.10.6 regarding personal email accounts);

s. 47E(d)

s. 47E(d)

- attempt to access or install unapproved software or hardware, including web-based platforms and mobile applications;

s. 47E(d)

- engage in actions that are **not** in accordance with the APS Code of Conduct (section 13 of the *Public Service Act 1999* (the PS Act)).

Failure to comply with the requirements specified above may be considered a breach of the APS Code of Conduct. Accordingly, where an IBP worker has been found **not** to have followed the procedures outlined above, their conduct may be referred to Integrity & Professional Standards (I&PS) Branch for assessment.

3.4. External information

s. 47E(d)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL**3.5. Special exemptions for professional use**

S. 47E(d)

3.6. Personal use/reasonable access

Personal use of departmental ICT resources **must** strictly comply with all relevant parts of sections 3.3–3.6 of this PI.

IBP workers are permitted to use the Department's internet access for reasonable personal purposes, provided the use is incidental, is not used to operate a private business or venture, and does not impact on their work or that of their colleagues.

S. 47E(d)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL**s. 47E(d)**

IBP workers who use the Department's ICT resources for personal purposes do so on the understanding that:

- information created on, stored, or transmitted across the Department's ICT resources is not separated from official information and therefore will be treated as the property of the Department;

s. 47E(d)

3.7. Securing the ICT environment

s. 47E(d)

Released by Department of Home Affairs
under the *Freedom of Information Act 1982*

OFFICIAL

OFFICIAL

s. 47E(d)

Released by Department of Home Affairs
under the *Freedom of Information Act 1982*

OFFICIAL

OFFICIAL**3.8. Security measures****3.8.1. Network threats**

S. 47E(d)

3.8.2. Access is subject to audit

S. 47E(d)

3.9. Logging on**3.9.1. Logon banner**

S. 47E(d)

3.9.2. Passphrase requirements

S. 47E(d)

3.10. Email and collaboration tools**3.10.1. Email use**

S. 47E(d)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

3.10.2. Internal departmental email

s. 47E(d)

3.10.3. Government email (other Australian government entities)

s. 47E(d)

3.10.4. Non-government email

s. 47E(d)

3.10.6. Personal email accounts

Unless otherwise authorised³, ICT resources **must not** be used to attempt to access web-based email accounts such as; Gmail, Yahoo, or similar.

s. 47E(d)

IBP workers **must not** send official information to a personal email account. However, information related solely to the IBP worker can be sent to a personal email account in limited circumstances, e.g., payslips, and job applications.

s. 47E(d)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

3.10.7. Receiving suspect email

s. 47E(d)

3.10.8. Email classification and security

s. 47E(d)

s. 47E(d)

3.10.9. Govlink

s. 47E(d)

s. 47E(d)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

3.10.10. Shared email accounts

s. 47E(d)

3.10.11. Collaboration tools

All IBP workers **must** use messaging and collaboration applications approved for the relevant security classification to access, discuss or share official information.

- **Signal** can be used for s. 47E(d), voice, messaging, and video conferencing, when used on a departmental device with no external parties in attendance.

s. 47E(d)

IBP workers **must not** access, discuss or share departmental information via an unapproved messaging or collaboration application, s. 47E(d)

s. 47E(d)

3.11. Telephony

3.11.1. Standard desktop phones

s. 47E(d)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL**s. 47E(d)****3.11.2. Mobility and personally owned devices**

The Department utilises technologies that facilitate connections to applications remotely. IBP workers are not to process official information on personally owned devices unless connected to the Department's approved ICT systems. Official information **must not**, except in the limited circumstances discussed at section 3.10.6, be saved or stored on personally owned devices.

s. 47E(d)**3.11.3. Accessing public networks/Wi-Fi****s. 47E(d)****3.12. Hardware and software****3.12.1. Connecting unapproved devices****s. 47E(d)****3.12.2. Virus protection****s. 47E(d)**

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL**3.12.3. Changes to departmental systems**

s. 47E(d)

3.12.4. Home drive access and use

All official information **must** be stored on the Department's record management system Content Manager (formerly known as TRIM). s. 47E(d)

s. 47E(d)

3.12.5. Shared network drive usage and SharePoint

The Department expects all official information to be stored in official approved systems such as Content Manager etc. s. 47E(d)

s. 47E(d)

3.13. Reporting events

s. 47E(d)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

4. Statement of expectation

The APS Code of Conduct states that an APS employee must comply with any lawful and reasonable direction given by someone in the employee's Agency who has authority to give the direction under subsection 13(5) of the PS Act.

Failure by an APS employee to comply with any direction contained in this document may be determined to be a breach of the APS Code of Conduct, which could result in sanctions up to and including termination of employment, as set out in subsection 15(1) of the PS Act.

The Professional Standards Secretary Direction 2024, issued under subsection 55(1) of the ABF Act requires all IBP workers who are not employed under the PS Act to comply with any lawful and reasonable direction given by someone in the Department with authority to issue that direction.

Failure by an IBP worker who is not an APS employee to comply with a direction contained in this PI may be treated as a breach of the Professional Standards Secretary Direction 2024, which may result in the termination of their engagement under section 57 of the ABF Act. Non-compliance may also be addressed under the terms of the contract engaging the contractor or consultant.

5. Accountabilities and Responsibilities

Role	Description
Assistant Secretary Cyber Risk Services	- Responsible for approving this PI (Document owner) - Escalation authority for violations relating to this PI - Management of access to inappropriate internet sites.
Connected Services	Facilitates procurement in accordance with the Department's approved ICT procurement procedures.
Cyber Detection and Response Section	Responsible for monitoring IBP worker actions while using the departmental ICT environment (e.g. using departmental email systems) and escalating to the appropriate authority, as required.
Cyber Risk Management Section	Responsible for drafting and maintaining this PI in accordance with Policy and Procedure Control Framework (PPCF) guidelines.
Cyber Risk Services Branch	- Responsible for approving connection of any external information source or device to any part of the network and/or accessing the information - Responsible for approving access internet sites and services that would otherwise be considered inappropriate - Monitoring of Department's network for unapproved devices.
IBP workers	Responsible for following all instructions as described within this PI.
Information Technology Security Advisor	- Responsible for providing cyber security advice in relation to this PI - Responsible for authorising exemptions from this PI - Responsible for approving portable electronic device(s) access in a restricted zone.

