s22 [redacted]

Australian Government
Department of the Prime Minister and Cabinet

Security

3.4.1.3 – Information Security Protocol

Effective Date: 30/01/2015
V2.4

s22 [redacted]

Approvals

Owner

Name:

Title:

Authorisation

Name: s22

Title: Senior Advisor, PM&C Security

Production History

Function	Date	Name	Position
Prepared	27/01/2015	s22	Technical Writer
Reviewed	29/01/2015	s22	Security Adviser, National Ops
Reviewed	30/01/2015	s22	Technical Writer

Release History

Version	Name	Description	Approval	Date
1.0	s22	Draft		20/06/2013
1.1	s22	Revisions		16/07/2013
1.2	s22	Further revisions and additions		20/08/2013
2.0	s22	Updating for publishing on Intranet		15/04/2014
2.1	s22	Migration to new Policy Template		30/01/2015
2.2	s22	Final Accessibility check		30/01/2015
2.3	s22	Accessibility added to Flowchart		02/02/2015
2.4	s22	Update section on disposal of classified information		21/05/2018

Table of Contents

Contents

List of Tables

List of Figures

1. Introduction

The fundamental rule of information security is that all access decisions are based on a 'Need-to-Know' requirement. A person must have a real need to access the information or area in order to carry out their official duties. Other justifications, such as seniority, grade, position of authority or even the need to enter controlled areas for the sake of convenience, are not valid.

All employees requiring regular access (i.e. more than two business days) to a PM&C Canberra tenancy and/or access to PM&C's Protected IT Network (PNet) must hold at least a Baseline clearance prior to access being granted.

Contractors or other personnel who will be accessing classified material or PNet systems as part of their contracted service provisions also require a Baseline clearance. Where this is the case, requirements should be clearly outlined in tender and contract documentation, and contract managers should ensure that checks are in place when contract personnel change. Financial Management Branch can provide assistance with drafting tender or contract documents to specify clearance requirements

2. Description and use

2.1 Description

This protocol has been created to provide further instruction of requirements set out in the PM&C Security Policy in relation to PM&C information security.

2.2 Intended use

This procedure outlines the security requirements for the handling, storage and destruction of all official and classified information held by PM&C people and entities.

3. Reference information

3.1 Referenced documents

Table 1 provides a list of all documents used as a reference for this document.

Table 1: References

Reference	Title
Policy	• Australian Government Protective Security Policy Framework, 2010 • AS/NZS 31000 Risk Management • Security Equipment Catalogue 2009
Legislation	• Public Service Act 1999 • Financial Management and Accountability Act 1997 • Crimes Act 1914 • Privacy Act 1988 • Freedom of Information Act 1982 • Archives Act 1983 • Public Order (Protection of People and Property Act) 1971 • Workplace Health and Safety Act 2011
Internal	• PM&C CEI X.X Security (obsolete) • PM&C Risk Management Framework • PM&C Business Continuity Framework • PM&C CEI 1.2 Preventing Fraud - Operational Guideline (2012-14 Fraud Control Plan) • PM&C Policy on Freedom of information and Privacy.

3.2 Associated documents

Table 2 provides a list of all other associated documents that should be read in conjunction with this document.

Table 2: Associated Documents

Reference	Description and Link
1	PM&C Security Policy
2	PM&C Information Security Protocol
3	PM&C Physical Security Protocol

3.3 List of acronyms

Table 3 provides a list of all acronyms referenced within this document.

Table 3: Acronyms

Acronym	Definition
ASA	Agency Security Adviser
BILs	Business Impact Levels
DLMs	Dissemination Limiting Markers
PM&C	Department of the Prime Minister and Cabinet
PNet	PM&C's Protected IT Network

3.4 Glossary

Table 4 provides an explanation of terms used within this document.

Table 4: Glossary

Term	Definition

4. Responsibilities

All PM&C people – encompassing all employees, contractors, clients or official visitors - are responsible for their actions relating to the maintenance of security within PM&C. Every PM&C person is to actively comply with all PM&C security policies and procedures relevant to their employment.

