Australian Government
Department of the Prime Minister and Cabinet

PM&C Cyber Security Policy

Version 3.1.3 July 2024

s 47E

Contents

List of Tables

1 Synopsis

DOCUMENT DESCRIPTION

This document details the cyber security and ICT requirements that must be adhered to when using PM&C information technology and communication systems.

2 Contact Details

2.1 Document Creation

Author	Title	Telephone	Email
s 22(1)(a)(ii)	s 47E(d)	s 22(1)(a)(ii)	s 22(1)(a)(ii) @PM&C.gov.au

2.2 Amendment, Review and Approval

Version	Name	Description	Approval	Date
0.14	s 22(1)(a)(ii)	Updated. Incorporation of other ICT networks	CIO	28 June 2010
1.0		Release	CIO	5 August 2010
2.0		Document updated. Incorporated CIO comments.	CIO	20 June 2013
2.1		Password changes added	CIO	2 Dec 2013
2.2		Document updated incorporating PM&C Unclassified network and ISM Updates	s 22(1)(a)(ii)	26 May 2014
2.3		Minor updates		26 Nov 2014

Version	Name	Description	Approval	Date
2.4	s 22(1)(a)(ii)	Departmental template applied	s 22(1)(a)(ii)	21 January 2015
2.7		Minor updates		5 February 2018
2.8		Clarity on remote access for WyW and personal data breach		2 March 2018
2.8.1		Minor updates and change to classifications		18 Feb 2019
2.8.2		Review, minor updates and transfer to new corporate template		23 Oct 2019
2.8.3		Minor updates and clarifications		30 Jul 2020
2.9		Moderate update to terms, requirements and shared service content		14 Jul 2021
2.9.1		Minor updates to links and clarification on policy		11 Aug 2021
3.0		Full review and update. Name change to Cyber Security Policy.		19 Oct 2022
3.1		Minor amendments to offboarding policy		17 Apr 2023
3.1.1		Minor updates and clarification		21 July 2023
3.1.2		Minor updates to reflect ISM changes.		9 Aug 2023

Version	Name	Description	Approval	Date
		Template change. Clarification on account closure after termination.		
3.1.2	s 22(1)(a)(ii)	Formatted to meet document accessibility requirements	s 22(1)(a)(ii)	5 Sep 2023
3.1.3		Offboarding processes reviewed and updated.		25 July 2024

3 Introduction

3.1 Purpose

This document supersedes any previous Information and Communication Technology (ICT) Security Policy, as well as PM&C Chief Executive Instructions (CEI) 6.2 Information Technology Security and CEI 6.3 IT and Internet Usage Policy.

This document is known as the PM&C Cyber Security Policy (PM&C CSP). Its purpose is to document cyber security policy statements applicable to all:

- PM&C APS employees and contractors;
- APS employees and contractors that use PM&C systems under ICT shared service arrangements;
- External persons and organisations which have been given authorised access to PM&C ICT and information assets; and
- Home-based and remote locations where access to s 47E(d) has been authorised.

This document deals primarily with the PM&C PROTECTED network (s 47E(d) s 47E(d) network (s 47E(d) and s 47E(d) OFFICIAL network (s 47E(d) with reference to other PM&C environments and systems where appropriate.

3.2 Authority

This document has been reviewed and ratified by the PM&C Chief Security Officer (CSO) and Chief Information Officer (CIO). Maintaining this document is the responsibility of the PM&C ITSA.

3.3 Multiple Agency Support

PM&C provides ICT services to a range of Australian government agencies and stakeholders. This policy covers all of these systems. Every effort has been made to include other agency documentation and policy into this document, however in some cases, linked or referenced documents will focus on a PM&C version of a corporate document.

Equivalent versions of documentation for other agencies are typically available through the agency intranet, or can be sourced directly by contacting an agency corporate business area.

3.4 Scope

The policy expressed in this document covers all hardware, software and personnel for the following PM&C systems:

- PM&C PROTECTED Network (s 47E(d))
- NIAA OFFICIAL Network (s 47E(d))
- Cabinet Network (s 47E(d)

This policy outlines the following key areas:

- Security requirements for users of PM&C systems
- Security objectives
- Physical security for ICT assets
- Logical security for ICT systems
- Operational security, including:
  - Archiving and backup; and
  - Operations and support staff.

In addition, this policy should be used in conjunction with any agency or system security policy attributed to networks used by PM&C personnel, but monitored and serviced by outside agencies. These other networks may include:

s 47E(d)

Each of the above external networks used within PM&C are subject to separate System Security Plans that documents additional and specific security requirements for each network. In an instance where an SSP is lacking or does not cover a particular security requirement for these networks, all systems listed above must defer and comply with the requirements in this document. Therefore, whilst these systems fall under the general principles of this policy, effectively their additional requirements are out of scope of this policy document.

3.5 Objectives

The objective of this policy is to establish methodologies and practices to protect PM&C from any adverse impact on its operations or reputation resulting from failures of confidentiality, availability and/or integrity. It is intended to describe policy applicable to the use of PM&C ICT systems for the protection and control of classified information. It is presented in clear language to ensure PM&C users understand their obligations for the protection of official information.

3.6 Minimum Standards

Policies and standards are essential to the conduct of PM&C's business. The policies and standards applicable to the Australian Government are imposed as a result of the legislation under which the Government operates. Refer to the Protective Security Plan for details of applicable legislation.

The following legislation provides controls which must be addressed in the conduct of PM&C's business:

- *Crimes Act 1914;*
- *Public Service Act 1999;*
- *Privacy Act 1988;*
- *Freedom of Information Act 1982;*
- *Electronic Transactions Act 1999;*
- *Evidence Act 1995;*
- *Copyright Amendment Act 1984;*
- *Occupational Health and Safety (Commonwealth Employment) Act 1991*; and
- *Archives Act 1983*.

To provide guidance in the application of the legislative requirements the Australian Government has produced the following policy documents to assist agencies in addressing their responsibilities for the protection of official resources:

- The Protective Security Policy Framework (PSPF); and
- The Australian Government Information Security Manual (ISM).

In addition, elements of this policy are drawn from the APS Values and Code of Conduct and PM&C's Data Breach Response Plan (DBR Plan).

Employees and contractors must adhere to the standards in this policy in order to satisfy their employment responsibilities.

A policy control within this document with a 'must' or 'must not' requirement indicates that use, or non-use, of the control is mandatory. Special dispensation must be sought from the Chief Security Officer (CSO) to deviate from a policy control outlined in this document that includes the term 'must'.

3.7 Accreditation and Authorisation

PM&C networks undergo a series of audits against the ISM to establish their baseline for compliance against the minimum security controls specified for Australian Government computer networks. These audits provide the CSO with assurance that risks to PM&C ICT systems and information stored on these systems are addressed with adequate mitigations.

As of the October 2019 revision of the ISM, there is no longer any 'accreditation' of systems. This term has been superseded by the authorisation process for ICT systems and networks.

The PM&C CSO, acting as the Chief Information Security Officer (CISO) as defined in the ISM, is considered the overarching Authorising Officer for PM&C ICT systems.

The decision to accept risk resulting from non-compliance with an ISM control is the decision of an appropriate authority:

- Non-compliance that offers a Low level of risk can be granted by the ITSA or a CIO.
- Non-compliance that offers a Moderate level of risk can be granted by the CSO.
- Non-compliance for controls that, in the judgement of the above authorities present a significant or department wide risk can only be granted by the Agency Head or the PM&C Executive Board.

Non-compliance with a control at any level of authority will be risk assessed, documented by the ITSA or their nominated delegates and accepted by the appropriate authority. Non-compliance with controls in the ISM for which the authority is Australian Signals Directorate will be referred to that authority by the ITSA.

4 Roles and Responsibilities

The department has implemented a security management framework which details the roles and responsibilities for security across the department. Within the department these roles and responsibilities have been allocated as detailed in the following sections:

4.1 Agency Head

The Secretary provides support for the development, implementation and ongoing maintenance of information security processes and infrastructure. For day to day operations, the Secretary has delegated his authority to approve variations from requirements in this policy to the Chief Security Officer (CSO), who is supported by Security Advisers including Agency Security Adviser (ASA) and the Information Technology Security Adviser (ITSA).

4.2 Executive Board

One of the objectives of the Executive Board is to monitor the department's preparedness to counter security threats and to report and make recommendations on any significant security risk management issues requiring attention.

4.3 Chief Security Officer (CSO)

A CISO is responsible for providing and contributing to the implementation of strategic-level guidance for their organisation's cyber security program, vision and strategy and also ensuring compliance with cyber security policy, standards, regulations, business continuity, and legislation. They are likely to work with, or report to, a Chief Security Officer (CSO) who is responsible for the full breadth of security within their organisation. In PM&C, the CISO and CSO position are both held by the First Assistant Secretary (FAS), Technology and Business Services (TABS) Division.

4.4 Agency Security Adviser (ASA)

The Agency Security Adviser (ASA) is responsible for the day-to-day management of the protective security function and ensures that physical and personnel security is implemented to appropriately protect the department. The ASA plays an integral role in the ongoing monitoring of agency security procedures and systems. The ASA is responsible for ensuring that agency employees and contractors are aware of their security responsibilities and obligations, and that they are security cleared to an appropriate level.

The ASA is the primary contact for issues relating to physical, personnel or information security. The ASA can be contacted at s 47E(d) @pmc.gov.au.

4.5 Information Technology Security Adviser (ITSA)

The Information Technology Security Adviser (ITSA) is responsible for information technology security management across the department. The ITSA is the lead IT Security Manager (ITSM) in the organisation.

The ITSA's responsibilities include:

- Provision of guidance and advice on the protection of ICT resources and other ICT security matters;
- Monitoring compliance with the implementation of required security documentation;
- Maintaining the currency and effectiveness of ICT security policies, practices and procedures within the department;
- Initiating, conducting and/or participating in reviews and audits of ICT security and documentation;
- Analysing the security impact of changes to the ICT environment; and
- Acting on reported ICT security incidents.
- Ensuring that all ICT security related tools and procedures comply with the relevant legislation, policies and standards.

For issues relating to ICT security, the ITSA can be contacted via s 47E(d) @pmc.gov.au, s 47E(d) @niaa.gov.au or s 47E(d) @apsc.gov.au, or by calling s 47E(d) .

4.6 Managers

Managers are responsible for ensuring that all staff they supervise are made aware of this policy. Managers are also users, and as such must also comply with the policies found within this document. Managers, including Senior Executives, do not have the ability to authorise the bypassing of policies found in this document for themselves or their staff.

4.7 System Administrators

System Administrators are authorised users with privileged access to systems, environments or services. Staff providing ICT system support will be provided a standard user access account for normal business and an administrator user access account for system administration activities. Privileged access to systems, applications and data repositories is limited to only what is required for users and services to undertake their duties. Administrative activity must be isolated to the administrative account. s 47E(d)

Administration accounts are not permitted to access the internet or have email addresses assigned to them. These functions must be conducted by the user's standard account only.