OFFICIAL

Role	Description
Integrity and Professional Standards Branch	- Responsible for the development and maintenance of the Department's integrity framework - Responsible for, but not limited to, investigating and/or evaluating varying circumstances such as: - potential breach of the APS Code of Conduct - deliberate misuse of information systems or resources - corruption or criminality (inside and outside of work) - conducting employment suitability assessments, and - assessments of integrity related information.
Line Management	- Responsible for determining the level of acceptable personal use of ICT resources by IBP workers under their responsibility - Responsible (EL2 or above) for approval of access to inappropriate internet sites (subject to authorisation from Cyber Risk Services Branch) - Responsible (SES Band 1 and above) for approval of removing any official information outside the Department facilities without a valid business reason.
Security Branch	- Responsible for operating the SCC - Responsible for managing the <u>Protective Security Portal</u> - Responsible for approving business cases to take printed departmental OFFICIAL and OFFICIAL: <i>Sensitive</i> material home for the purpose of working from home - Responsible for advice on secure telephone systems.

6. Version Control

Version number	Date of issue	Author(s)	Brief description of change
0.1	15/06/2022	s. 22(1)(a)(ii)	Minor administrative updates to previous document (ADD2021/2167699).
0.2	21/09/2022	s. 22(1)(a)(ii)	Incorporated stakeholder feedback.
0.3	10/11/2022	s. 22(1)(a)(ii)	Incorporated all staff consultation feedback.
0.4	20/12/2022	Legal Group	Legal review.
0.5	22/12/2022	s. 22(1)(a)(ii)	Legal changes implemented.
0.6	30/03/2023	s. 22(1)(a)(ii)	Minor amendment: update to telephony section reflecting uplift of phone capabilities.

Released by Department of Home Affairs under the Freedom of Information Act 1982

OFFICIAL

Version number	Date of issue	Author(s)	Brief description of change
0.7	4/07/2023	s. 22(1)(a)(ii)	Minor amendment: inclusion of section 3.11.3 relating to accessing public networks/Wi-Fi, some additional minor formatting changes, and removal of obsolete collaboration tools.
0.8	26/08/2024	s. 22(1)(a)(ii)	Minor amendment cleared with Director, Cyber Risk Management.
0.9	19/11/2024	s. 22(1)(a)(ii)	Minor amendment: updates to s 3.3.2 and s 3.7 relating to unauthorised access; update to s 3.7 to align with <i>Employment Suitability Screening – PI (SM-1554)</i> .
10	20/12/2024	s. 22(1)(a)(ii)	Minor amendment cleared with Director, Cyber Risk Management.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

Attachment A – Definitions

Term	Acronym (if applicable)	Definition
Australian Border Force	ABF	As defined in section 4 of the <i>Australian Border Force Act 2015</i>. The Australian Border Force means that part of the Department known as the Australian Border Force. The Australian Border Force, as operationally independent body within the Department of Home Affairs, is Australia's frontline border law enforcement agency and Australia's customs service. The Australian Border Force delivers critical border protection and national security outcomes while facilitating the movement of people and goods across the border.
Employment Suitability Screening	ESS	The ESS process is used by the Department to assess whether an individual is suitable to have non-public access to the Department's assets (for example, premises, information, systems or assets). Refer to the <u><i>Employment Suitability Screening – Procedural Instruction (SM-1554)</i></u> for further guidance.
Immigration and Border Protection Worker	IBP worker	This term is defined in subsection 4(1) of the ABF Act, and includes but is not limited to: • all APS employees in the Department; • persons employed by an agency under the <i>Public Service Act 1999</i> who are made available to the Department (often referred to as 'seconded');; • certain persons engaged as consultants or contractors to perform services for the Department 'in-house' in the Department; and • certain persons engaged as consultants or contractors to perform services for the Department that require non-public access to departmental assets. See also the Secretary's Determination of IBP Workers.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

Term	Acronym (if applicable)	Definition
Inappropriate sites		Sites that contain material that is inappropriate for usual access by IBP workers, such as (list is non-exhaustive): • adult/mature content/pornography/intimate apparel/nudity; • child grooming, including sexual exploitation and abuse; • chat/messaging/social media/media sharing/online meetings; • extreme violence/hate/racism/weapons; • gaming/gambling, dating/personal; and • illegal drugs.
Information		Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.
Information and Communications Technology environment	ICT environment	The Department's ICT environment includes, but is not limited to, any IBP worker using a computer, phone, mobile phone, laptop, tablet, printer, fax, smart whiteboard, approved storage device, camera, scanner, server, personal electronic device, electronic peripheral, email, internet, or any service that operates on or is accessed via any device that contains or has ever contained official government information.
Information Security Manual	ISM	The <i>ISM</i> outlines a cyber security framework that an organisation can apply, using their risk management framework, to protect their systems and data from cyber threats based the advice of the Australian Cyber Security Centre (ACSC) within the Australian Signals Directorate (ASD).

 Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

Term	Acronym (if applicable)	Definition
Need-to-know		The need-to-know principle applies to all departmental, or classified information. The principle restricts access or attempted access to records and information to only those that require it to fulfil the duties of their role. The need-to-know principle excludes people accessing information based on: • Convenience; • Personal or professional interest; • Someone's status, position, or rank; • Someone's level of authorised access (e.g. security clearance); or • Acting on behalf of another person, including other departmental employees, where such access would constitute an unauthorised access if undertaken by that other person.
Official information		Official information is all information created, sent and 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. (<i><u>Policy 8: Classification system</u></i> <i><u>Protective Security Policy Framework</u></i>)
Protective Security Policy Framework	<i>PSPF</i>	The <i>PSPF</i> 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, information security, personnel security and physical security. The Department of Home Affairs as a non-corporate Commonwealth entity subject to the <i>Public Governance, Performance and Accountability Act 2013</i> (the <i>PGPA Act</i>) must apply the <i>PSPF</i>.
Trusted		Something which: • is subject to Australian laws and regulations; • can be considered reasonably secure from intrusion or misuse; • functions correctly and provides a reasonable level of reliability; and is not associated with an entity owned, funded or influenced by a foreign government.
Untrusted		Something which is unknown or not trusted.

 Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

Term	Acronym (if applicable)	Definition
Valid business reason		A valid business reason must exist in order for an IBP worker to access any: departmental, or classified information; ICT system; or depart from an approved procedure. The valid business reason must consider legislation, policy, risk, and the need-to-know principle, and serves as justification for the access or action. An individual has a 'valid business reason' where each of the following requirements are met: 1. It must be necessary for the performance of official duties for the Department which includes the ABF and directly relevant to a current business deliverable; 2. Access and use of the information and/or systems must be lawful; 3. The need-to-know principle must be applied; 4. A conflict of interest must not exist; and 5. A valid business reason must be accepted and approved by an authorised person where outlined in this PI.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

Attachment B – Assurance and Control Matrix

Powers and Obligations

Implementation of this PI supports the requirements under section 16 of the PGPA Act but does not require any powers, delegations or authorisations.