5. Procedure

The Commonwealth has a prescriptive and structured approach to information security, and PM&C is required to ensure our own protocols are entirely consistent with Government business.

Information resources must be protected from compromise and misuse, as follows:

- All official information must be handled with care and in accordance with authorised procedures;
- All official information is only to be made available to those who have a legitimate need-to-know (i.e. you only access information that is necessary for you to carry out your work);
- All official information is only to be released in accordance with policies, legislative requirements, or directives of governments or courts;
- Unauthorised access and/or disclosure is to be prevented;

- Where necessary, employees or contractors are to have a current and appropriate Australian Government security clearance; and
- Employees and contractors must adhere to the clear desk policy.

5.1 Business Impact Levels

The Protective Security Policy Framework defines a series of commonly applied Business Impact Levels (BILs) to assist in collaborative Government operations.

These BILs are applied consistently across the Commonwealth to ensure consistency in the way information is classified and handled.

Notwithstanding issues of aggregation or other sensitivity, the BIL's loosely correspond to the Protective Marking standards, as discussed in Section 5 of this document, and are defined below:

Table 5: Business Impact Levels and the associated Protective Security Markings

MARKING	BUSINESS IMPACT LEVEL (BIL)
For Official Use Only (FOUO)	1 - LOW
SENSITIVE	2 - MEDIUM
PROTECTED (incl. SENSITIVE : CABINET)	3 - HIGH
CONFIDENTIAL	4 - VERY HIGH
SECRET	5 - EXTREME
TOP SECRET	6 - CATASTROPHIC

As the majority of PM&C's information resources fall into the LOW and MEDIUM category of these BIL's, our policy and risk management strategies are tailored accordingly. There is, however, very specific guidance relating to quantities of HIGH category information PM&C handles on behalf of the Australian Intelligence Community and Government.

5.2 Need to Know

The Protective Security Policy Framework defines the Need to Know principle as *"The availability of official information should be limited to those who need to use or access the information to do their work."*

Staff should be aware that access to official information must only be undertaken where a demonstrable Need to Know exists. Access to official information is recorded and monitored, and staff may be asked to explain the circumstances of access from time-to-time.

Staff found to be accessing information (including ICT systems) without a demonstrable Need to Know should be aware that breaches of this policy can result in disciplinary action under the APS Code of Conduct, and impact upon their ongoing eligibility to hold a Commonwealth security clearance.

Staff are also bound by applicable legislation regarding information security, including the Social Security (Administration) Act 1999 and the Privacy Act (1988).

5.3 Official Information

There are two types of Official Information within PM&C;

- *Information that does not need increased security.* This is defined as any information already sanctioned for public access or circulation, or any other record that does not contain sensitive or private information. This information can be marked UNCLASSIFIED.
- *Information that needs increased security to protect its confidentiality, integrity and availability.* This is defined as any information which could reasonably be expected to harm or adversely impact PM&C or our stakeholders. A range of protective markings can be used to identify information requiring additional protection.

5.4 Protective Markings

Once information has been identified as requiring some form of protection and special handling a protective marking is to be assigned to the information. The marking indicates:

- that the information has been identified as sensitive or security classified; and
- the level of protective procedures that are to be provided during the use, storage, transmission, transfer and disposal of the information.

Where an asset has been assessed as requiring protection, a protective marking should be assigned to it. An asset can be a paper based document, an email, electronic documentation or even portable ICT media such as USB drives, CDs/DVDs or laptops.

There are three types of protective markings that can be applied to an asset:

- security classifications;
- dissemination limiting markers (DLM); and
- caveats.

Further guidance regarding the types of information that requires classification can be found below. Alternatively, any queries regarding the classification of information can be referred to Security s22.

5.4.1 Security Classifications

Some information within PM&C will require a Security Classification, and the below guidance is provided as a basic tool for staff.

Further details can be sourced from the *Classification of Information Guide*.

