Australian Government

Services Australia

Cyber Security Event Logging and Monitoring Policy

July 2024

TECHNOLOGY AND DIGITAL PROGRAMS

Contents

Introduction

As the primary service delivery agency for the Australian government, Services Australia (the agency) supports millions of Australians through delivering social welfare services and payments. To support delivery of these services and payments, the agency holds and uses large volumes of sensitive customer data. This makes the agency a target for cyber security attacks by malicious groups and individuals known as threat actors. The agency regularly identifies attempts by threat actors to gain access to agency systems and the underlying data. The agency's cyber security risk assessments have identified the risks associated with these threat actors to be high.

The Cyber Security Event Logging and Monitoring Policy prescribes controls to protect the agency's ICT systems by detecting and analysing system anomalies, misuse or malicious activity through the collection, storage, retention, monitoring and analysis of cyber security event logs in a timely, accurate and coordinated manner. The agency's management of cyber security event logging and monitoring forms a critical part of detecting cyber security events and incidents. Event logs are also a valuable source of evidence for forensic investigations and may be used for court proceedings.

This policy supports business and compliance outcomes including early detection of cyber security events (events), timely and effective incident response, and adherence to mandatory Protective Security Policy Framework (PSPF) requirements and Information Security Manual (ISM) guidance.

This policy is a control in alignment with the agency Enterprise Risk Management Policy and Framework for risks against customer and staff data, and payment integrity. This policy must be read in conjunction with the System Authorisation Policy, the key cyber security mechanism established to manage risk at the system level. The event logging and monitoring controls detailed in this policy must be considered in the System Authorisation process and documented in the System Security Plan or Continuous Monitoring Plan as appropriate. Non-compliance risks associated with this policy must be managed in accordance with the System Authorisation Policy and may include a potential re-authorisation of the system.

Any system event logging outside of the agreement between cyber security and the system owner is outside the scope of this policy. All references to event logs or logging made within this policy should be taken as relating specifically to cyber security events unless otherwise stated. For management of cyber security incidents identified through event logging and monitoring or other activities, please see the Cyber Security Incident Management Policy.

This policy prescribes roles for the Chief Information Security Officer (CISO) or delegate, Business and System Owners of ICT systems, Policy Owner, Enterprise Architects and Shared Service Partners who represent Business Owners for their systems.

Policy Aims

The Event Logging and Monitoring Policy enables early detection of cyber security events, timely incident response and adherence to mandatory PSPF and other government requirements.

The policy supports the following business and compliance outcomes:

Business outcome

- To minimise the business impact of a potential cyber security incident or breach by enabling timely response to cyber security incidents identified through the early detection of cyber security events.
- To demonstrate business due diligence by enabling the investigation of past and current cyber security incidents to assist with continuous improvement of the agency's cyber security posture.

Compliance outcomes

- Adherence to:
  - Protective Security Policy Framework (PSPF) -mandated Essential 8 controls related to event logging for multi-factor authentication, restricted administrative privileges and other event types.
  - Australian Signal's Directorate (ASD) ISM requirements for event log retention as mandated by the Archives Act 1983 and the Administrative Functions Disposal Authority (AFDA) Express Version 2.
  - Enterprise Risk Management Policy and Framework to mitigate agency risks in a consistent and coordinated manner.
  - Mandatory agency-specific requirements and directions as included in this policy.

The Event Logging policy supports the following Information Security Manual (ISM) principles:

- **Detect Principle 1 (D1):** Event logs are collected and analysed in a timely manner to detect cyber security events.
- **Detect Principle 2 (D2):** Cyber security events are analysed in a timely manner to identify cyber security incidents.
- **Govern Principle 1 (G1)**: A Chief Information Security Officer provides leadership and oversight of cyber security.
- **Govern Principle 4 (G4**): Security risk management processes are embedded into organisational risk management frameworks.
- **Protect Principle 10 (P10)**: Only trusted and vetted personnel are granted access to systems, applications and data (while this policy does not have control over granting access, it does provide assurance that access is granted to only trusted and vetted personnel).

Policy Directions

The following directions have been developed to support the policy aims above. This includes supporting adherence to the relevant ISM principles and broader PSPF Essential Eight requirements pertaining to event logging and monitoring.