Controls and Assurance

Related Policy	<u>Security Incident Reporting – Procedural Instruction (SM-7126)</u> <u>Agency Security Plan – Policy Statement (HR-5535)</u>
Procedures / Supporting Materials	<u>Employment Suitability Screening – Procedural Instruction (SM-1554)</u> <u>Information and Communications Technology Access Control - Procedural Instruction (TI-1618)</u> <u>Use of social media and other online services - Procedural Instruction (SM-1560)</u> <u>Handling Protectively Marked Material - Procedural Instruction (HR-6361)</u> <u>Passphrase Management – Supporting Material (TI-6548)</u> <u>Removable media devices - PI (TI-5264)</u>
Training/Certification or Accreditation	Staff Induction Training and 'The Essentials Suite' (annually).
Other required job role requirements	Nil
Other support mechanisms (e.g. who can provide further assistance in relation to any aspects of this instruction)	Advice can be provided by the Information management and systems home page: http://intranet.bcz.gov.au/corporate/information and the IT security policies home page: http://intranet.bcz.gov.au/corporate/information/ict-security-policies
Escalation arrangements	Reporting of unacceptable use of IT resources is to be sent to the SCC via s. 22(1)(a)(ii)@homeaffairs.gov.au Queries can be submitted to Cyber Risk Management Section via mailbox: s. 22(1)(a)(ii)@homeaffairs.gov.au
Recordkeeping (e.g. system based facilities to record decisions)	Content Manager 10 (TRIM)
Program or Framework (i.e. overarching Policy Framework or Business Program)	<u>Australian Government Protective Security Policy Framework (PSPF)</u> <u>Information Security Manual (ISM)</u>
Job Vocational Framework Role	This PI applies to all job roles within the Department.

OFFICIAL

Attachment C – Consultation

Internal Consultation

The following internal stakeholders have been consulted in the development of this PI:

- Workforce Management and Conditions Section (Industrial Relations)
- ICT Division
- Security Branch
- Cyber Risk Management Section
- Cyber Detection and Response Section
- Integrity and Professional Standards Branch
- IT Security Advisor
- Major Capability Division
- Collaboration Infrastructure Services Section
- Organisational Compliance and Assurance Section Records Management Section
- All staff (myHR)
- Legal Group.

External Consultation

The following external stakeholders have been consulted in the development of this PI:

- Community and Public Sector Union (CPSU).

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL



OFFICIAL

Smart Mobile Device Security

Procedural Instruction

Document ID (PPN)	TI-6664
TRIM record number	ADD2023/3252187
BCS Function	Technology and Information Management
Document owner	Assistant Secretary Cyber Risk Services
Approval date	11 February 2021
Document Contact	Cyber Risk Management – s. 22(1)(a)(ii)@homeaffairs.gov.au

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

OFFICIAL**Table of Contents**

1. Purpose	4
2. Scope	4
2.1. In scope	4
2.2. Out of scope	4
3. Overview	5
4. Key principles	5
5. Procedural Instruction	6
5.1. Procurement and allocation	6
5.1.1. Hardware procurement	6
5.1.2. Device allocation	6
5.1.3. Specific/unlisted mobile devices	7
5.1.4. Bring Your Own Device (BYOD)	7
5.1.5. Mobile device credentials	7
5.1.6. Duty or pool devices	7
5.1.7. Carriage services provider	8
5.1.8. Accessories	8
5.2. Using a departmental mobile device	8
5.2.1. Acceptable use of departmental mobile devices	8
5.2.2. Reasonable personal use	8
5.2.3. Handling information	9
5.2.4. Approved applications for communicating	9
5.2.5. Cloud and synchronisation	10
5.2.6. Accessing public networks/Wi-Fi	10
5.2.7. Application restrictions	10
5.2.8. Overseas use	11
5.2.9. Use within Security Zone areas	11
5.3. Protecting departmental mobile devices	12
5.3.1. Physical security	12
5.3.2. Loss, theft or damage	12
5.3.3. Mobile Device Management	13
5.3.4. Encryption	13
5.3.5. Operating system and application updates	13
5.3.6. Device passcode settings	13
5.3.7. Connectivity	14
5.3.8. Remote wipe	14
5.3.9. Arrangements during extended leave	14
5.4. Disposal of departmental mobile devices	15
5.4.1. Returning a device	15
5.4.2. Sanitisation and disposal	15
5.5. Monitoring and system logs	15
5.6. Personal/externally-owned mobile devices	15
5.7. Reporting	17
5.7.1. Security Coordination Centre	17
5.7.2. Cyber Security Operations Centre	17
5.7.3. Telecom Assets team	17

OFFICIAL

5.8. Exemptions	17
6. Accountabilities and Responsibilities	18
7. Version Control	21
Attachment A – Definitions	22
Attachment B – Assurance and Control Matrix	27
1.1. Powers and Obligations	27
1.2. Controls and Assurance	27
Attachment C – Consultation	28
1.1. Internal Consultation	28
1.2. External Consultation	28

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

1. Purpose

This Procedural Instruction (PI) outlines procedures for managing Department of Home Affairs (the Department) security in the context of smart mobile devices (mobile devices).

The Agency Security Plan - Policy Statement (HR-5535) sets out the context and fundamental governance arrangements for protective security for the Department under the Australian Government's Protective Security Policy Framework (PSPF). The Agency Security Plan defines the key elements for the Department to meet its obligations under the PSPF and establishes the context for a suite of complementary policies, procedures and practices related to protective security in the Department.

This PI forms part of a suite of documents relating to the PSPF Information security outcome—*each entity maintains the confidentiality, integrity and availability of all official information*—and establishes procedures to implement relevant elements of:

- Policy 8, *Sensitive and classified information*;
- Policy 10, *Safeguarding information from cyber threats*; and
- Policy 11, *Robust ICT systems*.

To maintain best practice, this PI draws on relevant security controls in the Australian Government Information Security Manual (ISM), particularly controls for managing enterprise mobility.

2. Scope

2.1. In scope

This PI applies to all IBP workers, including service providers and vendors, who use departmental issued mobile devices.

These procedures apply to the management of smart mobile devices (mobile devices) only. Mobile devices are defined as devices which:

- are a multi-function or general-purpose computing platform;
- are lightweight and small in nature—generally able to be held/used in one hand;
- incorporate a self-contained power source; and
- have independent capability to transmit information wirelessly.

Typical examples of mobile devices under this definition are smartphones (iPhones, Android phones, etc.) and tablet computers (iPads, Android tablets, etc.).

2.2. Out of scope

This PI does not provide instructions for the management of devices other than mobile devices.

The following categories of devices are managed under other departmental cyber security policy framework documents:

- | | |
|---|--|
| • Laptop/notebook computers and Microsoft Surface tablets | • External hard drives/flash memory/memory cards |
| • Smartwatches/fitness trackers | • Satellite phones* |
| • Wireless headphones/keyboards/mice | • Handheld radio frequency devices |
| • eReaders* | • Single-function cell phones. |

OFFICIAL

* Where functionality is limited. Note: Some devices may be more appropriately categorised as a tablet computer or smartphone. If in doubt, please contact the Information Technology Security Advisor at [s.22\(1\)\(a\)\(i\)@homeaffairs.gov.au](mailto:s.22(1)(a)(i)@homeaffairs.gov.au).