4.8 Information Owners

Within PM&C-managed systems, information ownership is controlled on a Divisional basis (further information may be found within an agencies Information Management Policy found on each respective intranet). Each Division maintains their information on a group drive divided into various sub-folders, or on an instance of the Electronic Document Record Management System (EDRMS) ShareHub. Authorisation to access official information on a group folder or ShareHub site is provided by an EL2 or higher permanent staff member from that business area.

Cross Division authorisations are required where an authorised user requires access to another Division's information. Once granted, authorisation will allow select user's access to both their own and an authorised Division group file storage areas.

Task Forces are treated as a separate entity with their own group drive, ShareHub and file storage folders.

Information on an agencies organisation structure can be found under the directory tab on each agencies intranet.

4.9 Users

Users include PM&C, APSC or NIAA employees, contractors and contractor employees, consultants and equivalent members of other agencies who are authorised to access PM&C information systems. PM&C, APSC and NIAA employees must agree to abiding by the system usage policies before being granted to the system and its resources. This can be achieved by personnel signing a copy of a system usage policy or a written acknowledgement. Unprivileged access to systems, applications and data repositories is limited to only what is required for users and services to undertake their duties. As PM&C provides ICT services to a number of external agencies this policy is designed cover cyber policy for those agencies as well.

Users must read this Cyber Security Policy upon commencement of their duties, and comply with the policy set out within. Links to this document should be given to each user as part of their orientation package to a PM&C ICT-supported agency, as well as a brief sheet outlining their security responsibilities working with a new agency.

All authorised users, including administrators, must use unique login identifiers to access system resources for the purposes of visibility and accountability. In the event that a shared, non-user specific account is required, the ITSA must approve the creation and use of this account.

5 Information Security Policy

5.1 Information and Document Security

Information security is about ensuring the confidentiality, integrity and availability of information and information systems. Effective information security is a critical part of the any Australian government agencies activities and should not be viewed as just a technical problem.

In short, information security is everybody's responsibility.

5.1.1 Official Information

Any information received or collected by, or on behalf of, the Government, through its agencies and contractors is official information. As a valuable official resource, official information:

- Must be handled with due care and in accordance with authorised procedures as contained in this document;
- Must be made available only to people who have a legitimate 'need-to-know' to fulfil their official duties or contractual responsibilities; and
- Must only be released in accordance with the policies, legislative requirements and directives of the Government and the courts.

While not all official information requires classification, some information is especially valuable because it is critical to the performance of government functions or because its compromise could harm the national interest, national security, the operation of government, the community or the individual to whom it relates.

For this reason, the Government expects agencies to identify such information and protect it from compromise, including loss, damage, corruption or disclosure. This includes protecting personal information on individuals, in accordance with the Information Privacy Principles (IPPs) contained in the Privacy Act.

The classification system allows agencies to share and exchange information with confidence by ensuring a common recognition of confidentiality requirements and consistent application of protective security measures. The classification system also protects the information of other countries with which the Australian Government exchanges information.

5.1.2 Use of Official Information

Official information may only be used for the purpose for which it was originally obtained.

5.1.3 Use of Official Information for Other Purposes

Approval to use official information for purposes other than for that for which they were obtained must be endorsed by both the business owner and the CSO or authorised delegate. Unless permission to do so has been expressly granted, official information must not to be used for development, training or any form of testing unless all identifying or sensitive data items have been removed or sanitised, or the risks have been reviewed and quantified by the Cyber Security team.

Data sanitisation must occur in its original environment before data is made available in any other environment. In all cases, appropriate steps must be taken to ensure that:

- Official information is disposed of or deleted when no longer required; and
- Access to the data is restricted to individuals with a need to access the data.

Need to Know

The availability of information should be limited to those who need to use or access the information to do their work. Dissemination of information should be no wider than is required for the efficient conduct of the business at hand. This principle is commonly referred to as the 'need-to-know' principle.

It is the personal responsibility of all those who use or access official information to apply the 'need-to-know' principle in their official duties.

5.1.4 Accessing Classified Information

In order for an individual to be granted access to classified information, documents or equipment, they must have:

- An appropriate security clearance, and
- A need-to-know for that information.

If a user moves sections or areas, they must inform the IT Service Desk of any folders or systems they previously had access to that are no longer required in their new role.

5.1.5 Classifying and Reclassifying

Official information must be assigned a protective marking at the time it is created to denote different degrees of confidentiality, thereby helping to ensure that it is handled appropriately and only accessed by authorised users for approved purposes. This applies to all information, regardless of whether it is stored electronically or on paper.

Materials received from another organisation must be handled in accordance with the requirements of the original owner. Where an email is unmarked or has an unknown protective marking and has

originated from an Australian or overseas government agency, users should contact the originator to determine how it is to be handled.

Documents used by Cabinet to formulate policy and make decisions require special protective measures. These measures are detailed in the Cabinet Handbook. All documents prepared for consideration by Cabinet, including those in preparation, are to be marked at minimum PROTECTED Cabinet, regardless of any other security consideration. This is because Cabinet documents, unlike other official information, belong to the governments that create them. Cabinet documents can also require an additional, higher protective marking, depending on level of information contained within the document.

Supporting guidelines of the Protective Security Policy Framework (PSPF) provides guidance on the special requirements of dealing with security classified and sensitive information.

- Australian Government security classification system
- Protectively marking and handling sensitive and security classified information – see the relevant section of the PM&C Security Framework

5.1.6 The importance of classification

Protective markings applied to information show recipients or other users the measures that need to be applied to ensure the information is afforded the appropriate level of protection.

Protective markings also trigger automated and transparent security controls and checks when sent or stored, so choosing a correct classification is essential at all times.

5.1.7 Classification Levels

5.1.7.1 s 47E(d)

s 47E(d) is authorised to store and handle information with the following classifications and caveats/markings:

- UNOFFICIAL
- OFFICIAL
- OFFICIAL Sensitive
- PROTECTED
- PROTECTED Cabinet

It is not suited to hold material at these levels:

- SECRET
- TOP SECRET

5.1.7.2 s 47E(d)

s 47E(d) is authorised to store and handle information limited to OFFICIAL / OFFICIAL: Sensitive only.

5.1.7.3 s 47E(d)

[redacted] is designed to process and store information up to and including national SECRET s 47E(d) material. s 47E(d) is the only Australian Government network that is certified to hold official Cabinet documents up to the classification of SECRET. These documents will be marked as such for easy identification.

5.1.7.4 Other networks

Users should refer to individual network System Security Plans for details on the maximum classification levels and usable caveats of other networks used within PM&C or shared service agencies.

Any security classified or sensitive information over and above the classification levels listed above must not be created, stored on or transmitted via a network not certified for information of that level.

Further information regarding classification levels and the decision process for selecting classifications can be found on the Intranet: Information Security Policy and Guidelines.

5.1.8 Responsibility for Classifying

The originator must assess the consequences of damage from unauthorised disclosure or misuse of information and security classify accordingly.

All users must consider the contents of documents produced and apply the procedures described in the PM&C Protective Security Plan for the classification of information.

5.1.9 Caveats

Security caveats are a security marking applied to flag the need for additional, specific protection measures to be applied to the protection of that information. More information may be found in the Protective Security Framework - Policy 8.

PM&C users are most likely to encounter the following caveats:

- s 47E(d)
- s 47E(d);
- s 47E(d); and
- s 47E(d).

s 47E(d) and s 47E(d) are examples of an 'Eyes Only' marking and must only be shared with Australians holding the appropriate security clearance. Further information on the use of caveats can be obtained from the Security team (phone s 47E(d)). s 47E(d) and s 47E(d) caveats are not to be stored on s 47E(d)

5.1.10 When is it Possible to Reclassify Information?

Only the original information creator can determine whether their information is suitable for reclassification. It may be possible to modify information to remove or reduce the classification of certain information, but users should contact the original information creator before doing so.

5.2 Creating and Storing Documents

The policy applicable to the creation and organisation of official information is contained in the Information Management Policy on the Intranet. All corporate information including electronic data and documents should be created in file formats compatible with the existing approved suite of software products to ensure that it remains accessible over time and can be migrated or upgraded as required.

As with the arrangement of paper files, the proper organisation and naming of electronic files is essential to ensuring the availability, integrity and confidentiality of information. A properly managed file directory structure with appropriate security controls will enables business areas to:

- Quickly locate information;
- Protect the integrity of information by permitting access to only those users who have the authority to modify the information; and
- Protect the confidentiality of information by permitting access to only those users that have a need-to-know.

It is the responsibility of individual business areas to determine their teams file naming and folder structure. Users must conform to their business area's file naming and folder organisational structure.

5.2.1 Electronic Storage of Classified Information

Users must not store or transmit information that is classified higher than the level of accreditation of the system that is being used.

> **Common Question**
>
> **Q**: How much personal data can I store in my s 47E(d)?
>
> **A**: Approximately 100 megabytes

Users must ensure that official information is stored on a network drive (usually designated s 47E(d)) or in ShareHub. The use of ShareHub is preferred and encouraged as it meets legislative requirements for archiving. This ensures that agency processes can be applied to all official information, such as backups and Freedom of Information (FOI) requests.

Information stored on the local hard disks of computers (s 47E(d)) is not included in system back-ups and will be lost if the disk is corrupted or damaged. This includes a user's Desktop – in the event a PM&C provided device is lost, stolen or damaged, desktop files are typically not recoverable. The local

s 47E(d) must not be used to permanently store official data, but can be used to save files for temporary offline work.

PM&C ICT Service Delivery and Cyber Security teams are not responsible for the loss of any information stored on a local hard drive via upgrades, policy changes, hardware failure, security wipes or any other form of incident management.

Users must use the respective s 47E(d) or ShareHub site for their Division or work unit for the storage of official information. The s 47E(d) and ShareHub are not to be used for the storage of personal files such as music or photographs. Any personal items found on the s 47E(d) may be deleted without warning.

A s 47E(d) is typically provided on PM&C systems for the storage of a small amount of personal and sundry information (approx. 100Mb); it is not for the storage of official information and users may be breached if official information is founds stored incorrectly in this space.

5.2.2 Naming Electronic Files

The file name for an electronic document must be logical and meaningful so that the contents and context remain clear over time. File names must be based on logical naming conventions and be applied consistently so that they remain meaningful to individuals, workgroups and the agency over time.

Guidelines for selecting file names are also provided in ShareHub on s 47E(d) and s 47E(d).

5.2.3 Clear Desk Policy

Staff must ensure that sensitive material they are working on at their desks is locked away when they are out of sight of their desks. This means storing documents away in an appropriate storage container. Each agencies security framework, available on respective Intranets, outlines the appropriate container for storing different classifications of information at various sites around Australia.

The clear desk policy also extends to computer screens. Users must lock PM&C system computer screens when leaving their area. Screens can be locked quickly via the 'Windows Key + L' shortcut.

5.3 Electronic Sharing of Information

Anyone asked to share or transmit classified information via any form of communication facility must abide by the need-to-know principle. Users must ensure that the person or agency they are sharing the information with has a need-to-know for the information and the appropriate clearance level to access the information.