Policy directions align to the ISM principles supported by this policy and are categorised by event logging and monitoring lifecycle stages. Event logs are generated at the system level before being ingested into enterprise tools for cyber security analysis. To reflect this concept, policy directions are categorised as relating to the 'System Level' or 'Agency Level'.

The Roles and Responsibilities section defines the roles for each direction using a unique identifier.

Unique identifiers for policy directions are comprised of the policy reference, EL = Event Logging [and Monitoring], supported ISM principle, D1 = ISM Detect Principle 1, and the unique policy direction number, -1 denotes the first direction contained in the policy which supports the identified ISM principle.

Identifier Component	Description	Example
XX	Policy	EL = Event Logging
-Dx	ISM Detect Principle	D1 = ISM Detect Principle 1
-x	Policy Direction Number	-1 = Policy Direction 1

Designing and Establishing Event Logging Capability

To ensure critical event logs can be collected to assist with detecting cyber security events and incidents, the agency must establish and maintain an event logging and monitoring capability as part of any existing, new or enhanced ICT system. This capability must include provisions for cyber security event log collection, monitoring, storage and retention, and must also be compatible with the agency's endorsed Security Information and Event Management (SIEM) solution. A Continuous Monitoring Plan (CMP) for each system is developed under the System Authorisation Policy to include system-specific information regarding the ongoing security management of ICT systems, including provisions for event logging and monitoring.

Agency Level

EL-D1-1: An agency endorsed cyber security event logging and monitoring framework must be established and maintained to support the identification of applicable logging requirements for ICT systems.

EL-D1-2: Architecturally endorsed log collection patterns are to be developed to support centralised logging.

EL-D1-3: The agency's cyber security logging capability (e.g. a SIEM) must include provisions for protecting stored logs from unauthorised modification and deletion.

EL-D1-4: Processes are implemented at the agency level to monitor cyber security event logs to detect cyber security events and incidents.

EL-D1-5: Timeframes for cyber security event log detection and analysis are to be agreed upon in the system-level Continuous Monitoring Plans (CMP).

System Level

EL-D1-6: New or significantly enhanced ICT systems must include provisions for security event log collection, monitoring, and storage.

EL-D1-7: The logging capability for each system must capture event types, attributes and details commensurate with the assessed risk as agreed with the cyber security function and documented in the CMP.

EL-D1-8: New or changed system monitoring requirements advised by the cyber security function must be implemented within agreed timeframes.

EL-D1-9: System logging capability must include provisions for event log storage and retention, and protecting stored logs from unauthorised modification and deletion.

EL-D1-10: Implement mechanisms to enable extraction of log data from systems in an agreed format compatible with the agency's endorsed SIEM solution.

Using and Maintaining Event Logging Capability

To capture user activities that occur on agency systems for monitoring, detection, compliance, audit and investigation purposes, cyber security event logs and log details must be collected as agreed with the cyber security function. To assist with monitoring the security of agency systems, detecting anomalies or malicious behaviour, and contributing to investigations following cyber security incidents, these event logs must be available for ingestion to the agency's endorsed SIEM.

System Level

EL-D1-11: Cyber security event logs must be generated at the system level and made available to the agency's endorsed SIEM in alignment with endorsed architecture patterns and as agreed with the cyber security function.

Agency Level

EL-D1-12: Cyber security event logs must be ingested to the agency's endorsed SIEM as documented in the System Security Plan (SSP).

Cyber Security Event Log Storage and Retention

To ensure there is an accurate record of all ICT and user activity, all cyber security event logs must be stored and protected from unauthorised modification and deletion. Retaining stored event logs supports future cyber security investigations, retrospective incident detection and adherence to ISM guidance. The AFDA Express Version 2, which is authorised under the Archives Act 1983, states that retention periods for event logs are based on the minimum requirements set in the ISM.

System Level

EL-D1-13: All event logs stored at the system level must be protected from unauthorised modification and deletion in accordance with Essential 8 Maturity Level 2 requirements.

Agency Level

EL-D1-14: All cyber security event logs stored at the agency level are protected from unauthorised modification and deletion in accordance with Essential 8 Maturity Level 2 requirements.

EL-D1-15: All stored cyber security event logs (excluding those for Domain Name System (DNS) services and web proxies) at the agency level are retained for a minimum of seven years, or longer if required for investigation.