The disclosure of official information to any person in accordance with relevant departmental policy and procedures is outside the scope of this document.

3. Overview

Mobile devices such as smartphones and tablet computers are powerful tools which have become familiar and ubiquitous within the workplace and for personal use. These devices can perform many functions and can be adapted to suit multiple purposes. This provides a valuable capability to the Department, facilitating the availability of information and systems for an increasingly flexible workforce. However, mobile devices introduce particular risks to ensuring the confidentiality and integrity of the information and systems.

These risks must be managed appropriately to ensure the confidentiality and integrity of departmental information is maintained.

Some of the increased areas of risk for the Department which result from mobile devices include:

- **Data loss** - mobile devices are particularly susceptible to loss, theft or damage, which can make critical data and information irretrievable.
- **Data exposure** - the wide-ranging connectivity of mobile devices can leave sensitive data exposed through unsecure connections, such as public Wi-Fi networks.
- **Device and network compromise** - using insecure devices within sensitive and classified networks can provide a vector for cyber threats to compromise departmental information and communication technology (ICT) systems.

The risks associated with mobile devices are not only associated with departmental assets. Personal mobile devices used by IBP workers may compromise departmental information and systems if misused. Policy, administrative and technical controls outlined within this PI address the risks associated with both departmental and externally-owned mobile devices.

4. Key principles

The following key principles outline the broad departmental position for managing mobile devices owned by the Department or used on departmental premises.

- Departmental mobile devices must be procured from reputable manufacturers or their authorised reseller, and in an authorised manner. Procurement decisions at any value bracket must adhere to Policy 6 of the PSPF - Security governance for contracted goods and service providers, and consider supply chain risks, particularly extrajudicial and state-based control and influence.
- Departmental mobile devices must be protected from compromise through isolation from unsecure connections and the implementation of defence-in-depth security measures encompassing administrative, technical and physical controls.
- Departmental mobile devices must be subject to device management protocols for the purpose of maintaining robust ICT systems and mitigating common and emerging cyber threats. IBP workers issued with a departmental mobile device must take steps as directed by Cyber Risk Services (CRS) to ensure device management protocols are applied and maintained.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

- Despite any security controls in place on a mobile device, a residual level of risk to the confidentiality and integrity of departmental information remains. IBP workers using departmental mobile devices are subject to the Acceptable use of Departmental ICT Systems and Information - Procedural Instruction (HR-3320) and all security procedures applicable to specific work areas.
- Personal and externally-owned mobile devices are permitted to be used within departmental premises, subject to the Acceptable use of Departmental ICT Systems and Information - Procedural Instruction (HR-3320) and all security procedures applicable to specific work areas.
- Mobile devices are particularly vulnerable during travel outside of Australia. Additional procedures and controls for the protection of departmental mobile devices must be implemented when an IBP worker travels internationally.
- Departmental mobile devices must be securely disposed of when no longer required by the Department. Devices must be appropriately sanitised prior to the destruction, storage, sale or transfer of the device.

5. Procedural Instruction

5.1. Procurement and allocation

s. 22(1)(a)(ii)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

s. 22(1)(a)(ii)

5.1.5. Mobile device credentials

s. 47E(d)

5.1.6. Duty or pool devices

s. 47E(d)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

s. 22(1)(a)(ii)

5.2. Using a departmental mobile device

5.2.1. Acceptable use of departmental mobile devices

IBP workers using departmental mobile devices are subject to the Acceptable use of Departmental ICT Systems and Information - Procedural Instruction (HR-3320). IBP workers, including service providers and vendors, must comply with instructions concerning the use of departmental mobile devices at all times. This includes when outside departmental premises or when using the device for personal activities.

Workers must be aware that all information created on, stored on or transmitted via departmental ICT assets, including mobile devices, will be handled as official information and considered the property of the Department.

Departmental mobile devices are subject to monitoring and analysis. Personal information stored or accessed on a device may be reviewed during monitoring activities. Workers should not store or access personal information they wish to remain private using a departmental mobile device. Workers take full responsibility for any personal and/or financial information transmitted using the mobile device, including any consequences associated with this use.

The Department is not responsible for the loss, corruption, back-up or archiving of personal information and data stored on departmental mobile devices.

5.2.2. Reasonable personal use

IBP workers may use departmental mobile devices for reasonable personal activities, subject to security procedures that are in effect within their specific work area (outlined in section 5.2.9). Managers have discretion to determine whether reasonable personal use has been breached. CRS and Telecom Assets may also determine whether reasonable personal use has been breached, when authorised to do so by the Chief Security Officer (CSO), the Chief Information Security Officer (CISO) or the Deputy Chief Information Security Officer (DCISO). Generally, personal use of departmental mobile devices must not:

- circumvent or violate any lawful direction within:
 - this PI;
 - the Use of Social Media and Other Online Services - Procedural Instruction (SM-1560); and

 Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

- o the Acceptable use of Departmental ICT Systems and Information - Procedural Instruction (HR-3320).

- cause excess call and/or data usage, including Department network bandwidth;
- have an adverse or marked effect or influence upon a workers capacity (including that of their colleagues) to perform their duties with consideration to output, accuracy and efficiency; and
- undertake unsafe activities, such as auto-forwarding personal emails to a departmental email account to enable access to them on a departmental issued device.

CRS and ICT Division monitor departmental mobile devices to identify usage patterns which may indicate unreasonable personal use. Unreasonable personal use may be referred to Integrity and Professional Standards Branch for assessment under the Department's Professional Standards and Integrity frameworks.

5.2.3. Handling information

Departmental mobile devices may be used to access, store, process and communicate departmental information. IBP workers must adhere to the need-to-know principles which apply to all departmental information and systems - workers must only access official information and ICT systems which they require to undertake their role/duties.

S. 47E(d)

IBP workers must not provide a departmental mobile device to another person, even to make a phone call or check the weather, except in emergency circumstances. Workers must monitor any use of the device to ensure official information is not compromised. Duty or pool devices may be shared with another worker where measures outlined at section 5.1.6 are in place.

5.2.4. Approved applications for communicating

S. 47E(d)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

s. 47E(d)

5.2.5. Cloud and synchronisation

s. 47E(d)

IBP workers using a personal AppleID must take reasonable steps to ensure any native device applications, or those downloaded via the App Store, do not synchronise departmental information with other personal devices. Workers should:

- review application settings to turn off any synchronisation of data;
- review AppleID settings to turn off any synchronisation of data; and
- check application permissions when downloading a new application.