Under the Commonwealth framework there are four levels of Security Classification that can be assigned to an asset. These are:

- PROTECTED – used when the compromise of the information could cause damage to the Australian Government, commercial entities or members of the public;
- CONFIDENTIAL – used when compromise of the information could cause damage to national security;
- SECRET – used when compromise of the information could cause serious damage to national security, the Australian Government, nationally important economic and commercial interests, or threaten life; and
- TOP SECRET – used where compromise of the information could cause exceptionally grave damage to national security.

5.4.2 Dissemination Limiting Markers (DLMs)

Most of the sensitive information within PM&C falls within the category of Dissemination Limiting Marker (DLM).

Dissemination Limiting Markers are used for information where disclosure may be limited or prohibited by legislation, or where other special handling requirements may apply.

There are five recognised categories of DLM in use within the Commonwealth.

- FOR OFFICIAL USE ONLY (FOUO) – used on UNCLASSIFIED material **only**, when compromise or disclosure may cause limited damage to the Australian Government, commercial entities or members of the public.

  Examples within PM&C of information falling within this category include tender submissions, internal correspondence, departmental financial statements or any other routine information that could expose PM&C to risk.

- SENSITIVE – used with security classified or UNCLASSIFIED information. SENSITIVE should be used where secrecy provisions of enactments may apply or where disclosure is prohibited under legislation.

  Examples where this DLM would be used within PM&C could include security briefings or legislative reviews.

- SENSITIVE: PERSONAL – used with security classified or UNCLASSIFIED information. This marking must be used where the information pertains to sensitive personal information.

- SENSITIVE: LEGAL – used with security classified or UNCLASSIFIED information. This marking is used for information that may be subject to legal professional privilege.

- SENSITIVE: CABINET – used with security classified information of **at least** PROTECTED used for any document including business lists, minutes, submissions, memoranda or other correspondence that is or has been submitted to Cabinet.

5.4.3 Caveats

Some security classified information may bear a security caveat in addition to a Security Classification. The caveat is a warning that the information may have special requirements in addition to those indicated by the protective marking.

Caveats are not security classifications in their own right, and will only appear in conjunction with the appropriate Security Classification. Those personnel with a Need to Know will be appropriately briefed and cleared to access information bearing a caveat – all other staff must not have access to this information.

There are very few examples of caveat related information within PM&C, however some of the more common-place caveats staff may encounter are:

- AUSTEO means Australian Eyes Only. There are various other forms of "Eyes Only" caveats, specifying other nations. Typically these are Australia's "five eyes" partners, and are identified as:

  USA – United States of America

  UK – United Kingdom

  CAN - Canada

  NZL – New Zealand

- AGAO means Australian Government Access Only
- ORCON means that the information is Originator Controlled, that is that it cannot be disseminated without the originator's knowledge and consent
- LIMITED ACCESS means that the information must only be disseminated to those officers (or office holders) specified
- DELICATE SOURCE means that personnel should be aware that the originator of the information has identified the source as being highly sensitive.

Any staff-member required to access caveat marked information must seek guidance from Security (s22) before doing so.

5.4.4 Codewords

Codewords are used in addition to a classification (and sometimes in conjunction with caveats) to identify that the information relates to the activities of specific intelligence agencies (also referred to as "compartments"). Access to Codeword information is strictly controlled by the relevant agency (referred to as "compartment owners"), in conjunction with the Agency Security Adviser (ASA).

Current compartments accessed by PM&C staff are identified on access passes as C, D, E and G (also referred to as Charlie, Delta, Echo and Gamma). There are a number of codewords used within these compartments, some of which are classified.

Staff requiring access to a compartment must submit a business case, outlining why access is required, and have it approved by their Assistant Secretary before submission to Security s22.

Staff handling information with unfamiliar or unknown markings must contact Security as soon as possible to ensure appropriate handling and briefings are in place.