It can be reasonably expected that all users with an email account on a network have undertaken a security clearance process and have a clearance level suitable for use on that particular network.

5.3.1 Social Messaging and Personal Email

The use of consumer messaging products like Skype, WhatsApp, Wickr, Slack, Facebook Messenger or any other messaging tool must not be used for the distribution of official information. Similarly, there are restrictions on what video and voice conferencing platforms are suited for the distribution of official information. More information on the use of these platforms is available on the Cyber Security Intranet page.

Work (official) information must not be emailed to an employee's personal email accounts, including Gmail, Outlook.com or Hotmail. Access to webmail sites from PM&C official networks is blocked based on ISM requirements, including access to educational or contractor accounts. These types of webmail accounts should be accessed from a mobile or personal device instead.

If official information is accidentally delivered or received via these platforms, it is the user's responsibility to transfer this material to PM&C's record management tool in a searchable format. Using these services for the transfer or storage of official information may result in a formal breach notice.

5.3.2 Online Document Storage Systems

Online storage systems like OneDrive, Box, Dropbox or Google Drive are not permitted to be used for the transfer or storage of official information without explicit approval by the Cyber Security team.

In some cases when dealing with external parties, staff may be required to access files stored using these services. In these instances, a user should contact the ICT Service Desk to request access to the online storage facility. In most cases the file will be downloaded by the Service Desk on behalf of the user, and then placed in a nominated folder.

Requests for access to these types of services are assessed by the ITSA. It is important to include a detailed business case when requesting access to these services, as requests will be declined if insufficient justification is provided.

5.3.3 Security Implications of Incorrect Storage or Transmission of Official Information

Services which have not been tested or certified for use with Australian government information may contain security vulnerabilities. In a lot of cases, the End User Licence Agreement (EULA) of these products states that information shared using their systems can be shared with third parties, usually advertisers.

Staff found to be using these services for the transmission of official and/or classified information may be issued with a formal breach. For official purposes staff should only use authorised instant messaging products (Teams) and work issued email accounts (Outlook).

The availability of official information should be limited to those who need to use or access the information to do their work.

5.4 Transfer of Data between Systems

The transfer of data between two systems operating under different security policies presents a high level of risk to departmental systems. A user copying data to or from a PM&C-provided network must ensure that they take the precautions required by this policy.

Users must not copy executable files or program directories to any location between networks and may contravene copyright legislation in doing so. Contact the ITSA or IT Service Desk for further guidance on copying or distributing executable files or program directories.

Users unfamiliar with anti-virus scanning or data export procedures must consult the IT Service Desk before transferring data between networks.

Transfers using USB Media

When removable media is inserted into a classified system it is automatically classified at the level of the system. This means it must not be plugged back into a lower classified system, as per this policy.

s 47E(d)

Contact the Cyber Security team for more information.

5.4.1 Importing Data from a Lower Classified System

s 47E(d)

5.4.2 Importing Data from a Higher Classified System

Each file being transferred must be thoroughly reviewed by the transferrer to ensure that it does not contain information classified higher than the receiving network is rated or caveated information for which the network is not approved.

s 47E(d)

Note that removable media must be stored in a manner suitable for material of the highest classified network that media has ever been exposed to. For example, if media has been used to transfer between a PROTECTED and SECRET system, the media must be stored and handled as a SECRET item, even if no SECRET material was ever transferred using that media.

5.4.3 Exporting data to a Lower Classified System

Each file being transferred from a network to a lower classified network must be reviewed to ensure that it does not contain information classified higher than the system rating of the target system. The entire contents of the storage device must be inspected by the transferring user to ensure it has not been contaminated by any item classified higher than the protective marking label attached to the device.

Each file being transferred from a network must be reviewed by the transferring user to ensure that it does not contain caveated information unsuitable for the intended network.

s 47E(d)

The removable media used in this case must be labelled not higher than the system rating of the target system. If in doubt at any stage consult the Cyber Security team prior to undertaking the activity.

5.4.4 Exporting Data to a Higher Classified System

s 47E(d)

5.4.5 Importing Data – Machinery of Government Action

All data that is to be copied onto s 47E(d) must be scanned prior to the transfer to s 47E(d). Any malware is to be treated (i.e. removed). Quarantined items are not to be transferred to s 47E(d). This applies to single files, small groups of files, or bulk file transfers.

5.5 Data Retention and Archiving

The policy applicable to the retention and archiving of official information is contained in information management policies found on each agencies Intranet.

Email is a form of business correspondence and where it contains formal advice or directions, or documents significant decisions, it is also a corporate record and should be stored within ShareHub.

5.6 Disposal of Classified Media and Equipment

All classified media which has reached the end of its useful life must be destroyed in an approved manner.

Classified documents that are no longer required must be disposed of in a secure manner by using a classified waste bag/bin or appropriate shredder.

Users must deliver classified removable media, such as CDs, DVDs and USB storage drives, to the IT Service Desk for destruction by an approved method according to the classification of the data.

Users must contact the ITSA for assistance in sanitising, recycling or disposing of any computer equipment or electronic media that has contained security classified material. A Media Destruction and Sanitisation Guide is available upon request.

6 Computers and System Security Policy

ICT facilities, devices and services are provided by PM&C so that authorised users can conduct government business and perform the functions of their agency. These facilities include:

- All computer and computer-related facilities (fixed and mobile)
- Computer peripherals
- Mass storage devices
- Printers/multi-function devices
- Internet connectivity
- Email
- Smartphones
- Electronic tablets
- Audio/visual equipment

When using ICT facilities to conduct government business or perform the functions of their agency, users must be aware of the nature of information being handled and ensure that appropriate security is in place for accessing, creating, storing or transmitting data.

6.1 ICT Environment Overview

s 47E(d)

6.1.1 s 47E(d)

The main PM&C network (s 47E(d)) is rated to PROTECTED.

s 47E(d) is designed to provide basic computing services for the majority of PM&C and shared service users. This includes document creation, email, internet access, printing, document storage, backup, business applications and connections to other Australian government agencies and trusted partners.

s 47E(d) provides a Microsoft desktop environment with facilities for word-processing, database and spreadsheet creation and modification.

s 47E(d)

s 47E(d)

s 47E(d)

The classification of data and files that can be used with these devices is up to PROTECTED.

6.1.2 s 47E(d)

PM&C also has a separate network OFFICIAL Network (s 47E(d)) rated to OFFICIAL / OFFICIAL: Sensitive. Some UNOFFICIAL (personal) information can also be stored on s 47E(d). There is no PROTECTED or above information to be stored on s 47E(d) and users found doing so will be breached.

s 47E(d)

6.2 System Classifications

The table below provides guidance on the classification level of information that can be created and stored on each network. Classified information above the PROTECTED level must not be created or stored on s 47E(d)

Table 1: Classification of information permitted on various networks.

Network

Information classification	s 47E(d)						
Top Secret	✗	✗	✗	✗	✗	✗	✓
Secret	✗	✗	✓	✓	✓	✓	✓
Protected	✗	✓	✓	✓	✓	✓	✓
OFFICIAL OFFICIAL: Sensitive	✓	✓	✓	✓	✓	✓	✓

Information classification	s 47E(d)						
UNOFFICIAL	✓	✓	✓	✓	✓	✓	✓

6.3 Accessing Departmental Computers and Systems

SES officers or their delegates have responsibility for deciding the access rights for particular users for their respective business area.

The ITSA has responsibility for approving procedures used for the granting of access rights.

Each authorised user will be granted access to the information processing resources needed to perform that authorised user's duties and for which they have the required security clearance.

The IT Service Desk must maintain appropriate procedures and mechanisms to ensure that access profiles are kept accurate and current at all times, modified in a controlled manner and applied uniformly. This can only be done when users and managers provide timely advice and updates on staff movements however.

Access to PM&C-managed networks can be found on the Service Portal and must be approved by an authorised delegate for new users to gain system access. Further information for onboarding staff can be found on any agencies HR Services intranet page.

All users must acknowledge that they understand their responsibilities prior to being granted access to any departmental IT system via the onboarding process. Users will be reminded of this undertaking at the time of being issued their departmental security pass and login details.

6.4 Authorised User Responsibilities

6.4.1 Summary of User Responsibilities

All authorised users accessing departmental ICT services are responsible for:

- Understanding and complying with the security rules of PM&C's ICT facilities and systems
- Obtaining appropriate authorisation in order to access any ICT facility
- Content generated by their email account
- Authorising or allowing access to digital information they create on behalf of their agency
- Using available mechanisms and procedures to protect their own information and information under their control
- Ensuring anti-virus software is in place when using removable media or downloading files
- Ensuring corporate electronic records of continuing value are not destroyed prior to their capture into an agencies record-keeping system

- Storing official information within their area's ShareHub site in a manner such that it is easily found
- Managing their email environment by deleting all unsolicited 'junk' material from their account at the earliest opportunity
- Actively discouraging the use and circulation of 'junk' mail
- Notifying appropriate managers of any perceived misuse of ICT services or any suspected violation of this Policy
- Reporting any accidental access to inappropriate Internet sites to their supervisor
- Not altering or dismantling ICT equipment without proper authority from the Cyber Security team
- Not attempting to remove or circumvent security controls within ICT services and equipment
- Reporting any suspected or suspicious access by others to ICT facilities using shared credentials, or credentials not belonging to an individual to the Cyber Security team
- Securing their workstation from improper use by securely storing their password, not revealing their password to other people, locking their screens when away from their desk, storing laptops securely when not in use and shutting their workstation down at the end of the working day

Users must report all faults and security incidents in accordance with the processes described in this policy.

6.4.2 User Access Rights

The level of access granted to users will be limited to the level necessary to conduct their assigned work functions.

A users access rights must be set according to the role or function currently being performed, and according to the security clearances held by the user.

Users must inform the IT Service Desk as soon as possible if access to a system, folder or site is not required due to changes in their role.

6.4.3 User Identification

All authorised users of any network must have a login ID which uniquely identifies the individual. Login IDs are not classified, but should not be shared to external parties without consulting with the Cyber Security team.

Use of any network requiring generic or non-unique identifiers must be approved by the ITSA and an alternate method must be implemented to identify the user/s responsible for the use.

6.4.4 Multi-Factor Authentication

s 47E(d)

Authentication material such as passwords, tokens and material must not be kept unsecured or unencrypted with the system or device that the material grants access to.

6.4.5 Accountability

Users will be held accountable for all actions recorded against their network credentials, unless it can be shown without doubt that the user was not responsible for the actions in question in any way.

6.4.6 Variation of User Access Privileges

User authentication is required for access to various group drive folder or ShareHub sites, though this is typically transparent to the user.

All authorised user's access privileges must be modified or cancelled when they transfer to different duties within an agency or leave an agency entirely.

To vary a user's access privileges, the Service Portal should be used. Otherwise, directly contact the IT Service Desk via email or phone.