The Department does not ordinarily issue non-Apple mobile devices. However, the principles outlined in this section would similarly apply to non-Apple mobile devices.

s. 22(1)(a)(iii)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

s. 22(1)(a)(ii)

s. 22(1)(a)(ii)

s. 47E(d)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

s. 47E(d)

5.3. Protecting departmental mobile devices

s. 22(1)(a)(i)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

s. 22(1)(a)(ii)

S. 47E(d)

s. 22(1)(a)(ii)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

s. 47E(d)

s. 22(1)(a)(ii)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

s. 22(1)(a)(ii)

5.5. Monitoring and system logs

All usage of departmental mobile devices is subject to the ICT Event Logging and Auditing - Procedural Instruction (TI-6481).

Further, all events and activity on departmental mobile devices will be logged and recorded by the MDM solution. This information must be available for analysis and audit when required.

Monitoring may result in a referral to the SCC or Integrity and Professional Standards Branch.

5.6. Personal/externally-owned mobile devices

IBP workers must not use personal/externally-owned (non-departmental) mobile devices to store or process official information. However, workers may use a non-departmental mobile device to access and communicate official information, when using a method endorsed by the Department.

IBP workers must use an endorsed application when communicating departmental information using a non-departmental mobile device.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

S. 47E(d)

Note: Endorsed applications are not appropriate for recording official decisions. IBP workers must extract any official decisions made via an endorsed application and record it in a departmental recordkeeping system, in accordance with the Department's record keeping policy.

There are no endorsed applications for emailing official information from a non-departmental mobile device.

Where a service provider has a contract in place which specifies conditions where they may access, store, process, or communicate official information, they may do so using non-departmental mobile devices in accordance with any specific security requirements in that contract, and the Acceptable use of Departmental ICT Systems and Information - Procedural Instruction (HR-3320).

IBP workers may carry and use non-departmental mobile devices within departmental premises, subject to any security procedures applicable to the work area. Non-departmental mobile devices must not be taken into a Zone 4 area, unless an exemption for vital health/medical reasons or as a mobile device issued by another government agency is approved in accordance with section 5.2.9.

IBP workers must limit the use of non-departmental mobile devices to a reasonable level while performing official duties. Reasonable use is determined at the discretion of a worker's manager. Generally, reasonable use under this section would be defined as:

- incidental and not having an adverse or marked effect or influence upon a workers capacity (including that of their colleagues) to perform their duties with consideration to output, accuracy and efficiency;
- acting in accordance with any applicable Australian laws or Government or departmental policy, including:
 - o this PI;
 - o the Use of Social Media and Other Online Services - Procedural Instruction (SM-1560);
 - o the Acceptable use of Departmental ICT Systems and Information - Procedural Instruction (HR-3320).
- not accessing or conveying inappropriate content (for example; sexually explicit, racist, sexist, offensive, or politically extreme material); and
- not engaging in actions that are in conflict with section 13 of the *Public Service Act 1999* – the APS Code of Conduct.

Non-departmental mobile devices must not be used by IBP workers to circumvent controls established to protect official information (for example, using a mobile device to photograph information displayed on a workstation monitor). Care should also be taken to ensure non-departmental mobile devices do not directly or indirectly capture official information, such as photographing a whiteboard after a planning meeting, or capturing official information in the background of a photo.

IBP workers travelling to a high-risk country should consider leaving non-departmental mobile devices in Australia. Non-departmental mobile devices are at equal risk of loss and compromise as departmental

 Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

devices if a worker is targeted overseas. Workers should familiarise themselves with advice published by the ACSC on Travelling Overseas with Electronic Devices.

5.7. Reporting

5.7.1. Security Coordination Centre

All security events, including those relating to misuse or potential compromise of departmental mobile devices must be reported to the SCC using the Security Event Reporting Portal, as per the Security Event Reporting - Policy Statement (TI-5256). The SCC will liaise with relevant stakeholders to resolve security events, such as Integrity and Professional Standards or the Cyber Security Operations Centre (CSOC).

Even if the CSOC is contacted for an urgent response, the security event must still be reported to the SCC.

5.7.2. Cyber Security Operations Centre

Urgent or after-hours reports can be made to the CSOC by phone: s. 22(1)(a)(ii) or email: s. 22(1)(a)(ii)@homeaffairs.gov.au for action and escalation as appropriate.

5.7.3. Telecom Assets team

Most requests and reports to the Telecom Assets team must be submitted through the Connected Services Portal. Additional enquiries not facilitated within the CSP, such as reporting damage to a device, may be emailed to s. 22(1)(a)(ii)@homeaffairs.gov.au.

5.8. Exemptions

Any exemptions to the procedures described in this PI, must be referred to the ITSA for review and appropriate approval and/or escalation. This exemption process does not apply where an alternative method is described within procedures (for example, exemptions to allow the use of a mobile device in a Zone 4 area).

Requests for exemption must be emailed to s. 22(1)(a)(ii)@homeaffairs.gov.au and provide:

- a reference to the policy/procedures the exemption applies to
- a detailed description of the intended activity
- a valid business reason for the exemption
- an assessment of the risk of the activity
- any proposed controls to mitigate the risk
- endorsement by the relevant manager (minimum Director/Superintendent, though SES clearance may be also be requested)

The ITSA may reject any request for an exemption where the risk is assessed as unacceptable in reference to the Departments risk tolerance guide, departmental security risk management plans, a cyber security incident or an emerging cyber security threat.

Any existing approval by the ITSA may be withdrawn should the assessed risk change.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

6. Accountabilities and Responsibilities

Role	Description
Assistant Secretary Cyber Risk Services	- Responsible for approving this PI and ensuring it is maintained appropriately (Document owner). - Escalation authority for violations relating to this PI. - Performs the role of Deputy Chief Information Security Officer.
Chief Information Security Officer	- Responsible for managing communication between security, ICT and business functions to ensure the alignment of business and security objectives. - Responsible for providing strategic level guidance for the Department's security program by ensuring compliance with national policy, regulation, and legislation.
Cyber Risk Management	- Responsible for drafting and maintaining this PI in accordance with PPCF guidelines. - Responsible for coordinating ITSA advice and guidance in relation to this PI.
Cyber Prevention	- Responsible for identifying intelligence on vulnerabilities, proofs of concept, and active exploitation of mobile device operating systems and mobile applications. - Responsible for assessing cyber security vulnerabilities identified in departmental mobile devices and issuing advice to the Telecom Assets team. - Responsible for assessing intelligence on mobile applications of concern, and issuing advice to Cyber Risk Management or Cyber Detection and Response sections.
Cyber Detection and Response	- Responsible for monitoring event and activity logs relating to mobile device use on the Department's network and identifying threats and potential compromises. - Responsible for managing the CSOC and coordinating responses to cyber security events or escalating to the appropriate authority, as required. - Responsible for maintaining and allocating the Overseas Mobile Device fleet.
Cost Centre Managers	- Responsible for managing cost centre resources and making sound financial decisions. - Responsible for ensuring requests for departmental mobile devices are submitted and approved through the appropriate channel.
Deputy Chief Information Security Officer	Supports the Chief Information Security Officer.