5.4.5 Cabinet Documents

Documents used by cabinet to formulate policy and make decisions require special protective measures. All documents prepared for consideration by cabinet, including those in preparation are to be marked SENSITIVE: CABINET, as well as carry the Security Classification protective marker PROTECTED as a minimum. An example of the appropriate Header and Footer for these documents would appear as below:

Figure 1: Protected and Sensitive: Cabinet Label

5.5 Clear Desk Policy

At the close of business and during extended absences from their workplace, employees must ensure that official information and assets are secured appropriately. Managers and staff must ensure that:

- There is no security classified or DLM information left out in the workplace, including files, papers, photocopies or other materials left on printers or fax machines;
- Laptops and other electronic media (USB, CD's etc.) storing security classified information are secured by a Kensington lock, or in an appropriate locked container;
- Whiteboards and other displays are cleared of any sensitive or security classified information;
- Safes and containers (e.g. compactus shelving, filing cabinets) are locked;
- Office doors are locked;
- Keys to secure "C-class" containers are removed from the locks, and secured in a Security-approved key container, or by Security;
- Keys to all other containers are not left accessible or visible; and
- Staff log off from all electronic systems.

In order to ensure compliance with this policy, regular reviews of PM&C work-spaces will take place. These checks will involve security staff and/or security guards reviewing work-stations and containers to ensure classified information and resources are appropriately secured.

Whilst the ultimate aim of this policy is to maintain the confidentiality, integrity and availability of information, staff should be aware that serious or ongoing breaches of this policy can result in disciplinary action under the APS Code of Conduct. Ongoing infringements or breaches can also impact upon a person's ongoing eligibility to hold a Commonwealth security clearance.

5.6 Storage of Sensitive Information

All Official Information should be appropriately secured in the work-place; however specific handling requirements apply to information bearing a Security Classification and/or a DLM. The table, as displayed on page provides advice to staff who handle this type of information.

5.6.1 Storage of Sensitive and Classified Information

Table 6: Storage of Sensitive Information within PM&C tenancies

MARKING	PM&C CANBERRA TENANCIES	PM&C REGIONAL TENANCIES
For Official Use Only (FOUO)	Locked commercial grade (D-Class) container	Locked commercial grade (D-Class) container
SENSITIVE	Locked commercial grade (D-Class) container	Locked commercial grade (D-Class) container
SENSITIVE: PERSONAL	Locked commercial grade (D-Class) container	Locked commercial grade (D-Class) container
SENSITIVE: LEGAL	Locked commercial grade (D-Class) container	Locked commercial grade (D-Class) container
SENSITIVE: CABINET	Locked C-Class Container	Locked C-Class Container
PROTECTED	Locked C-Class Container	Locked C-Class Container
CONFIDENTIAL	Locked B-Class Container	Locked B-Class Container
SECRET	Locked B-Class Container	*Contact Security* s22*
TOP SECRET	*Contact Security* s22*	*Contact Security* s22*

**This information must only be handled and stored in approved spaces. A list of these spaces is outlined in the Physical Security Protocol. Any access or storage of this level of information outside of these spaces is likely to constitute a serious breach of Departmental policy and Commonwealth legislation.*

Any further queries regarding the storage of sensitive information should be directed to Security s22.

5.7 Transfer of Sensitive Information

5.7.1 Transfer of Sensitive Information within PM&C

There are several ways to transfer DLM or Security Classified information within and between PM&C tenancies. Staff should always be mindful of ensuring that sensitive information is afforded appropriate protection before transfer occurs.

The first means of transferring information relates to physical information. The table found over the page can be applied to the transfer of paper files as well as portable ICT hardware which contains sensitive or Security Classified information.

Where sensitive or classified information is transferred internally staff must ensure it is protected appropriately. Ministerial Support Division and Records Management have their own policies and practices for ensuring the security of information within the internal mail system; however, staff are asked to ensure the following guidelines are used for transit of any sensitive or security classified information.