Some corporate applications, such as PM&C Finance One or Expense8, may have specific access requirements for specialised roles. The IT Service Desk should be contacted through the Service Portal for access to these systems.

6.4.7 Login Banners

On accessing PM&C networks, users are presented with a login banner reminding users of their responsibilities when connecting to PM&C assets. On agreeing to the login banner message and proceeding to enter any PM&C managed network, the user has acknowledged their acceptance of security policy outlined in this document.

The login banner text is included in full below:

> Security warning and official undertaking.
>
> The Department of the Prime Minister and Cabinet computer network is operated by the Commonwealth of Australia and access is restricted to authorised users only. It is an offence under the Crimes Act 1914, punishable by imprisonment, for any person to:
>
> • Obtain access to data stored on the network without authority
>
> • Insert, destroy or erase data on this network without authority
>
> • Interfere with, interrupt or obstruct the use of the network without authority
>
> • Impede or prevent access to or impair the usefulness or effectiveness of data in the network without authority
>
> Unauthorised use of this network by an employee in any of the ways specified above or the disclosure of or misuse of data held on the or within the network is also a breach of the Public Service Act 1999 and the APS Code of Conduct. Such actions will result in disciplinary action and may result in termination of employment and/or legal action under the Crimes Act 1914 or other legislation. For monitoring and audit purposes, your access to the network and systems is retained.

6.5 Unattended Electronic Equipment

Unattended electronic equipment provides an avenue for attackers to gain access and masquerade as an authorised system user. If a user leaves their computer, tablet or mobile device logged in and unlocked while it is unattended, they are considered responsible for any actions performed using their credentials.

When an agency issued electronic device is to be left unattended for extended periods, or to be used by another authorised user, the original authorised user must log off from that system first.

At the close of business each day, authorised users must ensure that they log out from any computer systems prior to finishing their work day.

Users should turn off their computer equipment at the end of each day as well as logging off, for both security and environmental reasons.

Security breaches or infringement notices may be issued when computers are detected as not being locked or logged off when the authorised user is absent.

6.5.1 Session Time-Out (Automatic Screen Lock)

Password-protected lock screen are configured to automatically activate after a period of not more than ten minutes inactivity at the terminal. Users must not circumvent this security control to prevent screens from locking after ten minutes of inactivity.

6.6 Passwords

s 47E(d)

Passwords must be used on all departmental systems. Users are encouraged to enable biometric authentication or any other form of multi-factor authentication (MFA) wherever available.

The following statements refer to the password use for any PM&C-managed systems, as well as any login credentials for online services used to process and stored official information:

- Passwords must not be divulged by the authorised user to any other person
- If a password has been compromised or suspected to be compromised, it must be changed immediately and the incident must be reported to the ITSA

s 47E(d)

- All password administration activities must be recorded in the system's log.

6.7 Personal Usage

6.7.1 Incidental Personal Use of Departmental Resources

PM&C and other shared service agencies using PM&C systems recognises that users may occasionally wish to take advantage of the convenience of email, internet and or other ICT facilities for occasional incidental personal use. In seeking to maintain a balance between the needs of a user's agency and a user's personal requirements, and with regard to the proper use of public funds, some incidental personal use of ICT facilities is permitted provided that:

- It does not constitute an unacceptable use as detailed *Section 7.4* Misuse of Computer and System resources
- Its impact on the costs and operations on PM&C and/or any relevant shared service agency is negligible.

Incidental personal use is defined as an activity that is infrequent and brief and applies to all PM&C managed networks and systems.

Users should bear in mind the following aspects if using systems for personal use, which may represent costs to an agency:

- The time spent in composing, reading, reviewing
- Time spent in surfing the Internet
- The use of printer resources: paper, toner and maintenance
- The use of other resources (server storage space, network traffic caused by sending emails with large attachments or downloading large objects such as pictures, videos, sound files)
- The interruption to the flow and pattern of work
- Occupational health issues related to excessive time spent at a computer screen and keyboard
- Impact on the work of colleagues, particularly how colleagues may feel about receiving unsolicited emails or seeing a staff member constantly accessing personal websites
- The risks of viruses being transferred to departmental computers
- The risks of leakage of departmental and personal information by users if visiting malicious internet sites

Whilst it is difficult to establish what determines a reasonable or acceptable level of incidental personal use, users should take note of these indicators:

- Intrusion into one's ability to fulfil required duties is unacceptable
- Personal use of IT facilities should preferably be confined to times which are outside of normal working hours, such as when on break or before the start of a work day
- Personal use that occurs more than a few times per day and/or for periods longer than a few minutes or in a way that attracts comment from colleagues is probably excessive
- Use outside of normal working hours for the pursuit of study or research etc. from which the Department or Commonwealth will benefit, is considered reasonable.

6.7.2 Personal Use of Internet Services

The occasional use of internet facilities for personal browsing is acceptable.

The *occasional* use of internet facilities for personal financial transactions, such as online shopping and Internet banking for convenience is permitted with an understanding that the user is solely responsible for the transaction. This includes responsibility for transaction content and technical support. The department will not be held liable for any financial loss incurred through using the Department's facilities for personal financial transactions, whether the loss is due to systems failure or any other reason.

Users need to ensure that this type of personal use does not disrupt the operation of the ICT services or interrupt on-going departmental work.

6.7.3 Personal Use of Work Email Accounts

Users are permitted to use their provided email address for occasional personal use.

Users should be aware there can be situations where the mere association of a statement or opinion with the name of an Australian government domain or agency may appear to give an endorsement or authority that is not intended or is inappropriate. Users must take care not to create such a situation.

Users should bear in mind that the inclusion of their email address on distribution lists of some organisations (e.g. clubs, political groups, wikis) may create an impression that is not consistent with the image of the Department, Agency or Commonwealth. Users should use a personal email address for such purposes.

Users should note that whilst the sharing of jokes can contribute to the maintenance of morale, some users may find these intrusive. Users are responsible for ensuring that they do not distribute unwelcome or inappropriate jokes to anyone.

s 47E(d)

6.7.4 Personal Use of Issued Mobile Devices

The use of PM&C issued mobile devices for occasional personal conversations, browsing and the installation of personal apps is permitted. PM&C reserves the right to block the installation and use of apps it has assessed as malicious or damaging. This list of unapproved apps is available from the Cyber Security team.

Care must be taken to ensure there is a distinction between personal and enterprise data on these devices. While technical controls are in place to prevent official information from being distributed via unofficial and personal apps, users are required to ensure they know the difference between the two types of data, and which apps are suitable for which data type.

As Australian government owned devices, users should be aware that any personal information stored on these mobile device may be subject to inspection or review at any time.

Care must also be taken to not overuse data download limits through personal use. Users found to overuse data limits due to personal use of the system may have their access removed or curtailed.

6.7.5 Monitoring of Personal Use

Users should be aware that their use of IT facilities is monitored and logged for operational reasons to determine whether the networks are operating efficiently, to protect the security of the system and to isolate and resolve problems.

> The department actively monitors staff use of the Internet to identify unacceptable use and to determine compliance with this policy.

Email and internet usage is logged and routinely inspected. Records of transactions may be obtained and provided to internal and external parties in cases of concern, fraud, code of conduct, FOI or complaint.

With web browsing, s 47E(d) . s 47E(d) PM&C reserves the right to open and inspect the content of any secure HTTPS connection that traverses its systems, including secure links to personal websites or services.

s 47E(d)

A limited number of IT support officers have access to these records as part of their operational duties and the extent of this access will not exceed the minimum essential for performance of these duties. Normal routine analysis does not involve reading the content of electronic messages or files in order to comply with the need-to-know principle.

However, if due to routine analysis or a complaint an agency reasonably suspects that a user is misusing facilities or is disrupting system performance, further investigation and action s 47E(d) . Any such investigation will be conducted in accordance with the *Privacy Act 1988* and other relevant legislation.

Users should also be aware that all email, files and telephone records may be inspected by authorised IT support officers for the purpose of responding to external persons (for example, FOI requests) or to bodies such as the Australian Federal Police, Australian Parliament or Auditor General or the courts. The content of email and files may also be inspected to protect system security and the rights and property of an agency or for the purpose of advising agency Senior Executive staff or in response to internal investigations.

6.7.6 Complaints and Investigation

Instances of unacceptable use of PM&C-provided ICT facilities should always be reported in the first instance to the Cyber Security team. Where the unacceptable use involves issues believed to fall within an agencies harassment guidelines a user should bring the matter to the attention of the a Workplace Harassment Contact Officer or People/HR Branch.

Complaints are investigated in accordance with an agencies procedures for determining breaches of the Code of Conduct or, where necessary, referred to the Australian Federal Police. Where a compliant involves harassment, complaints will be handled in accordance with an agencies Appropriate Workplace Behaviour Policy.

6.8 Suspension of Access for Users on Extended Leave

6.8.1 Extended Leave

Users departing on extended leave for more than 45 days will have their access PM&C-managed computers and system resources temporarily suspended for the duration of the leave.

Users may apply to retain access to systems during extended leave by provided a detailed business justification to the ITSA.

s 47E(d)

6.9 Termination of Employment

6.9.1 Users Leaving PM&C

Users departing their agency permanently will have their access to PM&C-managed computers and system resources deactivated at the time of departure. Access to accounts and systems should be disabled on the day of departure wherever possible.

If account access past the date of departure is required, or the offboarding process cannot be competed in a timely fashion resulting in accounts remaining open after a user has left the organisation, the Cyber Security team or the IT Service Desk must be contacted.

Access to any account past the date of departure for any reason may be reviewed or investigated by the Cyber Security team to ensure no malicious activities occurred. If access to an account is required after a fixed termination date, written approval must be sought from the Cyber Security team prior to any login or activity.

The process is initiated by a user completing an Offboarding form on Service Portal. Users and their managers must ensure that proper process is followed when staff leave the organisation or a contract has finished in order to ensure:

- Payment systems do not continue to disburse salaries to staff that have left
- Accounts are not left open and unused on the systems
- Email traffic is properly bounced to inform that a user has left an organisation
- Software audits do not falsely report extra licence requirements.
- User's assets and equipment must be returned to the department.

A complete instructional guide for offboarding can be found on each agencies specific intranet – Search for the term 'Offboarding' on an agency intranet for more information and frequently asked questions.

A user's s 47E(d) (personal files) and email accounts are archived after their account has been deactivated for one month. Users must ensure that no departmental or official records will be archived or lost as part of this process prior to leaving their organisation.

Users wishing to retain their personal email or personal information when departing should contact the IT Service Desk at least two weeks prior to the date of departure to obtain a copy of that information. This copy will be reviewed by Cyber Security for departmental material before being released. The release of official information under these circumstances is managed on a per case basis, depending entirely on the reason for leaving and the need for the user to access official information in their new role.

Users wishing to take work related materials to another agency for a new role should contact the IT Service Desk. The ICT teams from PM&C and the receiving agency will get in contact and transfer information on the user's behalf.

6.9.2 Return of Assets

Users terminating employment with an agency must return all electronic assets to the IT Service Desk prior to their departure. Failure to return departmental assets may result in difficulties in final salary disbursement or the progression of offboarding tasks.