EL-D1-16: Stored cyber security event logs (at the agency level) for DNS services and web proxies are retained for a minimum of 18 months, or longer if required for investigation.

Cyber Security Event Log Monitoring and Analysis

To ensure cyber security events and incidents can be detected, analysed and responded to, processes must be implemented at the agency level to monitor security event logs. Internet-facing servers are at higher risk of compromise due to a larger attack surface. If left unmonitored, exposures such as cyber security vulnerabilities may become active attack vectors which increases the risk of a data breach and cyber intrusions. Therefore, event

logs from internet-facing servers must be analysed in an agreed timeframe to detect security events. To ensure faster detection and response to cyber security incidents which will significantly reduce the damage to agency systems and require a lower amount of resources and time to recover, cyber security events must be analysed in an agreed timeframe to identify cyber security incidents.

Agency Level

EL-D1-17: Event logs from internet-facing servers are analysed to detect cyber security events in accordance with Essential 8 Maturity Level 2 requirements and as agreed and documented in the Continuous Monitoring Plan (CMP).

EL-D1-18: Event logs from all systems excluding internet-facing servers are analysed to detect cyber security events in accordance with timeframes agreed and documented in the system's CMP.

EL-D2-1: Cyber security events are analysed at the agency level to identify cyber security incidents in accordance with Essential 8 Maturity Level 2 requirements.

Managing policy

Governance of this policy is managed by the CISO who has responsibility for leadership and oversight of cyber security (ISM Principle G1).

To provide visibility of policy compliance to the broader agency and external reporting authorities, and identify remediation action where non-compliance exists, the following reporting activity must occur:

AC-G1-1: Compliance with this policy must be assessed, documented, and reported to the policy owner using separate reports for each agency system (Cyber Security function) on a periodic basis in alignment with the ICT Governance Framework.

The following actions are required by policy owners to ensure policies remain effective:

AC-G1-2: Review and update the policy as required at least every 18 months.

AC-G1-3: Ensure policy directions are in line with regulatory requirements and industry standards.

AC-G1-4: Report compliance and performance metrics to the Cyber Resilience Board (CRB) and any other boards on a quarterly basis or as required by ICT policy EDM01 Ensure Governance Framework Setting and Maintenance.

AC-G1-5: Identify broad non-compliance with specific policy directions to improve the policy.

AC-G1-6: Use feedback provided by stakeholders to improve the policy.

AC-G1-7: Ensure changes to the policy are approved by the Policy Owner and the Cyber Resilience Board.

AC-G1-8: Use Essential 8 metrics under this policy to inform annual ASD Cyber Security Survey for Commonwealth Entities (Essential 8 Assessment) and annual PSPF Maturity Self-Assessment reporting.

Roles and Responsibilities

To deliver the outcomes described within this policy, there are several roles with accountability and responsibility to achieve the policy directions:

- **Business Owner** - The Senior Executive Service (SES) officer(s) accountable for the business functions an ICT system supports. At a high level, the Business Owner is accountable for identifying, communicating, and accepting business risks associated with the system.
- **Chief Information Security Officer (CISO)** – The Services Australia Chief Information Security Officer or their delegate. The CISO provides cyber security leadership and guidance for the agency and acts as an independent advisor and assurer for matters relating to cyber security.
- **Enterprise Architect –** The SES officer(s) responsible for developing and maintaining ICT architectural patterns, policies, principles, and frameworks for the agency.
- **Policy Owner** - Responsible for the development, implementation, and maintenance of the policy. They are responsible for ensuring that the policy is followed and that it remains up to date and relevant. The Policy Owner for this policy is the CISO.
- **System Manager** – The SES officer(s) responsible for the operation and management of a component system that is not an application (e.g. operating systems, network systems, databases), including (but not limited to) managing updates, ensuring system availability, monitoring performance and addressing technical issues that arise. The system manager is also responsible for the implementation and testing of controls in alignment with ICT policies.
- **System Owner** - The SES officer(s) responsible for the operation and management of an ICT application (component) system, and accountable for the oversight of the technology stack supporting the application. The System Owner is not responsible for the operation and management of other component systems (e.g. operating systems, network systems, databases). At a high level, the System Owner is accountable for selecting, implementing, and assessing controls to reduce cyber security risks to an acceptable level for Business Owners and monitoring the security and compliance of their system in line with ICT policies.