5.7.2 Transfer between PM&C Tenancies via Mail or By Hand

Table 7: Transfer between PM&C Tenancies via Mail or by Hand

MARKING	SINGLE LOCATION	BETWEEN TENANCIES
For Official Use Only (FOUO)	Uncovered, by hand	Single Envelope, Internal Mail
SENSITIVE	Uncovered, by hand	Single Envelope, Internal Mail
SENSITIVE: PERSONAL	Uncovered, by hand	Single Envelope, Internal Mail
SENSITIVE: LEGAL	Uncovered, by hand	Single Envelope, Internal Mail
SENSITIVE: CABINET	Covered, direct delivery by hand	Single opaque envelope, approved briefcase, direct delivery by hand and receipt **or** Double enveloping, safe-hand courier and receipt
PROTECTED	Covered, direct delivery by hand	Single opaque envelope, approved briefcase, direct delivery by hand and receipt **or** Double enveloping, safe-hand courier and receipt

MARKING	SINGLE LOCATION	BETWEEN TENANCIES
CONFIDENTIAL	Covered, by hand person to person	Double enveloping, tamper-evident seal, approved briefcase, direct delivery by hand and receipt **or** Double enveloping, safe-hand courier and receipt
SECRET	Covered, by hand person to person	Double enveloping, tamper-evident seal, approved briefcase, direct delivery by hand and receipt **or** Double enveloping, tamper-evident seal, safe-hand courier and receipt
TOP SECRET	Covered, by hand person to person	Double enveloping, tamper-evident seal, approved briefcase, direct delivery by hand and receipt **or** Double enveloping, tamper-evident seal, safe-hand courier and receipt

For material marked with both a Security Classification and a DLM, use the instructions for the Security Classification level. For example, follow the PROTECTED instructions for a document classified **PROTECTED Sensitive: Personal.**

5.7.3 Transfer of Information via Electronic Systems

Transfer of information via electronic systems provides fast and effective means to disseminate information. When using any electronic means to transfer sensitive or classified information, staff should take care to ensure the distribution list is correct and in accordance with Need to Know principal.

The following table outlines how information can be transferred within PM&C.

Table 8: Transfer via Electronic Systems

MARKING	PM&C TENANCIES
For Official Use Only (FOUO)	PM&C Protected Network **or** PM&C Unclassified Network
SENSITIVE	PM&C Protected Network **or** PM&C Unclassified Network
SENSITIVE: PERSONAL	PM&C Protected Network **or** PM&C Unclassified Network
SENSITIVE: LEGAL	PM&C Protected Network **or** PM&C Unclassified Network
SENSITIVE: CABINET	CABNET#
PROTECTED	PM&C Protected Network **or** MCN **or** SATIN HIGH
CONFIDENTIAL	MCN **or** SATIN HIGH*
SECRET	MCN **or** ASNET **or** DSN **or** SATIN HIGH*
TOP SECRET	*Contact Security* s22

**SATIN HIGH can be used for the transfer of information classified up to SECRET where appropriate. Please contact Security on s22 for guidance.*

#Any document that is drafted in the Cabinet Submission/Memorandum template, or document which looks like a Cabinet submission (pre-exposure drafts, exposure drafts, drafts for coordination comments, final submissions and drafting comments) must only be circulated between departments via the CABNET system, even if it is only classified Protected. Cabinet Submissions and Memoranda

that are being circulated for consultation must be locked-down and lodged on the appropriate CABNET database.

5.7.4 Transfer of Sensitive Information to non-PM&C Personnel

Australian Government employees are to have agency authorisation to release any information to members of the public. Authorisation may be granted by the agency head or a person authorised by the agency head. When personal information is involved, any release is to comply with the Privacy Act 1988 (the Privacy Act).

Even if information is intended for public release or publication it could have confidentiality requirements before release—for example, Budget papers. In this case, the point at which the information will be publicly available is to be marked. When this information ceases to need secure treatment, agencies need to consider continuing availability and integrity requirements.

All personal information held—even if it is publicly available—is to be handled in accordance with the Information Privacy Principles (IPPs) in the Privacy Act.

Circumstances may arise where information is required to be transferred to personnel outside of PM&C. Examples of this might include other Commonwealth entities or even Ministerial and Electorate staff.

Where transfer to other entities is required staff must ensure a Need-to-Know exists and that the recipient has an appropriate security clearance and/or storage facilities to meet PM&C requirements.

The physical transfer of hard-copy or portable media is covered in the following table.