6.9.3 Transfer of Assets

Assets may only be transferred after transiting the IT Service Desk. This process ensures equipment is functioning and that assets are associated with the correct individual. Users must not transfer or leave departmental assets for their successor or acting staff without notifying the IT Service Desk of the transfer.

6.9.4 Removal of Access Rights

User credentials must be deactivated and system access explicitly removed on cessation of an individual's employment at their agency or when access is no longer required to perform their duties. Any exceptions to this rule must be authorised in writing by the CIO, the CSO or the Cyber Security team.

6.10 Access While Overseas

Users must consult the Security and/or Cyber Security teams if they intend travelling overseas with any agency-issued electronic devices. Completing a 'Reporting Overseas Travel' form on the Service Portal fulfils this requirement.

The Cyber Security team will advise of arrangements for the protection of IT equipment overseas, as well as proper storage and handling processes and procedures. Advice can be given for protection of personal devices to be taken overseas as well.

Further information on this topic may be found in the Overseas Travel - Cyber Security Requirements.

6.10.1 Private Travel

There must be a significant business justification for wanting to take a PM&C-issued device on personal overseas travel. Any request to do so should be sent via Service Portal at least 2 weeks prior to travel.

Note that taking a device 'just in case' on personal overseas travel is not considered a valid business requirement, regardless of position or agency. Users should ensure that good succession planning is in place in their business area to avoid any situation where a user on private travel needs to log in for work purposes.

6.10.2 Accompanying Spouse/Partner

When an agency staff member wishes to accompany their spouse/partner on an overseas posting and wishes to access a PM&C managed system while overseas, they must first forward the request through the Service Portal or directly to the Cyber Security team, giving all available details, including:

- Length of time staff member will be away from Australia
- Business justification for wanting to access agency resources while living overseas
- Indication of endorsement by appropriate authority (e.g. AS, FAS)
- Overseas residential location and indication if the residence is on a compound, part of Embassy/High Commission grounds, etc.
- Where ICT assets will be stored when overseas and not in use (e.g. 'B' class safe, on site at residence)
- Who may have potential access to the PM&C device/devices, including any foreign nationals that may have access to a home (cleaners, nannies, etc)

The request will be reviewed by security teams within PM&C and shared service agencies to come up with a formal risk assessment and recommendation. Each request will be assessed on an individual basis and will have specific mitigations and treatments provided to reduce risk.

6.11 Printing, Scanning and Photocopying

A multi-function device (MFD) is a combination printer, scanner and photocopier in a single device.

MFDs provide the majority of printing and scanning functions for all system users. A single large MFD is preferred to multiple smaller printers due to cost savings, centralised management and simplified maintenance. Most PM&C-managed MFDs make use of 'swipe-to-print' or 'Find-Me' printing system, requiring users to swipe their building access passes to print or scan any document. This is designed to limit paper wastage and documents being left on printers. Users must not use someone else's pass for any purpose, including scanning a document or recovering a print job.

MFDs also provide photocopying capabilities. Care must be taken to ensure that an MFD does not scan or photocopy a document over and above the classification of the network it is connected to. MFDs should all have labels on them, indicating what network they belong to.

6.11.1 Printing Classified Documents

Simple errors, such as mistakenly sending sensitive or classified documents to an incorrect printer, can compromise the security of classified information. Use extra care when printing any classified information.

When printing classified information users must ensure the document is properly labelled, sent to the correct printer and that all copies of printed material are picked up immediately.

Users must not circumvent MFD 'swipe-to-print' access or controls.

Classified printed material left on a printer will be treated as a security breach or infringement.

All documents printed are logged on all networks, and are directly attributable to individuals.

6.11.2 Photocopying Classified Documents

In some areas, MFDs are utilised for the photocopying of higher-level classified information. Users must consult with members of their team, their supervisor or the Cyber Security team to determine if the MFD in their area is able to be used to photocopy material classified material.

Photocopiers (MFDs) suitable for copying classified information must be marked as such.

6.11.3 Scanning Classified Documents

The MFDs connected to s 47E(d) are only permitted to scan information classified up to PROTECTED.

s 47E(d) MFDs are suitable for scanning documents up to OFFICIAL Sensitive under most circumstances. s 47E(d) staff with a requirement to scan PROTECTED documents in regional areas with s 47E(d) equipment only should contact the Cyber Security team for advice.

Scanned documents remain stored on MFDs for a period of 24 hours. After one day the image should be automatically and securely erased from the memory of the MFD. If a user notices a MFD that does not seem to be automatically deleting scanned documents after 24 hours, they should contact the IT Service Desk as soon as possible.

Most MFDs have a direct 'Scan-to-me' functionality, allowing staff to swipe their pass to have a scanned document sent directly to their email inbox. Users must not try to circumvent this security control, or modify the scanned document to directly send to an external email address.

6.12 Software

6.12.1 Software Installation

Users must not install software on department systems without seeking approval via the IT Service Desk. The installation of unknown or untested software may introduce vulnerabilities into PM&C environments, allowing outside attackers to access the network. Similarly, known software installed in an incorrect manner may not be installed with a necessary security profile, and may introduce vulnerabilities to an environment. Unknown software in an environment may cause conflicts with approved software that is already installed on a system or introduce an unnecessary drain on network resources. All software installed on PM&C-managed systems must be appropriately licensed.

s 47E(d)

6.12.2 Browser-Based Applications

Users must not install browser plug-ins or extensions without consulting with the IT Service Desk. Common browser plug-ins required for standard business tools are already installed on users'

workstations. Certain browser extensions, including ad blockers, are pre-approved for installation and can be installed by the user – s 47E(d)

If in doubt about a browser plug-in/extension, or if a business need requires a specialised browser plug-in, users must contact the Cyber Security team for further information. Certain extensions cannot be permitted due to the classified nature of material available on PM&C-managed networks.

6.12.3 Software Piracy

To ensure that agencies are able to fulfil their obligations under the Australian *Copyright Act 1984*, only software licensed to an agency is to be installed. All software purchases and installations are to be performed by the IT Service Desk. This applies to all software products.

6.13 Virus Protection

The introduction of a virus into onto PC, server or a computer network can cause significant disruption to an agencies work and may lead to loss, compromise or corruption of data. To minimise the threat of a virus attack, the following must be observed by all users:

- Before importing any data onto a departmental computer, the media must come from a trusted source;
- After downloading a file from the internet or saving an attachment from an email from an unknown source, the user should scan the file to ensure it does not contain malicious code (*Instructions on how to scan are found in the breakout box on the right*);
- All personal computers and servers must be scanned frequently (this is performed automatically at 12pm each day); and
- All instances of virus detection should be reported by users to the IT Service Desk immediately.

Virus Scanning

To virus scan a file, folder or entire drive, find the resource you would like to scan in Windows Explorer and simply right-click it. You should see the option to Scan with s 47E(d) or Scan with s 47E(d) Selecting this option will immediately open up the systems inbuilt anti-virus software (shown below).

s 47E(d)

6.14 Removable Storage Media

Removable media refers to traditional storage methods such as USB memory storage devices (also called memory sticks, thumb drives, USB keys, USB sticks, etc.) and CD-ROMs but also includes other forms of personal electronic devices that could distribute files such as tablets and mobile phones.

6.14.1 Authorised Removable Media

Only approved equipment may be connected to PM&C networks. Personal USB flash drives (often called thumb drives or memory sticks), memory cards, PDAs and mobile phones must not be connected to departmental systems, including for the charging of mobile phones.

If users need access to a specific item of equipment as part of their work, they must contact the IT Service Desk. Users wishing to obtain a departmental authorised USB flash drive will need to contact the service desk or log a request via the Service Portal to obtain an approved device.

s 47E(d)

Temporary USB Access

s 47E(d)

All data transferred via removable media is subject to scanning for malicious software and appropriate protective s 47E(d)

s 47E(d)

Users must continue to report the loss or theft of any removable media to the IT Service Desk.

Removable media classified higher than PROTECTED must not be connected to s 47E(d) unless sanitised and covered by a standardised and agreed upon data transfer process. Contact the ITSA for more information.

6.14.2 Copying to Removable Media

User must ensure that only the intended information is copied to removable media prior to its removal from the source system.

If the information is to be transferred to another system refer to *Section 5.4 Transfer of Data between Systems* for additional guidance.

6.14.3 Storage of Removable Media

All removable media must be stored in the same manner as a paper document of equivalent classification. Refer to the PM&C Security Plan for guidance on storage requirements.

Approved removable media devices must be stored in an accredited security container

In secure areas, use of removable media must be approved by the ITSA. Approval to use removable media in secure areas must include:

- Standard operating procedures on handling for the USB device
- Storage in an approved key-safe for accountability of the media (preferred)
- Use of a document transfer register for accountability of classified information

6.14.4 Labelling Removable Media

All removable media must be classified and labelled at the level of the most highly classified data contained on them. Smaller drives may require basic writing in permanent ink in lieu of a proper classification sticker.

Removable disk drives, USB flash drives, magnetic tapes, cartridges, and similar media must remain classified at the level of the most highly classified data ever written to them and must be labelled as such.

6.14.5 Disposal of Removable Media

All classified media, removable or otherwise, which has reached the end of its useful life must be sanitised or destroyed in an approved manner.

Refer to *Section 5.6 Disposal of Classified Media*.

6.15 Keyboards and Mice

Users found installing and using unapproved peripherals may be breached for not following security policy.

6.15.1 Keyboards

The use of wireless keyboards is not permitted without ITSA approval. Non-standard keyboards are permissible for WH&S reasons, but the brand and model must be approved by the Cyber Security team first. Prior to purchase of any new peripheral, a user should contact Cyber Security to discuss.

6.15.2 Non-Standard Mice

Some types of non-standard mouse or other pointing devices are permissible for WH&S reasons. Wireless mice that operated via Bluetooth 4.0 or higher are permissible if ordered through the IT Service Desk. Prior to purchase of any new peripheral, a user should contact the Cyber Security team to discuss.

6.16 Wearable Devices

Most standard wearable devices, including devices that assist disabled users like hearing aids, are connectable to agency-issued mobile devices.

Only certain wearable devices can be used within highly secure s 47E(d) . Their use depends on the type or style of device and the classification of the security zone that the wearer wishes to access. A list of approved devices for highly classified areas is available on the PM&C intranet as PM&C has access to the most secure areas. Users of other agencies should consult with the Cyber Security team to discuss access requirements for their secure spaces.

Consult the Cyber Security team if you wish your add your own device to be considered for inclusion on the list of wearable devices suited for highly secure areas.

6.17 Telephony and Video Conferencing

PM&C's primary telephony solution is via Microsoft Teams, in what is called a 'soft-phone' (software telephone) configuration. Because of this, traditional phone handsets on desks are being replaced in most offices with a variety of personal headsets, shared handsets or various other audio/visual systems that suit an individual user's requirements.