R	**Responsible:**	Agreed to complete task/activity
A	**Accountable:**	Authorise/accountable for completion
C	**Consulted:**	Persons who must be consulted/updated
I	**Informed:**	Must be informed after decision/action

Activity	System Owner/ System Manager	Business Owner	CISO	Enterprise Architect	Policy Owner
EL-D1-1: An agency endorsed cyber security event logging and monitoring framework must be established and maintained to support the identification of applicable logging requirements for systems.	C	-	R/A	I	-

Activity	System Owner/ System Manager	Business Owner	CISO	Enterprise Architect	Policy Owner
EL-D1-2: Architecturally endorsed log collection patterns are to be developed to support centralised logging.	I	-	C	R/A	-
EL-D1-3: The agency's cyber security logging capability (e.g. a Security Information and Event Management (SIEM) system) must include provisions for protecting stored logs from unauthorised modification and deletion.	-	-	R/A	-	-
EL-D1-4: Processes are implemented at the agency level to monitor cyber security event logs to detect cyber security events and incidents.	I	I	R/A	C	-
EL-D1- 5: Timeframes for cyber security event log detection and analysis are to be agreed upon in the Continuous Monitoring Plan (CMP).	R/A	C	C	-	-
EL-D1-6: New or significant enhanced ICT systems must include provisions for security event log collection, monitoring, and storage.	R/A	R	C	-	-
EL-D1-7: The logging capability for each system must capture event types, attributes and details commensurate with the assessed risk as agreed with the cyber security function and documented in the Continuous Monitoring Plan (CMP).	R/A	C	C	-	-
EL-D1-8: New or changed system monitoring requirements advised by the cyber security function must be implemented within agreed timeframes.	R/A	I	C	-	-

Activity	System Owner/ System Manager	Business Owner	CISO	Enterprise Architect	Policy Owner
EL-D1-9: System logging capability must include provisions for event log storage and retention, and protecting stored logs from unauthorised modification and deletion.	R/A	-	C	-	-
EL-D1-10: Implement mechanisms to enable extraction of log data from systems in an agreed format compatible with the agency's endorsed System Information and Event Management (SIEM) solution.	R/A	-	C	-	-
EL-D1-11: Cyber security event logs must be generated at the system level and made available to the agency's endorsed SIEM in alignment with endorsed architecture patterns and as agreed with the cyber security function.	R/A	-	C	-	-
EL-D1-12: Cyber security event logs must be ingested to the agency's endorsed SIEM as documented in the System Security Plan (SSP).	A	-	R	-	-
EL-D1-13: All event logs stored at the system level must be protected from unauthorised modification and deletion in accordance with Essential 8 Maturity Level 2 requirements.	R/A	I	C	-	-
EL-D1-14: All cyber security event logs stored at the agency level are protected from unauthorised modification and deletion in accordance with Essential 8 Maturity Level 2 requirements.	-	-	R/A	-	-

Activity	System Owner/ System Manager	Business Owner	CISO	Enterprise Architect	Policy Owner
EL-D1-15: All stored cyber security event logs (excluding those for Domain Name System (DNS) services and web proxies) at the agency level are retained for a minimum of seven years, or longer if required for investigation.	-	-	R/A	-	-
EL-D1-16: Stored cyber security event logs (at the agency level) for DNS services and web proxies are retained for a minimum of 18 months, or longer if required for investigation.	-	-	R/A	-	-
EL-D1-17: Event logs from internet-facing servers are analysed to detect cyber security events in accordance with Essential 8 Maturity Level 2 requirements.	-	-	R/A	-	-
EL-D1-18: Event logs from all systems excluding internet-facing servers are analysed to detect cyber security events in accordance timeframes agreed and documented in the Continuous Monitoring Plan (CMP).	-	-	R/A	-	-
EL-D2-1: Cyber security events are analysed at the agency level to identify cyber security incidents in accordance with Essential 8 Maturity Level 2 requirements.	-	-	R/A	-	-
AC-G1-1: Compliance with this policy must be assessed, documented, and reported to the policy owner using separate reports for each agency system on a periodic basis in alignment with the ICT Governance Framework.	R/A	-	R/A	-	-