Table 9: Transfer to non-PM&C Personnel

MARKING	TRANSFER TO NON-PM&C PERSONNEL
For Official Use Only (FOUO)	Single envelope Australia Post – general mail
SENSITIVE	Single envelope Registered mail or safehand courier
SENSITIVE: PERSONAL	Single envelope Registered mail or safehand courier
SENSITIVE: LEGAL	Single envelope Registered mail or safehand courier
SENSITIVE: CABINET	Double enveloped and safehand courier, receipted and registered in accordance with Cabinet requirements
PROTECTED	Double enveloped and safehand courier
CONFIDENTIAL	Double enveloped, tamper-evident seals, safehand courier and receipting

MARKING	TRANSFER TO NON-PM&C PERSONNEL
SECRET	Double enveloped, tamper-evident seals, safehand courier and receipting
TOP SECRET	Double enveloped, tamper-evident seals, safehand courier and receipting

5.7.5 Travelling with Sensitive Information

From time to time PM&C staff may be required to travel interstate with sensitive/classified information. When this circumstance arises staff should take care to ensure that any sensitive/classified information is handled carefully. The table on the following page outlines staff requirements regarding travel with sensitive/classified information.

Table 10: Travelling with Sensitive or Classified Information

MARKING	TRAVEL WITHIN AUSTRALIA
For Official Use Only (FOUO)	Single Envelope Secured or hand luggage
SENSITIVE	Single Envelope Lockable Briefcase or Secured Luggage
SENSITIVE: PERSONAL	Single Envelope Lockable Briefcase or Secured Luggage
SENSITIVE: LEGAL	Single Envelope Lockable Briefcase or Secured Luggage
SENSITIVE: CABINET	Double Envelope with Wafer Seals Lockable SCEC Endorsed Briefcase* Carry-on luggage only
PROTECTED	Double Envelope with Wafer Seals Lockable SCEC Endorsed Briefcase* Carry-on luggage only
CONFIDENTIAL	Double Envelope with Wafer Seals Lockable SCEC Endorsed Briefcase* Carry-on luggage only
SECRET	Double Envelope with Wafer Seals Lockable SCEC Endorsed Briefcase* Carry-on luggage only
TOP SECRET	*Contact Security s22*

**Please contact Security if you have a requirement to access a SCEC endorsed lockable briefcase.*

Staff travelling internationally with sensitive information should contact Security S22 for specific guidance at least three weeks prior to undertaking travel.

5.8 Disposal of Classified and Official Information

Every staff member in the Department has a responsibility to protect classified and privileged information. This will require all staff to develop and maintain a positive attitude about information entrusted to them, and how it needs to be managed.

Disposal of paper-based information

The following table outlines options to dispose of information.

Table 11: Disposal of Paper

MARKING	ALL PM&C OFFICES
UNCLASSIFIED – no DLM information	General Recycling Bin (unlocked bin)
For Official Use Only (FOUO)	Secure Waste Bin (locked bin)
SENSITIVE	Secure Waste Bin (locked bin)
SENSITIVE: PERSONAL	Secure Waste Bin (locked bin)
SENSITIVE: LEGAL	Secure Waste Bin (locked bin)
SENSITIVE : CABINET	Secure Waste Bin (locked bin)
PROTECTED	Secure Waste Bin (locked bin)
CONFIDENTIAL	Class A Shredder Only
SECRET	Class A Shredder Only
TOP SECRET	Class A Shredder Only

TOP SECRET, codeword and registered Cabinet documents must be returned to the originator. These documents require a destruction certificate that must be witnessed by two staff.

Information and Records Management must be consulted for specific guidance regarding the Archives Act (1983) prior to disposal of any sensitive or security classified information.

Blue waste bins

PM&C staff will have access to two types of paper waste disposal. The first is general waste, which can be used for all unclassified paper-based information. Information assigned a DLM rating must not be disposed in unsecure bins. These bins are unlocked, and generally blue. They have yellow signage on top instructing staff that Unofficial or Unclassified documents can be disposed of in the bin.