Agencies have the capability to investigate the origin and destination of telephone and video calls made from all departmental phone and video conferencing systems. Information recorded includes the origin of the call, called number, duration, and time/date. Departmental telephone and mobile phone accounts are routinely monitored to identify billing errors and patterns of excessive use, and to certify expenditure.

Users are advised to be aware of their surrounding when using telephones to ensure their conversations are not overheard or recorded by someone without a need-to-know.

6.17.1 Microsoft Teams

Microsoft Teams can be used to send and distribute OFFICIAL Sensitive information to any network or platform. Teams used on s 47E(d) can be used to distribute and transmit PROTECTED information provided it is only to other s 47E(d) users, or a connection to another PROTECTED agency.

Users must not discuss classified information when making standard or international calls to people outside of their agency on landlines or mobile phones. Contact the Cyber Security team for advice on

telephone or video conferencing services authorised to support classified conversations or carry security classified material.

Classified conversations require three separate assurances:

1. The clearance of all involved attendees
2. The technology used to make the call (Teams, Zoom etc.)
3. The security assurance of the device attendees are dialling in from (Australian government issued device, personal device, shared devices etc.)

Only when all three of these factors are confirmed to meet the requirements for a classified conversation can classified material be discussed and transmitted over a telephony or video conferencing service.

6.17.2 Mobile Phones

Mobile phones, both departmental and personal, are potentially vulnerable to interception, remote access and compromise. These devices must not be used to discuss or send classified or sensitive information over standard phone calls or SMS. This includes departmental smartphones which cannot be used for voice conversations above OFFICIAL Sensitive without using a secure app like Teams. It is also discouraged to use gifted or unauthorised peripherals with mobile devices.

Teams is provided on agency-issued mobile devices and can be used for the transmission of sensitive or classified material to the level of the network the devices are linked to. For s 47E(d) this is PROTECTED. Teams voice and video chats, as well as instant messaging, are encrypted and provide much more security compared to a standard phone call or SMS.

Signal is an app that was previously permitted to transmit and send some classified information, however this app has been superseded by Teams and should no longer be used in an official capacity unless approval has been sought. Contact the Cyber Security team for more information.

Mobile phones should be kept secure at all times as they can be easily lost or stolen, resulting in unauthorised access to the information stored on the device. Any departmental mobile device that is lost or stolen must be reported to the Cyber Security team as soon as possible. Users are instructed to submit a formal police statement in the event of a theft.

Personal mobile phones or multimedia devices must not be connected to departmental computer assets for syncing or charging. USB charging points are located within most agency-managed facilities as part of a standard desk power deployment.

No mobile devices, even PM&C-provided devices, are permitted to be taken to areas designated to hold and store s 47E(d) material without the express approval of the ITSA. Some s 47E(d) areas have different electronic device policies – users are instructed to read the posters and material available outside a specific area to determine what devices are permitted in which areas.

6.17.3 Hacked devices

Users that have taken their departmental or personal mobile phones overseas and are now experiencing issues with battery life, bad connections, changes to language, strange error messages or unknown applications installing themselves must contact the Cyber Security team as soon as possible. These are all signs a phone could have been hacked or compromised.

6.18 Internet Usage

The internet is an enormous information source, providing details and information on almost any subject. It is important to acknowledge that when researching via the internet much of the material available may be inaccurate or inappropriate and should be checked thoroughly for correct research and accountability if being used as an information source.

6.18.1 Appropriate Use of the Internet

PM&C allows its users 'fair use' of the internet for personal tasks on department resources. All websites visited by users are logged and filtered by PM&C systems, and accessing inappropriate or offensive websites may result in a code of conduct investigation.

Users are also reminded that any information they submit to a third-party website from department assets is potentially identifiable as originating from the Department of the Prime Minister and Cabinet and has the potential to cause embarrassment to PM&C or the Australian government if found to be inappropriate or sensitive in nature.

6.18.2 Social Networking Sites

Whilst not prohibited, users are discouraged from accessing social networking sites such as Facebook, LinkedIn, Twitter, YouTube and personal blogs from their agency-issued computer unless it forms part of their role.

Social networking sites provide a vehicle for launching a social engineering attack on unsuspecting participants. Any information which may identify an individual as a government employee has the potential to make them the target of an attack. User should be particularly careful of posting information such as personal telephone numbers, family details and addresses online.

Personal information stored on social networking sites should be considered at risk of compromise and agency users are cautioned regarding information which they make available about themselves.

Users should not reveal their association with their agency on social networking sites to the general public, unless it involves following or attaching their online profile to an official agency maintained social portal. Disclosure of their place of employment to a 'friends and family' group is permissible, but it is advised that users not disclose the division or branch they work in.

Special care must be taken to prevent official information from being published on social networking sites. Any official use of social networking sites to represent an agency must be conducted on an

account separate of any personal account. Official use must be sanctioned by the Cyber Security and Communications teams.

Further information on social networking is available in the PM&C Social Media Policy.

6.18.3 Instant Messaging

External instant messaging services like WhatsApp, iMessage, Facebook Messenger etc. must not be used to distribute official information, and provisions have been put in place to prevent the use of most major external instant messaging communication platforms.

Users must not use Teams voice services to discuss classified information (i.e. above OFFICIAL) with external entities, unless those agencies shave been confirmed as being 'federated' to the same level as the network being used to contact them. The IT Service Desk can provide more information on agencies that are federated with PM&C systems.

Teams can be used to discuss official information within an agency, however if any official decisions or recommendations were reached within a Teams 'chat session', they must be exported to ShareHub or formalised in a follow-up email between all parties containing exactly what was agree to and the points used to make that decision.

All use of Teams is subject to the PM&C ICT and Internet Usage Policy.

Teams instant messaging (IM) feature is currently provided as a means of communicating small pieces of information or conducting brief, informal conversations. It is not yet suited for official information or decision making. Users are reminded that IM conversations may be used in evidence reporting for bullying/harassment complaints and may also be exposed during FOI requests.

If official information does make it onto Teams in any format, it is the user's responsibility to extract that information and store it correctly in their agencies record management tool in a searchable format.

Users must not circumvent controls in place to use external instant messaging services.

Mobile messaging services like Facebook Messenger, iMessage, WhatsApp, Telegram or similar are not to be used for the distribution of official information. Users must extract any official decisions made via messaging services to be stored in ShareHub as a record.

More information on these services and how to choose the best service for your needs can be found on the Intranet Cyber Security section.

6.18.4 Downloading Files from the Internet

If a user downloads files from the internet, it is their responsibility to ensure that the download does not contravene the usage policy defined in this document.

Users must not download executable files and certain compressed files. Users must not download compressed (zip) files from unknown websites. File extensions are usually comprised of three letters that denote the type of file. Common file extensions not permitted for download are:

TABLE 2:NON-PERMITTED FILE EXTENSIONS

s 47E(d)

The above list is not exhaustive and only shows the more common types of non-permitted file types. If a user unsure of the appropriateness of a file they intend to download, they must seek advice from the IT Service Desk.

s 47E(d)

6.19 Emails

When sending email from your desktop or mobile email system, the intended recipient may be internal or external to a user's agency. Internal addresses function within PM&C's secure networks so there is minimal risk of the email being intercepted by an unauthorised individual. External addresses function outside of PM&C's secure network. Externally addressed emails are sent across the Internet, an open network, where there is a significant risk of the message being intercepted by unauthorised individuals.

Note that s 47E(d) does not have any connections to external internet networks, so all email exchange is considered secure. s 47E(d) users should note that certain agencies they are able to send emails to can only accept a limited range of file types, or only file types without any active content included.

Users must be conscious of whether they are sending an email to an internal or external party, as this will determine the type and classification of information able to be sent.

6.19.1 Email System Use

All email messages that are sent using an agencies email system can be considered official documents and should be handled with the normal courtesy, discretion and formality. All emails must be handled in the same manner as any other agency communication. This includes ensuring that the email message relating to the official business are classified, stored and managed in accordance with agency record management guidelines.

6.19.2 Sending Classified Information via Email

All email messages addressed to external recipients are transmitted via the Internet. Consequently, classified or caveated material must not be included in external email messages.

GOVLINK is a network of encrypted links between Australian Government federal agencies. GovLink allows secure transmission of information up to a PROTECTED level between agencies.

GovLink-connected agencies can be found at the GovLink User List page.

No action is required in most cases if an email has bounced due to the classification marking, but users should contact the Cyber Security team if they have any questions about the process.

OFFICIAL Sensitive information may be sent to recipients not connected to GovLink, provided there is a need to send that information to a particular email recipient or address. All care must be taken to ensure that only OFFICIAL or OFFICIAL Sensitive information is released, there is a need to send to a particular email address and that the information is only sent to intended recipients.

To establish which agencies participate in GovLink and at what level they are connected, consult the current list of GovLink Connected Agencies and Departments.

6.19.3 Right to Review

PM&C maintains the right to review any user initiated actions on its systems, including emails sent from agency systems or devices. Users should also be aware that all email records may be inspected by authorised IT support officers for the purpose of responding to internal requests (Fraud, HR investigations) or to external persons (for example, FOI requests, Australian Federal Police or court cases).

The content of email and files may be inspected to protect system security, information security, for advising agency Senior Executive officers or in response to internal investigations.

6.19.4 Forwarding Email

When manually forwarding email users must be aware of the contents of the email and any attachments to ensure that they do not send information to individuals without a need-to-know or the correct security clearance.

Users must not use automatic forwarding of email (via Outlook Rules) without consulting the Cyber Security team. This particularly includes automatic forwarding of email to external email accounts or external agencies. To do so without permission is considered a code of conduct breach.

6.19.5 Applying Protective Markings to Email

Classification of email is mandatory across the Australian Government.

All email sent from a PM&C account must be classified using a protective marking. Email that does not have a protective marking may be blocked at the email gateway. Email that does not have a protective marking or is misclassified may be sent to a network not suited for that level of information, which is considered a security breach.

Users must review the contents of the message, including attachments, and security-classify all email they create, to ensure the correct classification label is applied to emails sent. Note that emails sent via iOS devices do not automatically apply classification markers. Users are responsible for using the provided classification marker keyboard app to add a classification prior to sending an email from a mobile device. Further information on this app can be found on the Service Portal wiki.

If email protective markings are not being applied to emails due to a malfunction of the classification software, it is the user's responsibility to report this error to the IT Service Desk.

6.19.6 Attachments

Emails must inherit the classification of their attachments. For instance, a PROTECTED attachment connected to an email means that that email must also be marked PROTECTED.

6.19.7 Using Web-based Email Services

Users must not use departmental computers to access web based email services, such as Gmail, Hotmail or Yahoo. Users may inadvertently download a malicious file to the desktop from a web based email system, or it may allow a user to send classified information over an unsecure network.

If a user requires access to a public web based email service for the conduct of their duties, they must contact the Cyber Security team for authorisation to use this service. A business case to access web based email must be approved by the ITSA or CIO. Users are recommended to use their mobile phones or personal devices to access these services instead.