Activity	System Owner/ System Manager	Business Owner	CISO	Enterprise Architect	Policy Owner
AC-G1-2: Review and update the policy as required at least every 18 months.	-	-	-	-	R/A
AC-G1-3: Ensure policy directions are in line with regulatory requirements and industry standards.	-	-	-	-	R/A
AC-G1-4: Report compliance and performance metrics to the Cyber Resilience Board (CRB) and any other boards on a quarterly basis or as required by ICT policy EDM01 Ensure Governance Framework Setting and Maintenance.	-	-	-	-	R/A
AC-G1-5: Identify broad non-compliance with specific policy directions to improve the policy.	-	-	-	-	R/A
AC-G1-6: Use feedback provided by stakeholders to improve the policy.	-	-	-	-	R/A
AC-G1-7: Ensure changes to the policy are approved by the Policy Owner and the CRB.	-	-	-	-	R/A
AC-G1-8: Use Essential 8 metrics under this policy to inform annual ASD Cyber Security Survey for Commonwealth Entities (Essential 8 Assessment) and annual PSPF Maturity Self-Assessment reporting.	-	-	-	-	R/A

Governance

Policy Management

This policy is managed in accordance with the directions set out in the Managing Policy Compliance section and directions provided by ICT policy EDM01 Ensure Governance Framework Setting and Maintenance.

Implementation and Compliance

This policy must be obtained from the Cyber Security Policy Repository to ensure that the most recently approved version of the policy is used.

The compliance status for this policy must be reported to the Cyber Security function to facilitate assurance reporting to the CRB.

System Owner metrics will focus on operational efficiency, performance, and security at the system level. System Owners are required to provide specific compliance reporting for each of their systems. This ensures transparency and accountability in reporting to the Policy Owner.

Policy Owner metrics will align to compliance and risk management, such as number of security incidents, compliance with regulatory standards, adherence to security policies, and evidence of compliance through audit logs and reports.

Compliance with this policy will be assessed by the CISO and reported to the CRB on a quarterly basis using the following target metrics:

Essential 8 Control Category	**System Owner or Cyber Security Function Metrics (to report to Policy Owner)**	**Policy Owner Metrics (to report to governance bodies)**	**Variables to Track**
Restricting Administrative Privileges and Multifactor Authentication	The system has effective controls for protecting logs from unauthorised modification and deletion (Yes/No) (System Owner)	Percentage of agency systems with effective controls for protecting logs from unauthorised modification and deletion.	• Time that ineffective controls have been in place for unauthorised log modification and deletion.
	Event logs from internet-facing servers are analysed by security/detection rules within agreed timeframes (Yes/No) (Cyber Security Function)	Percentage of internet-facing server event logs analysed using security/detection rules within agreed timeframes.	• Time from log generation to event analysis.
	Cyber security events are analysed within agreed timeframes to identify security incidents (Yes/No) (Cyber Security Function)	Percentage of cyber security events analysed within agreed timeframes to identify security incidents.	• Time from event detection to incident identification.
	The system's Continuous Monitoring Plan requirements for log storage and retention meets the retention requirements set out in the	Percentage of agency systems with ISM-compliant Continuous Monitoring Plans (CMPs).	• Specified retention period if different from ISM requirements.

	ISM. (Yes/No) (System Owner)		
	Cyber security event logs are stored and retained as agreed in the Continuous Monitoring Plan (CMP) (Yes/No) (System Owner)	Percentage of agency systems with logs retained for the time period agreed in the Continuous Monitoring Plan (CMP).	• Actual retention period if different from CMP requirements.