PM&C staff will also have access to secure waste bins. These locked bins have a white sign on top instructing staff that documents up to PROTECTED Sensitive Cabinet can be disposed of in the bin.

When full, all bins are moved to the basement for processing. Prior to moving, unclassified 'recycling' bins are labelled by the cleaners (or persons changing the bins), to identify the area from where they are collected, and moved to the basement. The bins are spot checked by Security, and then placed in a holding area when ready for collection by an external contractor.

The blue bins used for the larger document shredders are treated in the same manner as the unclassified recycling bins.

Secure bins are moved from the floors to the basement by SNP guards. They are stored in a secure access controlled holding area rated to accept PROTECTED documents. These bins are collected on Thursdays. The bins remain locked as they are loaded on the truck, and transported to the Iron Mountain destruction facility.

Should staff encounter a situation where they are uncertain about a document and whether it can be disposed of safely in any blue bin, they are advised to shred the document.

Staff awareness and outreach

There are circumstances where the risk of incorrect disposal is higher than usual particularly during staff relocation. Staff are given training that covers information handling and disposal as part of induction, and special briefs are also arranged to assist staff prior to bulk relocations. Information on document handling is provided on the intranet to assist staff.

Management of improper disposal of official and classified information

Classified or DLM information recovered from the blue unsecured recycling bins will be treated as a security breach. The basic principles to be followed to manage the process is highlighted below.

Detection and Recovery

Security undertake spot checks to uncover information incorrectly disposed of in the blue recycling bins. Information incorrectly disposed will be recovered by Security and details will be recorded in the incident database. The area responsible for the information may be contacted to provide one or more staff to check the bins. If the information is deemed accountable material, a formal record will be retained in a CDR.

Notification

Security will dispatch an email to the SES 1 level staff member in charge of the area where the information originated, advising of the breach and seeking an explanation of why the material had been disposed of incorrectly. The Security executive will also be included in the email. The aim of the process is to give notice, to observe if they acknowledged accountability and if any activities are suggested to prevent recurrence.

Evaluation

If the breach was a first – and depending on the classification of the material, and type of response from the SES staff member – a caution should be issued. However, a formal breach can and should be issued if deemed more appropriate. If accountable material is recovered, or is classified higher than PROTECTED, a formal breach should be issued.

Return of documents

Documents recovered by Security will be returned to the SES 1 staff member, or a suitable representative. The line area is responsible for disposing of the recovered information.

Process review

Security will monitor the disposal process and adjust these if new vulnerabilities are identified, or to improve destruction controls as required.

5.8.1 Disposal of ICT storage devices

Where ICT storage media (e.g. CD/DVD, USB thumb drives, external hard drives) are surplus to requirements and are to be disposed of, they must be sanitised using a Australian Signals Directorate (ASD) approved product- e.g. FEDERASE.

Where the device cannot be sanitised, the unit must be destroyed. Media devices can be surrendered to PM&C Security for destruction within the ACT. Regionally-based staff should contact PM&C Security for advice before disposing of electronic media.

5.9 Working from Home

Home-based work must occur in a suitably secure environment. Security must undertake a risk assessment of a staff member's home and provide a report to the staff member's supervisor and Assistant Secretary as well as the People, Capability and Performance Branch before approval can be granted for home-based work.

Any person seeking to undertake home based work must use the Citrix Remote Secure Access (RSA) facility provided for remote access to the PM&C network. Official Information must not be emailed to an employee's personal e-mail accounts, and electronic information must not be uploaded onto non-Departmental ICT equipment (including portable media such as USB drives, DVDs etc.).

Any physical documents removed from PM&C premises must be handled and stored in accordance with the requirements outlined in this protocol, however it should be noted that unless exceptional circumstances apply, it is not permissible to work on Security Classified or DLM marked information from the home environment.

5.10 Contracted Services Providers and PM&C Information

Staff should be mindful of ensuring the security of PM&C information when dealing with contracted providers. Security should be consulted regarding storage, handling and transfer of any sensitive information a contractor accesses on behalf of PM&C.

Any instance where a contracted provider advises PM&C of information loss or compromise must be reported to Security s22 immediately.