6.19.8 Accessing Another Employee's Email Account

Users may choose to provide access to certain functions of their mailbox to other staff. This is done by delegating permissions to the selected delegate. Contact the IT Service Desk for assistance.

If users do not set delegates to access their email, agencies may seek to gain access to the files or email messages of users where this is necessary for the purpose of retrieving official information. For example, a Branch may need to access the email of a user on leave who has not granted permission to an appropriate delegate to access and handle their email.

If someone wants to access information in another person's home drive or email account without the owner's prior written permission, they must request permission from that person's Branch Head (AS level). If approved, that Branch Head must formally submit or approve the request by email through the IT Service Desk or Service Portal to permit that information to be released to the person making the request.

The extent of access is restricted to no more than necessary to locate and retrieve the relevant information. Full access to another user's email inbox is not usually given to co-workers without the express permission of the inbox owner due to privacy concerns.

6.20 Use of Privately Owned Computers, Equipment or Software

Privately owned computers, equipment or software must not be used for processing official information unless connected via the s 47E(d).

Privately owned computers and devices must not be connected to departmental systems without prior permission from the Cyber Security team. This includes charging of personal electronics via USB ports on PM&C computer systems.

6.21 Use of Other Agency Owned Computers, Equipment or Software

The use of other government agency computer systems is governed by that agencies security policy. Users must adhere to that agencies security policy when using other agency computer systems even if

it diverts from PM&C policy. The Cyber Security team must be consulted where any confusion or doubt is present in the use of another agencies system.

6.22 Remote Access

6.22.1 Remote Access to Departmental Computing Resources

PM&C provides all agency users with facilities to remotely connect to their agency network to access email accounts, files, applications and other network services. s 47E(d)

Further information on the responsibility of users when working remotely can be found on agency intranet sites.

6.22.2 Employee Responsibilities

Users working remotely must use the same or a higher level of care and discretion as if working in their usual office environment. Working from a home environment raises a number of security issues in addition to those found in a traditional workplace – the most obvious is that family, housemates or friends could be close by. This increases the risk for people without a need-to-know or an appropriate security clearance to access or view official information or other official resources.

6.22.3 Telecommuting

Telecommuting is performed by an authorised user away from a traditional office environment. Telecommuting is a general term that refers to regularly working remotely, not just working from a home environment. Telecommuting may also refer to users working from shared office facilities not owned by their agency.

This working arrangement introduces a number of specific risks not encountered in the office environment. The physical security measures inherent in an agencies office facilities may not be available. Careful consideration must be taken regarding the physical environment and other people that may be in close proximity. It is very important that the individual take additional precautions to ensure that official information is provided the necessary level of protection as required by departmental policies.

When selecting a location to engage in agency work, the user must consider the possibility of an unauthorised individual being able to observe official information. Care must also be taken when discussing matters by telephone to ensure that conversations cannot be overheard.

6.22.4 Home-based Work

Home-based work (HBW or 'working from home') is where an authorised user operates from an approved installation in their home. Employees in a HBW arrangement should use ICT equipment provided by their agency and must comply with all aspects of this policy.

Organisation owned mobile devices and desktop (laptops) computers when being used as part of the working from home agreements, should not be used for personal purposes and should ensure separation of personal and work data.

Where provided, ICT equipment is strictly for employee use only. Users found to be sharing HBW ICT systems with family members may be formally breached.

Policies relating to PM&C users performing HBW may be found in the Flexible Work Policy and the Working Mobile at PM&C on the Intranet. Other agencies using PM&C systems have similar policies and requirements that can be sourced from the agencies HR area.

6.22.5 Laptops

When an authorised user is required to transport a portable laptop computer from an agency facility, there is risk that the computer may be stolen, lost or accessed by unauthorised persons. Accordingly, users must secure all laptop computers in an appropriate and reasonable manner when transporting them.

s 47E(d)

Portable and attractive electronic items should not be left unattended when away from the office. Leaving devices in a locked vehicle is not recommended, however if the authorised user needs to leave an agency device in a vehicle, it must be secured where it is not visible to onlookers. Users must use all reasonable precautions to protect agency-issued devices.

6.22.6 Hand-held Electronics

Mobile phones, tablets and portable storage devices create numerous opportunities for thieves due to their size and weight. The devices are highly attractive items based on the intrinsic financial value of such items and the value of data that they may hold. Handheld devices should not be left unattended whenever possible. Particular care must be taken to ensure that these items are not left in easily stolen scenarios, such as in hostel rooms, unlocked vehicles or unattended on desks in public spaces.

6.23 Smart Phones

This section refers to departmental issued iOS (Apple) mobile phones and iPads.

Agency-issued mobile devices linked to PM&C-managed networks integrate with existing agency environments for wireless and effective access to email, calendar, notes and other services.

Any user travelling overseas who wishes to take their agency-issued mobile phone with them must lodge a request via the Service Portal and provide an effective business justification for the request. All locations to be travelled to and transited through are to be provided in the request. The Cyber Security team will then review the request and either approve or reject the request. See *Section 6.10 Access While Overseas* for further information.

6.23.1 Approval

A user being issued with an agency connected mobile device must adhere to and acknowledge the requirements set out in this policy and any related procedures and undertake prerequisite training before being allowed to use the service.

6.23.2 Requesting a Mobile Device

Users wishing to obtain a mobile device must submit a request through the Service Portal. BYOD (bring your own device) is not permitted on PM&C-managed networks.

6.23.3 Processing of Classified Data

s 47E(d) devices may be used for the transmission and storage of all information available to the network it is linked with, within provided work related apps on the device only. All material outside of these work applications must only be used for personal information.

Agency issued mobile devices must not be used for the transmission and storage of s 47E(d) or s 47E(d) information. The only exception to this are a small fleet of modified s 47E(d) devices that do allow higher classified material to be uploaded via established processes.

Users must not circumvent security requirements by incorrectly classifying emails on mobile devices or by using external services to transmit official information.

Currently, mobile devices do not have the capability to automatically insert an email classification marking into emails. Users must ensure that emails sent from the device is correctly classified or are not being sent to outside agencies.

When sending an email from a mobile device, users should insert a [SEC=<CLASSIFICATION>] tag within the subject line, to show that they have consciously applied a label to the information. Agency-issued iOS devices have a special keyboard to allow one touch classification marking to emails. Step by step processes on how to enable this keyboard is available on the Service Portal wiki.

6.23.4 Voice Service

Mobile devices do not provide much basic security when making a standard phone call. Standard phone calls must be limited to OFFICIAL Sensitive material only. Users may use Teams to make secure phone and video calls to other agency-provided devices. Teams must not be used for discussions over PROTECTED.

Signal may be used in some rare cases as a voice service when talking to external agencies that are not federated. Contact the Cyber Security team for more information.

6.23.5 Connecting to Other Networks

Users must not connect mobile devices directly to any desktop device via a direct link cable, Bluetooth or other method, including agency-provided laptops. s 47E(d)

s 47E(d)

6.24 Use of Recording Devices

Users are reminded that the covert use of voice and photographic recording capabilities has the potential to contravene a number of Australian laws. This action would also be deemed a contravention of the Australian Public Service (APS) Code of Conduct.

Users must ensure that all parties in recorded meetings or conversations are aware that they are being recorded, and are given the choice to opt out of being recorded prior to any recording beginning.

6.24.1 Photographic Equipment

Photographic equipment must not be used within an agencies secure facilities without the approval of the Cyber Security or Security teams.

Photographs must not be taken of official information.

Photographs of social events within an agencies facilities must be reviewed for sensitive or inappropriate material before being distributed.

Personal photographic equipment must not be connected to agency assets without consultation with the Cyber Security Team.

6.25 Video Conference Facilities

Care must be taken when determining the classification level of a conversation can be held via video conferencing. Not all platforms are suited for the distribution of official or sensitive information, and users are reminded to confirm the clearance level of meeting participants prior to having any classified video conference.

Further information on video conferencing platforms can be found on individual agency intranets.

7 ICT Security Incident Reporting

The detection and reporting of cyber security incidents, breaches and violations is a major contributor to the maintenance of a system security. Users must report any observed or suspected security weaknesses, vulnerabilities or threats to the Cyber Security team as soon as possible.

7.1 Violations, Breaches and Incidents

7.1.1 What is an Incident?

Any activity or occurrence that compromises or has the potential to compromise official resources or information is a security incident.

Common security incidents have the following indicators:

- Poor system performance
- A PC failing to boot
- A suspected compromise of a system password
- Web sites not behaving as expected
- Detection of inappropriate content on the system
- Social engineering attempts
- Unexpected email containing an attachment
- Accidental equipment loss
- Theft or loss of ICT equipment
- Missing files or directories on a home or group drive
- Alerts from virus detection software.

7.1.2 What is a Breach?

The term security breach refers to an action perpetrated by an individual which could lead to the compromise of official resources. Breaches are categorised according to their severity as discussed below.

Further information regarding Security Incidents, Advice Notices and Breaches can be found on any agencies Security Intranet sections.

7.1.3 What is an Infringement?

The term security infringement refers to a minor accidental or unintentional failure to observe an agencies security procedures. Multiple infringements by an individual may result in a formal violation.

7.1.4 What is a Violation?

In this document the term violation is used to identify a deliberate breach, infringement, or transgression of this policy which has the potential to lead to a compromise of official resources.

7.2 External Incident Types

The following are typical techniques used by external attackers to gain access or information from Australian Government system users. All users must report any incidents of this nature to either the Cyber Security or Security teams immediately after occurrence or identification.

7.2.1 Social Engineering

Social engineering is a technique employed by hostile parties in an attempt to circumvent security protections implemented by an individual or organisation. The technique involves tricking an individual into divulging confidential information. This could be targeted at directly revealing classified information or such details as an individual's user name and password.

Users should be aware of the various methods of launching a social engineering attack, and if they feel they have been targeted the occurrence must be reported as an ICT security incident. Some of the most common approaches for social engineering are described below:

Pretexting

Pretexting is an act of creating and using an invented scenario (the Pretext) to persuade a targeted victim to release information or perform an action. This is typically done over the telephone to give a sense of urgency and immediacy. The deception most often involves some prior research or set up and uses fragments of information such as telephone numbers, date of birth, etc., to deliver the perception that the perpetrator is legitimately representing an organisation with which the victim has a relationship.

The most obvious method of pretexting is an attacker contacting the IT Service Desk to ask for a password reset on an account. By pretending to be the account holder and using basic details gleaned from online sources, an attacker can have a password reset and get full access to an official account.

Pretexting may utilise a more elaborate approach whereby the perpetrator telephones a number of individuals within an organisation and by asking what appears to be quite harmless questions, builds a profile on the intended target before launching the genuine attack. Pretexting is often used to target executives of various major corporations and senior government officials.

Phishing

Phishing is a criminal technique for fraudulently obtaining private information. Typically the phisher sends an email or SMS that appears to come from a legitimate source. The scenario may involve an email which appears to come from a bank or financial institution warning of some dire consequence and requesting verification of some information.