Glossary

Definition or Acronym	Description
Agreed timeframes	An agreed timeframe is considered based on whether an action is taken as soon as possible with the available resources in the agreed timeframes set out in the Continuous Monitoring Plan (CMP).
Cyber security event	A cyber security event is an occurrence of a system, service or network state indicating a possible breach of security policy, failure of safeguards or a previously unknown situation that may be relevant to security. This can include a user sending an email or a firewall blocking a connection attempt.
Cyber security incident	A cyber security incident is an unwanted or unexpected cyber security event, or a series of such events, that either has compromised business operations or has a significant probability of compromising business operations. This can include a violation or imminent threat of violation of computer security policies, system usage policies, or standard security practices.
Cyber Resilience Board (CRB)	The current name of the governance committee overseen by the CISO to manage cyber security related matters for the agency.
Data breach	A data breach occurs when personal information is accessed, mishandled, lost, disclosed, or destroyed without consent or legal authorisation.
Insider threat	An insider threat is a type of cyberattack originating from an individual who works for an organization or has authorized access to its networks or systems. An insider threat could be a current or former employee, consultant, board member, or business partner and could be intentional, unintentional, or malicious.
Malware	Malware or 'malicious software' describes software installed into a computer system to cause harm to computer systems or networks. This includes viruses, spyware, trojans, worms.
System	A related set of hardware, software and supporting infrastructure used for the processing, storage or communication of data and the governance framework in which it operates.
Unsecured network	An unsecured network refers to a wireless network that does not have any security measures to protect the data transmitted over it. These networks are vulnerable to various types of security threats potentially exposing sensitive browsing data.

Referenced Documents

Document
Continuous Monitoring Plan
Enterprise Risk Management Policy and Framework
Information Security Manual (external document)

Protected Security Policy Framework (external document)
System Authorisation Policy
System Security Plan

Document Control

Version Control

Version	Date	Author/Reviewer	Comments
V0.09	21/06/2024	Cyber Capabilities Branch	Initial Draft and consolidated feedback from NM
V0.10	1/07/2024	Cyber Capabilities Branch	For SRO Approval to Consult
V0.11	4/07/2024	NM Cyber Capabilities	SRO Review
V0.12	4/07/2024	Cyber Capabilities Branch	SRO review updates incorporated
V0.13	19/07/2024	Various Stakeholders	Consolidated from Security Branch, Integrated Cyber Risk Management Team and Veterans and Department of Social Services Systems Branch
V0.14	25/07/2024	Various Stakeholders	Incorporated further feedback from Cyber Operations Branch.
V0.15	25/07/2024	Sent for SRO review and approval	

Document Endorsement

Status	Endorsed
Issue Date	06/08/2024
Authority	Chief Information Security Officer (CISO)

servicesaustralia.gov.au

Australian Government
Services Australia

OFFICIAL

Cyber Security Policy

Acceptable Use of ICT Facilities

This policy describes Services Australia staff responsibilities for using the Information Communication Technologies (ICT) facilities. It provides authoritative information for both acceptable and unacceptable use of our agency ICT facilities.

Status:	Approved
Approved by:	Services Australia Chief Information Security Officer (CISO)
Dissemination limiting marking:	OFFICIAL
Version:	3.3
Electronically approved date:	28 September 2023
Initial issue date:	7 November 2016

Table of Contents

1. Authority

The Chief Executive Officer (CEO) for Services Australia (the agency) is the authority accountable to the minister and the government for the security of the agency [1]. Accordingly, the agency's Protective Security Control Plan [2] sets out our CEO's expectations for all staff (including contractors) to implement and adhere to the agency's security policies.

This policy forms part of the suite of cyber security policies created under the authority of the Chief Information Security Officer (CISO), and is a component of the agency's Information Security Management Framework (ISMF) [3]. Any exceptions to this policy must be approved by the CISO.

An employee found to have violated this policy may be subject to disciplinary action under the agency's Conduct and Behaviour Policy [4], up to and including possible termination of employment.

2. Introduction

Services Australia staff use our agency's Information Communication Technology (ICT) facilities – such as computer equipment, software, operating systems, storage media, email and messaging, and internet browsing - as required to carry out their day-to-day duties. Inappropriate use of our agency's ICT facilities can cause identity theft, fraud, theft of data, or make our systems vulnerable to targeted cyber intrusions. An important risk mitigation measure in this context is to outline the expected staff behaviour in using our agency's ICT facilities.

Users can contact the cyber security function [5] for any questions about acceptable use of ICT facilities.

3. Objectives

The objectives of this policy are to:

1. Define the accountabilities of managers responsible for promoting and maintaining effective cyber hygiene in day-to-day work of Services Australia staff.
2. Define rules for acceptable and unacceptable use of ICT facilities.

4. Terminology

The following table is sourced from the ISMF and defines the terms used to describe accountabilities and application of controls within cyber security policies.