Released by Department of Home Affairs under the Freedom of Information Act 1982

OFFICIAL

Role	Description
Group Manager Technology and Major Capability Group	Performs the role of Chief Information Security Officer.
Security Branch	- Responsible for establishing and maintaining access controlled zones at departmental premises. - Responsible for managing the SCC and Security Event Reporting Portal, and coordinating responses to security events.
Senior Executive Service officers	Responsible for understanding, accepting and managing the risk posed by mobile devices in Zone 4 areas which they are responsible for.
ICT Hardware Procurement team	Responsible for ensuring all purchases of departmental mobile devices are made in accordance with Accountable Authority Instructions (Part 3 – Procurement), the Commonwealth Procurement Rules, departmental policy and this PI.
Information Technology Security Adviser	- Responsible for providing cyber security advice in relation to this PI. - Responsible for approval of exemptions/implementation of processes relating to departmental mobile devices which are not outlined in this PI.
Unisys / IT Support	Responsible for providing level one ICT support to workers regarding departmental mobile devices.
Telecom Assets team	- Responsible for initiating procurement requests for departmental mobile devices. - Responsible for service delivery, management, maintenance and sanitisation/end of life procedures for the departmental mobile device fleet. - Responsible for implementing and enforcing mobile device management protocols. - Responsible for the delivery of end-user communications regarding security patch updates.
Managers	- Responsible for determining if the personal use of a departmental mobile device by a worker they supervise is reasonable. - Responsible for determining if the personal use of an externally-owned mobile device in the workplace by a worker they supervise is reasonable. - Responsible for considering whether workers they supervise have a valid business reason for a departmental mobile device, and instructing them to return it if not.

 Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

Role	Description
IBP workers	- Responsible for maintaining awareness of the Department's mobile device policy and procedures. - Responsible for securing departmental mobile devices when not in use. - Responsible for using departmental mobile devices in accordance with the <u>Acceptable use of Departmental ICT Systems and Information - Procedural Instruction (HR-3320)</u> and this PI. - Responsible for reporting the loss, damage or suspected compromise of departmental mobile devices.

6.1. Statement of Expectation

The APS Code of Conduct states that 'an APS employee must comply with any lawful and reasonable direction given by someone in the employee's Agency who has authority to give the direction' (subsection 13(5) of the *Public Service Act 1999* (Cth) (Public Service Act)).

Failure by an APS employee to comply with any direction contained in a PPCF document may be determined to be a breach of the APS Code of Conduct, which could result in sanctions up to and including termination of employment, as set out in subsection 15(1) of the Public Service Act.

The Secretary's Professional Standards Direction, issued under subsection 55(1) of the *Australian Border Force Act 2015* (Cth) (Australian Border Force Act), requires all IBP workers who are not APS employees (such as contractors or consultants) to comply with any lawful and reasonable direction given by someone in the Department with authority to issue that direction.

Failure by an IBP worker who is not an APS employee to comply with a direction contained in a PPCF document may be treated as a breach of the Professional Standards Direction, which may result in the termination of their engagement under section 57 of the Australian Border Force Act. Non-compliance may also be addressed under the terms of the contract engaging the contractor or consultant.

For all other provisions of PPCF documents, the Secretary and the Commissioner of the ABF expect all IBP workers to:

- consider whether a proposed departure from any provision set out in a PPCF document is reasonable and justified in the circumstances;
- consider the risks of departing from any provision set out in a PPCF document;
- be responsible and accountable for the consequences of departing from, or not adhering to the content of all PPCF documents, including where such departure or non-adherence results in a breach of any legal or other obligations which lead to adverse outcomes for the Department; and
- be responsible for documenting the reasons/justification for their decision to depart from, or not adhere to, any PPCF document.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

7. Version Control

Version number	Date of issue	Author(s)	Brief description of change
1.0	11/02/2021	s. 22(1)(a)(ii)	Initial publication.
1.1	11/05/2021	s. 22(1)(a)(ii)	Minor update to overseas travel security procedures and application classifications.
1.2	23/09/2021	S Hugo	Minor Updates to reflect the departments Zone 4 security policies
1.3	11/05/2022	s. 22(1)(a)(ii)	Minor Updates to reflect new form to complete and submit for Zone 4 access
1.4	24/06/2022	s. 22(1)(a)(ii)	Minor Updates to remove reference to a defunct form.
1.5	06/03/2023	s. 22(1)(a)(ii)	Minor update to include Teams guidance.
1.6	2/06/2023	s. 22(1)(a)(ii)	Minor update to incorporate DCISO change to s 5.2.7.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

OFFICIAL

Attachment A – Definitions

Term	Acronym (if applicable)	Definition
Australian Cyber Security Centre	ACSC	The ACSC is the leading operational arm for the Australian Government responsible for strengthening the nation's cyber resilience, and for identifying, mitigating and responding to cyber threats against Australian interests.
Chief Information Security Officer	CISO	The CISO provides strategic-level guidance for the Department's cyber security program and ensures the agency's compliance with cyber security policy, standards, regulations and legislation. The CISO is also the Authorising Officer that will issue the Interim Authority to Operate for systems below TOP SECRET and for commercial providers providing services to the Department, where the risks are assessed to be High.
Cloud services		As defined by the Australian Cyber Security Centre, services that enable "network access to a shared pool of computing resources such as data storage, servers, software applications and services."
Connected Services Portal	CSP	The Department's self-service web interface for requesting IT goods and services, managing those requests, or approving requests for others.
Cyber Security Operations Centre	CSOC	The CSOC operates within the CRS Branch and is responsible for the defence of the Department's network and ICT systems and continuously monitors, detects and reports on cyber security events and investigates cyber security incidents.
Department of Home Affairs	The Department	The Department of Home Affairs.
Deputy Chief Information Security Officer	DCISO	The DCISO assists the CISO in the performance of their responsibilities and functions under the PSPF and is the Authorising Officer that will issue the Authority to Operate for ICT systems below TOP SECRET and for commercial providers providing ICT services to the Department, where the risks are assessed to be Medium or lower. The DCISO is also the Authorising Officer to implement the appropriate responses to ICT security incidents and acts as an advisor to the Department's Chief Security Officer on matters related to information and ICT security.
Externally-owned		An item which is not owned or managed by the Department.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