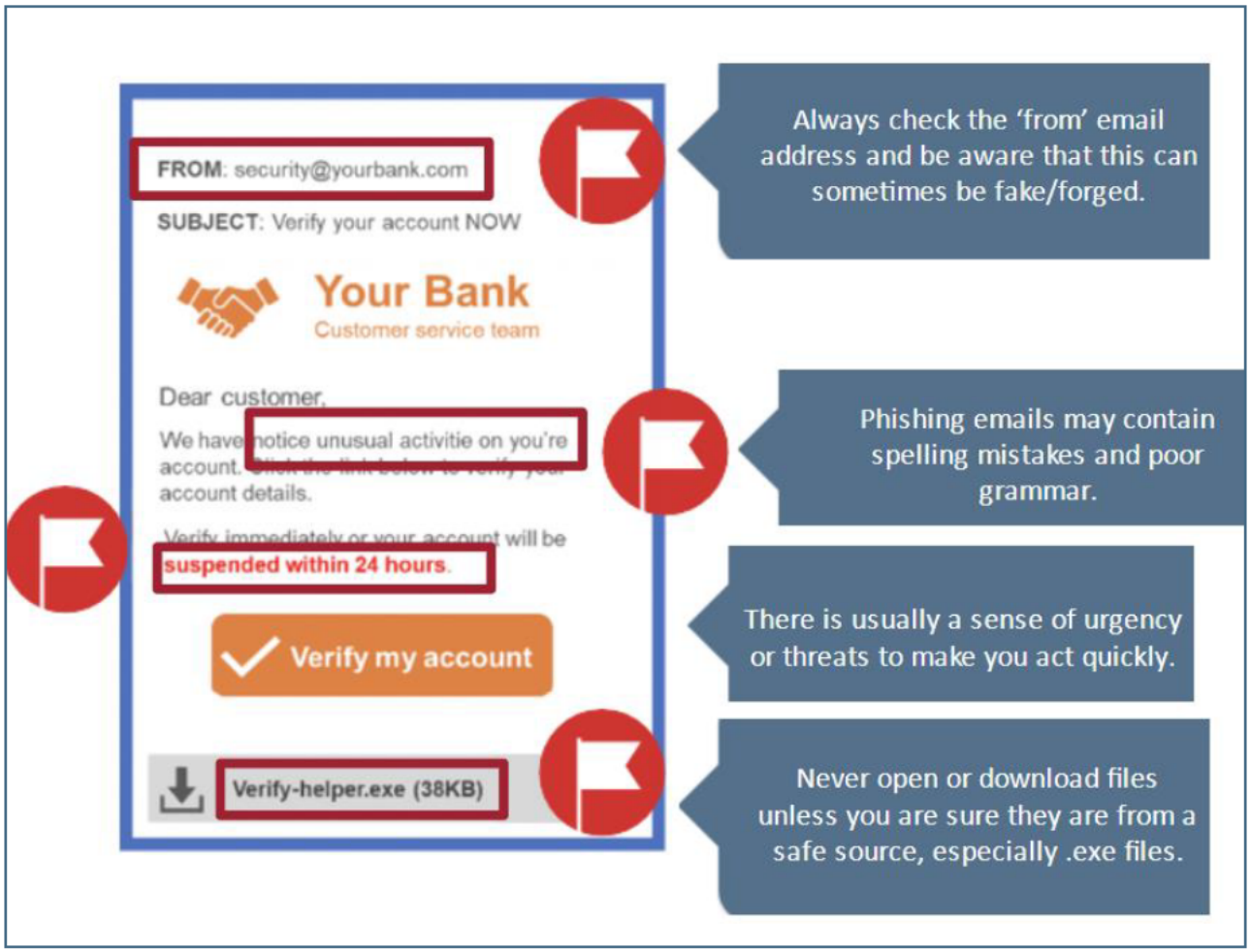
Phishing scams usually involves a link to a fraudulent web page which has been created to appear legitimate by providing company logos and a similar look and feel to the authentic page. The victim is directed to a rogue web page where they are requested to complete a form or download a 'security' file. The victim has then either provided the information required for an attacker to access a

secure resource such as an on-line bank account or has downloaded a malicious software file which may compromise their computer.

A malicious software file can also lead to a successful ransomware attack where files become locked or encrypted so victim can no longer access them. A ransom, usually in the form of cryptocurrency, is demanded to unlock or restore access to the files.

Users are to refer to their mandatory security basics training available on the Acorn Learning Management System (LMS) and follow the following precautionary measures.

- Always check where an email is sent from (check senders domain, the bit after the @)
  - Don't open or reply to emails from unfamiliar sources
- Don't open attachments from unknown senders
- Don't click on links you are unsure of or are not expecting
- If unsure of an email or sender refer the email or attachments to the Cyber Security team or the IT Service Desk



The figure above shows a phishing example and how to identify a phishing emails (adapted from https://www.scamwatch.gov.au/).

Baiting

Baiting is like the real world Trojan horse that uses physical media and relies on the curiosity or greed of the victim. In this attack, the attacker leaves a malware infected USB flash drive or media device in a location where it is sure to be found. Often people will plug in and open up these devices at the next computer they have access to, possibly their work computer. As soon as they plug in that device, the attack has a chance to execute on the victims computer and compromise the rest of the network it is attached to.

7.3 Testing Security Weaknesses

Anyone that discovers a perceived security weakness in agency-provided ICT systems must not attempt to prove a suspected weakness. Unauthorised testing of perceived security weaknesses may be interpreted as misuse of agency systems. Such testing may result in disciplinary action being taken.

This includes the practice of 'baiting' a scammer or phishing attacker. Users must not respond to any confirmed threat email for any reason.

7.4 Misuse of Computer and System resources

Use an agencies ICT facilities for purposes other than to conduct government business or to perform the functions of an agency may have a number of adverse effects:

- Misuse of IT facilities could impact on the operations of a Government agency and an individual or business area ability to perform their duties
- Exposure of users to obscene, sexist or racist material or other offensive material or bullying of a person by another employee using IT services is considered harassment and can negatively impact the wellbeing and health of staff; and
- Misuse of IT facilities could lead to legal liability or damage the reputation of an agency or the Australian government.

Authorised users must not misuse an agencies ICT facilities, devices or services for any reason. All reported or suspected instances of misuse will be investigated and may be treated as an APS code of conduct or security breach.

7.4.1 Continuous Monitoring Program

All systems managed by PM&C are subject to continuous monitoring principles in line with ACSC requirements, including:

s 47E(d)

s 47E(d)

This continuous monitoring and the outputs of these scans may be used to detect misuse of PM&C-managed systems.

7.4.2 Types of Misuse

Misuse of departmental systems includes, but is not limited to:

- Attempting to modify or remove computer and system resources without proper authorisation
- Attempting to install unauthorised hardware or software
- Aiding or allowing members of the public (including family members) to access departmental ICT resources
- Using computer and system resources for purposes other than those for which they were intended or authorised
- Taking advantage of another user's naivety or negligence to gain access to computer and system resources
- Software piracy, illegally streaming content or downloading inappropriate content
- Impacting on computer and system resources through activities such as video games, sending excessive or frivolous messages or printing excessive copies of personal documents
- Disclosing or removing third-party proprietary information.

Unacceptable uses of agency ICT facilities include:

- Any use in breach of a Commonwealth law or the Australian Public Service (APS) Code of Conduct
- Distributing material that is harmful to, or that conflicts with, the interests of the Commonwealth or the Department
- Breaching intellectual property rights, including copyright on software
- Interfering with the authorised use of the ICT facilities by others
- Intentionally disrupting the operation of the ICT facilities, spreading viruses with intent to cause harm or gaining unauthorised access to a computer system
- Gaining, or attempting to gain, unauthorised access to ICT facilities and information
- Altering, deleting, inserting, or damaging that information
- Using ICT facilities for private commercial activities, or private activities such as online gambling, or for party political activity
- Intercepting another person's communications or email without permission from the individual or the Cyber Security team
- Importing, creating, intentionally accessing, possessing or distributing any offensive, obscene or indecent images, data or other material including material which has as its main focus pornography, nudity or sexual acts
- Distributing defamatory, abusive, sexist or racist material or material likely to promote hatred or to incite violence against identifiable groups

- Distributing chain, nuisance or offensive emails
- Distributing email anonymously, using a false identity or using another person's user account
- Using internal contact lists, addresses or email address lists for personal circulation (i.e. for non-official purposes) and providing such information to external organisations or individuals
- Distributing communications or email that disclose personal information without appropriate authorisation
- Intentionally using the ICT facilities to harass, intimidate, threaten or offend another person.

The distribution of union material using agency ICT systems may be sanctioned by an agencies Senior Executive Staff. Union representatives or affiliates should contact an agencies HR team for more information on this matter.

7.5 Reporting of an Incident, Breach, Infringement and/or Violation

ICT Security incidents are a subset of the reportable security incidents for an agency. A reportable incident is any failure, suspected failure or identified deficiency which may result in a security exposure of an agencies ICT systems.

In order to ensure that all ICT resources remain secure, all users must report ICT security incidents, breaches, infringements and violations as soon as possible after detection or suspicion of activity. To report an incident, a user should contact the Cyber Security team, agency Security team or IT Service Desk directly for further instructions.

Cyber Security incidents can be directly reported via the Service Portal as well.

The breach or loss of information that is likely to result in serious harm to any individuals whose personal information is involved in the breach must be reported to the Office of Australian Information Commissioner (OAIC) under the Notifiable Data Breaches scheme (NDB). The NDB scheme applies to all agencies and organisations with existing personal information security obligations under the Australian Privacy Act 1988 (Privacy Act).

The NDB scheme introduced an obligation to notify individuals whose personal information is involved in a data breach that is likely to result in serious harm. This notification must include recommendations about the steps individuals should take in response to the breach. The Australian Information Commissioner (Commissioner) must also be notified of eligible data breaches. In almost all cases NDB reporting will be done by the Records Management team within PM&C, or the ITSA or ASA.

7.6 Reporting Theft and Loss of Computer and Mobile Media Equipment

On detecting the loss or theft of departmental equipment the user must alert the Cyber Security team or IT Service Desk as soon as possible. The Service Portal has an online form designed for this situation.

Reports of lost and stolen devices must include the following details:

- Device owner
- Nature and location of loss
- Date of loss
- Brief outline of data stored on the device.

A police report should be obtained in those cases where the loss is known or suspected to be the result of theft, robbery or fraud.

In the case of a lost or stolen Apple or other PM&C-issued device, and on instruction from the Director of ICT Operations or CIO, the IT Service Desk will initiate a 'Kill Handheld" signal causing deletion of all data on the lost or stolen device. Users should note that no personal data will be recoverable from a phone that has had this command applied.

7.7 Sanctions

Penalties for misuse of computers and system resources can range from counselling or suspension of system access rights, through to dismissal and/or legal action.

Any penalties against employees will comply with the terms and conditions of their employment and appropriate legislation.

A breach of this Policy could result in disciplinary action (including dismissal) under the *Public Service Act 1999* or criminal prosecution or both.