When non-compliance with this policy is identified, staff must engage with the cyber security function [5] [6].

Term	Description
MUST	This word, or the terms 'REQUIRED' or 'SHALL', means that the definition is an absolute requirement of the specification.
MUST NOT	This phrase, or the phrase 'SHALL NOT', means that it is an absolute prohibition of the specification.
SHOULD	This word, or the adjective 'RECOMMENDED', means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
SHOULD NOT	This phrase, or the phrase 'NOT RECOMMENDED' means that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.
MAY	This word, or the adjective 'OPTIONAL', means that an item is truly optional.

5. Accountabilities

5.1 CISO

The Senior Executive Service (SES) officer responsible for this role acts as the final authority on:

1. Coordinating cyber security awareness for the acceptable use of ICT facilities.
2. Coordinating awareness training for cyber security best practice.
3. Coordinating availability and awareness of this policy for all users of the agency's ICT facilities.

Additionally, the CISO must:

4. Execute the authority to block, deactivate or render inoperable all unauthorised devices connecting to the agency network.
5. Provide advice to both Business and System Owners on cyber security best practices for the acceptable use of ICT facilities.

5.2 Business Owner

All Business Owners are responsible for ensuring and maintaining effective cyber hygiene through established practice within their business areas. The relevant Senior Executive Services (SES) officers responsible for managing business functions that require the use of ICT facilities must:

1. Ensure that staff are made aware of their responsibilities under this policy and undertake any corresponding training, including refresher training at least yearly.
2. Ensure internal processes are developed and communicated to their staff to remain compliant with relevant cyber security policies [7], [8], [9].
3. Ensure that staff are aware of the process for seeking certification and digital signing of all macros [10].
4. Ensure that staff are aware of the accepted file types and extensions used within the agency and that this information is updated when changes have been communicated.

5. Ensure that staff using the agency's email and messaging systems are aware of the risks associated with electronic communication, including the potential threat from suspicious emails [11], and how to report incidents [12]).
6. Ensure that staff are aware that by using the agency's ICT facilities, this use will be treated as consent to the monitoring and auditing of the use of the ICT facilities at all times.

5.3 System Owner

All System Owners are responsible for ensuring that ICT facilities are established and maintained in a manner which supports staff in maintaining cyber hygiene. The relevant SES officers must:

1. Ensure controls are implemented as outlined in the relevant cyber security policies [8], [7], [13].
2. Ensure that unacceptable use of ICT facilities is logged and reported to the appropriate authorities.
3. Ensure the effective and secure operation of the agency's ICT facilities at all times.

6. Background

To protect its systems the agency uses a defence-in-depth approach, which provides assurance that the consequences of a cyber intrusion are reduced, and the extent of malicious activity is contained effectively [14]. Since people are a critical factor in cyber security, this approach relies upon agency staff having requisite knowledge of their responsibilities to help protect the agency's ICT systems and information [1].

Maintaining the agency's cyber security posture is both an expectation of acceptable use and a business enabler. Acceptable use of ICT facilities includes incorporation of security measures identified as best practice within this and other supporting documents. The use of the agency's ICT facilities constitutes consent to the monitoring and auditing of the use of those facilities at all times. This monitoring can include the tracking of all communications and digital transactions within internal networks, and through external gateways including internet access.

7. All Users of ICT Facilities: Responsibilities

7.1 Acceptable Use

1. All staff must ensure that they are familiar with the agency's Acceptable Use of ICT Facilities Policy (this document).
2. Staff must ensure that basic security precautions are taken in day-to-day use, including:
    a. Shutting down computers and switching all monitors off at day's end, and as far as business requirements permit [15] [16].
    b. Locking workstations when leaving them unattended.
    c. Allowing timely updates and system patches as prompted.
    d. Seeking security advice where necessary from the cyber security function [5].
3. Staff must use a strong password and are responsible for all activities conducted using their authentication information as outlined in the User Access Control for ICT Systems Policy [17].
4. Staff must only install software and applications that have been formally approved by the agency, or in line with Whole of Government direction using the agency approved process [18]. Installation and use of applications including (but not limited to) TikTok, gambling or dating applications are not permitted.