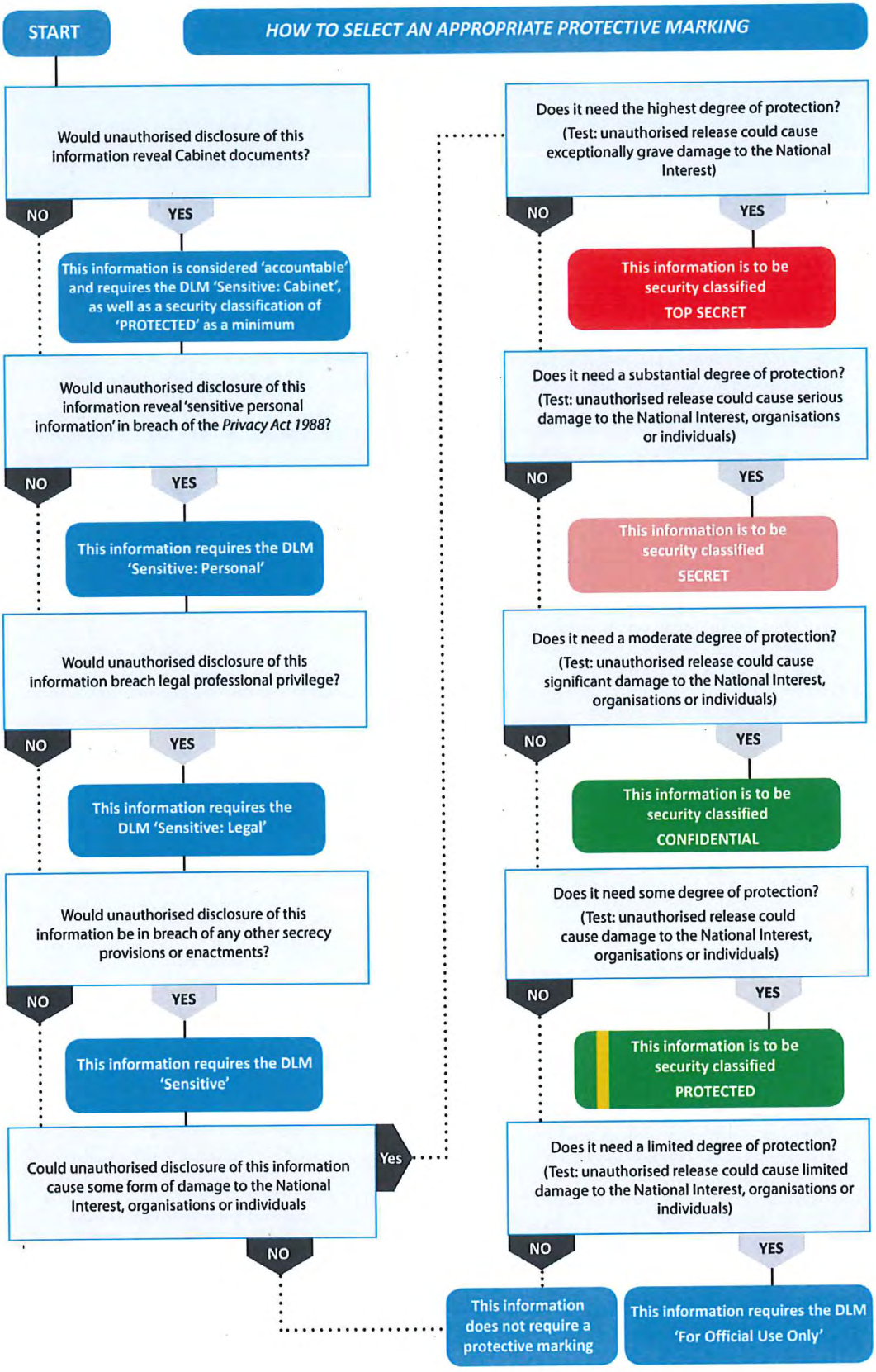

Figure 2: How to Select an Appropriate Protective Marking Flowchart