Term	Acronym (if applicable)	Definition
Immigration and Border Protection worker	IBP worker	Immigration and Border Protection worker means: (a) an APS employee in the Department; or (b) a person covered by paragraph (d), (e) or (f) of the definition of officer of Customs in subsection 4(1) of the <i>Customs Act 1901</i>; or (c) a person covered by paragraph (f) or (g) of the definition of officer in subsection 5(1) of the <i>Migration Act 1958</i>; or (d) a person who is: (i) an employee of an Agency (within the meaning of the <i>Public Service Act 1999</i>); or (ii) an officer or employee of a State or Territory; or (iii) an officer or employee of an agency or authority of the Commonwealth, a State or a Territory; or (iv) an officer or employee of the government of a foreign country, an officer or employee of an agency or authority of a foreign country or an officer or employee of a public international organisation; and whose services are made available to the Department; or (e) a person who is: (i) engaged as a consultant or contractor to perform services for the Department; and (ii) specified in a determination under subsection 5(1); or (f) a person who is: (i) engaged or employed by a person to whom paragraph (e) or this paragraph applies; and (ii) performing services for the Department in connection with that engagement or employment; and (iii) specified in a determination under subsection 5(2).
Information and Communication Technology	ICT	The generic term used to describe the infrastructure and components that make up the technology environment.
Information Security Manual	ISM	The ISM is a set of guidelines produced by the ACSC to assist organisations in using their risk management framework to protect their information and systems from cyber threats.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

Term	Acronym (if applicable)	Definition
Information Technology Security Adviser	ITSA	The ITSA is responsible for information technology security management across the agency, and acts as the first point of contact for the CISO and the DCISO and external agencies on any information technology security management issues. The ITSA also advises System Business Owners and System Technical Owners of the level of information security risk presented to the agency arising from ICT systems and their operation and management. The ITSA is also the Certification Authority for ICT systems operated or consumed by the agency and makes recommendations to the CISO and DCISO regarding their fitness for purpose and security accreditation status.
IT Support workers		A user employed or contracted by the Department to support the workforce in accessing departmental ICT systems and supporting the efficient resolution of any issues which occur.
Need-to-know		The need-to-know principle applies to all departmental, sensitive, or classified information. The principle restricts access or attempted access to records and information to only those that require it to fulfil the duties and functions of their role. The need-to-know principle excludes people accessing information based on: • convenience; • personal or professional interest; • someone's status, position, or rank; • someone's level of authorised access (e.g. security clearance); or • acting on behalf of another person, including other departmental employees, where such access would constitute an unauthorised access if undertaken by that other person.
Official information		Official information is all information created, sent and 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. (<u>PSPF – INFOSEC-8 Sensitive and classified information</u>)
Policy and Procedure Control Framework	PPCF	An internal framework outlining governance arrangements for all organisational policies and procedures, providing direction to all departmental workers on the development and management of policy and procedure documents.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

Term	Acronym (if applicable)	Definition
Protective Security Policy Framework	PSPF	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, information security, personnel security and physical security.
Sanitisation		Sanitisation is the process of removing information from media so that the information is not recoverable. This differs to simply deleting or formatting media, as these processes do not completely remove the information, they simply remove the reference to the information.
Security Coordination Centre	SCC	The central collation point for security event reporting, which conducts targeted analysis and trend reporting on reported security events. It is also responsible for the day-to-day management of the security event dataset.
Security event		An activity, event, incident, or situation that directly or potentially affects the security posture of the Department.
Smart mobile device	Mobile device	Smart mobile devices are defined as devices which: • are a multi-function or general-purpose computing platform; • are lightweight and small in nature—generally able to be held/used in one hand; • incorporate a self-contained power source; and • have independent capability to transmit information wirelessly. Typical examples of mobile devices under this definition are smartphones (iPhones, Android phones etc.) and tablet computers (iPads, Android tablets etc.).
Synchronisation		The coordination of information between two or more devices. For example, a mobile device uploading messaging history to a cloud service which is accessible via other devices.
Trusted		Something which: • is subject to Australian laws and regulations; • can be considered reasonably secure from intrusion or misuse; • functions correctly and provides a reasonable level of reliability; and • is not associated with an entity owned, funded or influenced by a foreign government.

Released by Department of Home Affairs under the Freedom of Information Act 1982

OFFICIAL

Term	Acronym (if applicable)	Definition
Untrusted		Something which is unknown or not trusted.
Valid business reason		A valid business reason must exist in order for an individual to access any: departmental, sensitive, or classified information; ICT system; or depart from an approved procedure. The valid business reason must consider legislation, policy, risk, and the need-to-know principle, and serves as justification for the access or action. An individual has a 'valid business reason' where each of the following requirements are met: 1. It must be necessary for the performance of official duties for the Department or ABF and directly relevant to a current business deliverable; 2. Access and use of the information and/or systems must be lawful; 3. The need-to-know principle must be applied; 4. A conflict of interest must not exist; and 5. A valid business reason must be accepted and approved by an authorised person where outlined in this document.

OFFICIAL

Attachment B – Assurance and Control Matrix

1.1. Powers and Obligations

Implementation of this PI supports the requirements under section 16 of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) but does not require any powers, delegations or authorisations.

1.2. Controls and Assurance

Related Policy	Agency Security Plan 2020-2021 - Policy Statement (HR-5535) Security Event Reporting - Policy Statement (TI-5256)
Procedures / Supporting Materials	Acceptable use of Departmental ICT Systems and Information - Procedural Instruction (HR-3320) ICT Event Logging and Auditing - Procedural Instruction (TI-6481) Media and ICT equipment: sanitisation, re-classification and disposal - Supporting Material (TI-1628) Use of Social Media and Other Online Services - Procedural Instruction (SM-1560) Overseas Travel Security – Procedural Instruction (HR-6709) System Security Accreditation Framework ACSC - Travelling Overseas with Electronic Devices ACSC - Protect your internet connection
Training/Certification or Accreditation	Nil
Other required job role requirements	Nil
Other support mechanisms (e.g. who can provide further assistance in relation to any aspects of this instruction)	Cyber Risk Management section s. 22(1)(a)(ii)@homeaffairs.gov.au
Escalation arrangements	Escalation of concerns or issues can be sent to the Director CRM via s. 22(1)(a)(ii)@homeaffairs.gov.au marked to the attention of the Director.
Recordkeeping (e.g. system based facilities to record decisions)	TRIM RM8
Program or Framework (i.e. overarching Policy Framework or Business Program)	Australian Government Protective Security Policy Framework (PSPF) Australian Government Information Security Manual (ISM) Australian Signals Directorate (ASD) Strategies to Mitigate Cyber Security Incidents (Essential Eight)
Job Vocational Framework Role	This PI applies to all job roles within the Department.

Released by Department of Home Affairs under the Freedom of Information Act 1982

OFFICIAL

Attachment C – Consultation

1.1. Internal Consultation

The following internal stakeholders were consulted in the development of this PI:

- Classified Systems Delivery section
- Cyber Detection and Response
- Cyber Prevention
- Cyber Risk Management
- End User Platforms
- Finance Division
- ICT Division Support
- Identity Management and Access Control
- Integrity and Professional Standards Branch
- IT Security Advisor
- Legal Group
- People & Culture Division
- Policy and Procedures Control Framework
- Procurement & Panel Management
- Records Management
- Security Coordination Centre
- Security Policy, Communications and Skilling
- Technology Architecture
- Telecom Assets team

1.2. External Consultation

The following external stakeholders were consulted in the development of this PI:

- N/A

Released by Department of Home Affairs
under the Freedom of Information Act 1982

STAYING SAFE

NOVEL CORONAVIRUS (COVID-19)

For Official Use Only

Signal app use in Home Affairs

What's happening?

The Department has enabled access to the Signal application from 7 April 2020 as an approved encrypted messaging platform on corporate iOS devices, replacing the use of the WhatsApp messaging platform.

What is Signal?

Signal is a cross-platform messaging service that uses standard mobile service numbers as identifiers and uses robust end-to-end encryption. Signal can be used for up to PROTECTED voice, messaging and video conferencing when used on a Department device and with no external parties in attendance.

NOTE: In line with the department's [Records Management Policy](#) official decisions made on this platform must be documented and saved to TRIM.

Benefits of using Signal

- Signal uses standard mobile service numbers as identifiers and uses end-to-end encryption for all communications.
- Signal supports secure one-to-one and group messages, which can include files, voice notes, images and videos.
- Signal also support one-to-one secure video and voice calls.
- Signal is designed to never collect or store any sensitive information. Signal messages and calls cannot be accessed by anyone other than the intended recipients and all sensitive information is only stored on the sender and recipient devices.
- Signal messages can be sent with an expiry time after which messages are deleted from the sender recipient devices.
- Encryption keys are only stored on the sender and recipient devices.
- Each Signal conversation has a unique safety number that allows you to verify the security of your messages and calls with specific contacts.

Installing Signal on your iOS device

Signal can be downloaded and installed from the Apple App Store by following these steps:

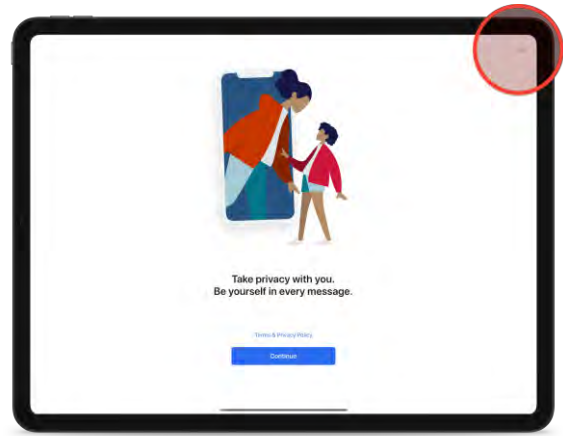
iPhone

1. Check that your iOS device is running the most recent iOS version and [update iOS](#) if required.
2. [Install and open Signal](#).
3. Follow the on-screen instructions to complete the registration process.

For Official Use Only

iPad

4. Check that your iOS device is running the most recent iOS version and [update iOS](#) if required.
5. [Install and open Signal](#).
6. Follow the on-screen instructions to
 - a. [link the iPad](#) to your phone or
 - b. Select the unlink icon  in the top right to register this iPad as a separate device and number.



Already using an iPad? [Update to the latest version](#) or [follow these troubleshooting steps for linking](#).

Initial configuration advice

Notification Privacy

Even when your iOS device is locked with a password, anyone who picks it up can still read the message and the sender's name from your lock screen. To avoid this follow these steps in the Signal app:

- Click Settings > Notifications > Show. To receive notifications with no information about the sender or the content of your messages, turn on "No Name or Content."

Screen Security

The Signal app also gives you options to lock your screen and prevent a preview from being shown unless you are in the app when a message is received:

- Click Settings > Privacy > turn on Screen Lock and set the Timeout to 15 minutes
- Click Settings > Privacy > turn on Enable Screen Security

Additional security advice

Disappearing messages

While Signal lets you delete individual messages, these messages will only be deleted on your device and are still accessible by anyone else in your conversation thread. You can use Signal's "disappearing messages" feature that allows you to remove messages from a conversation automatically after a period of time.

- Tap on your colleague's name at the top of the screen to open the settings menu for this conversation. Tap Disappearing Messages.

Safety Numbers

Signal allows you to verify that your session is encrypted and cannot be intercepted by a third party. Each Signal conversation has an automatically generated and unique safety number that allows you to verify the security of your messages and calls with specific contacts.

Verification of safety numbers is a good security practice for sensitive communication. Once a safety number has been marked as verified, any change must be manually approved before sending a new message.

How do you view a safety number?

Open a conversation thread with a contact and look for their safety number. This number verifies a secure and encrypted connection between your device and your contact's device.

- Tap your colleague's name (at the top of the screen) > View Safety Number

Signal advises you whenever a safety number has changed. This allows users to check the privacy of their communication with a contact and helps protect against any attempted communications interception.

The most common scenarios where a safety number advisory is displayed are when a contact switches to a new device or re-installs Signal. However, if a safety number changes frequently or unexpectedly it may be a sign that something is wrong.

Registration Lock

Whether it's your regular device number or a secondary number, you'll need to maintain access to this number. Why? If you lose access to the number and someone else re-registers it, now they own the Signal number.

You can lock in the registration for your Signal number, using Registration Lock:

- Open the Signal app > Tap in the icon in the top left corner (usually your initials) > Tap Privacy > Scroll down and tap Registration Lock > Enter a PIN number

What else must I do?

- Signal for business use is not to be installed on your departmental PC or laptop or on your personal mobile device.
- Signal software is to remain up to date.
- Screen Lock is to be enabled and Timeout set to 15 minutes.
- Enable Screen Security is to be turned on, this must include blocking screenshots from within Signal.
- Limit the Notifications Content to display Name Only.
- Add Signal PIN to the Registration Lock.
- All communication on Signal iOS is private and end-to-end encrypted.
- Chat backup is not to be enabled
- Signal-to-Signal messages are secure and free to send and receive using any internet connection enabled on your phone, including WiFi and mobile data.
- Signal can also serve as your unified messenger for insecure SMS/MMS messages in addition to Signal messages. Insecure SMS/MMS messages are sent through your mobile provider.
- Having issues installing on an iPhone? Follow these [troubleshooting steps](#).

More information

Contact IT Support on s. 22(1)(a)(ii) or log a [Service Request](#)

Security Coordination Centre: s. 22(1)(a)(ii)@homeaffairs.gov.au

Visit the [Signal homepage](#)