5. In some cases, staff may receive approval to use an Unfiltered Internet Connection for specific capabilities. In those cases staff must only use those connections on isolated equipment (which must never be connected to the agency's network).
6. Staff must ensure that all agency information is stored on the agency's network with appropriate access permissions. When business needs require the storage or transfer of information outside the agency's network, staff must comply with the applicable cyber security policies and other relevant policies available on the intranet [19], [20], [21], [22], [23], [24], [8], [25], [26] [27], [28], [29], [30].
7. Staff must ensure that they only store limited amounts of personal information on agency networks, and that this information is for work purposes.
8. Staff must ensure that any use of social media is undertaken as outlined by the agency's social media policy [9].
9. Staff must have a demonstrated business need to use Microsoft Office macros.
10. Staff must ensure that they only save file types using the modern formats introduced since MS Office 2007 (excluding macro-enabled software) including but not limited to:
    a. .docx – Word Document.
    b. .xlsx – Excel Workbook.
    c. .pptx – PowerPoint Presentation.
11. Staff must only connect devices to the agency network that are:
    a. First assessed and approved by the infrastructure and the cyber security functions. [31] [32].
    b. Built according to the agency's approved process.
    c. Remotely managed by our agency.
12. All agency network devices, in particular portable devices, must be connected to the network within a 90 day period to receive the necessary security and software updates. Otherwise, devices may be locked and undergo integrity checks. Supervisors are to ensure that staff on leave for more than six weeks must return their devices [33].

7.2 Unacceptable Use

The following controls apply to examples of unacceptable use of ICT facilities:

1. Staff must not use the agency's ICT facilities in any way which:
    a. Contravenes Commonwealth, State or Territory law.
    b. Results in a breach of the APS Code of Conduct.
2. Staff must not use ICT facilities for:
    a. Distributing material that is harmful to the reputation of the agency, including forwarding such material to a user's personal email account.
    b. Distributing material that conflicts with the interests of the agency.
    c. Downloading any programs or executables without prior approval from the cyber security function [5].
    d. Intentionally accessing internet sites containing discriminatory, offensive, sexually oriented or other such unacceptable material.
    e. Creating, intentionally accessing, saving, possessing, soliciting or distributing any material that is discriminatory, offensive, sexually oriented or otherwise unacceptable.
    f. Intentionally spreading malicious software or code, such as viruses or Trojans.
    g. Installing, storing or disseminating any unacceptable images, videos or executable files.

h. Breaching intellectual property rights, including copyright on software.

i. Distributing communications or email that discloses personal information of another person without proper authorisation.

j. Distributing chain letters or other bulk email that is not authorised or work related (except for email distribution lists authorised by the agency).

k. Distributing email using a false identity.

l. Registering other users' agency email accounts or personal details without their permission.

3. Staff must not, in their use of ICT facilities, engage in behaviours or practices which involve:

   a. Altering, moving, dismantling or modifying settings of ICT equipment without proper authority.

   b. Attempting to remove, alter, manipulate or circumvent security processes associated with ICT facilities.

   c. Interfering with or intentionally disrupting the operation of ICT facilities.

   d. Gaining unauthorised access to any official information entered onto, stored on, distributed or transmitted using ICT facilities.

   e. Using ICT facilities for private commercial activities such as online gambling, online share trading, political activity or performing duties for another job.

   f. Connection of unapproved auto configuring devices [34] to agency ICT equipment (for example via serial, parallel, FireWire, USB, HDMI and wireless).

   g. Connecting ICT equipment via an unapproved internet connection.

   h. The 'Call-home-to-the-vendor' feature of any ICT equipment connected to the agency network must be configured to communicate through the agency network. The 'Call-home-to-the-vendor' feature must not bypass the agency's network or security controls. Call home features must be configured to obtain approval from the System Owner prior to initiating each remote access connection.

   i. Using ICT facilities to conduct business for 'not for profit' organisations, professional organisations or charities unless prior approval has been received.

   j. Accessing unapproved online file sharing, chat lines, blogs and web based 'friend' or social networking applications from work [35].

4. Staff must not engage in behaviour or practices which:

   a. Causes physical damage to systems.

   b. Bypasses, strains or tests security measures.

   c. Introduces or uses unauthorised ICT equipment or software on a system.

   d. Assumes the roles and privileges of others.

   e. Attempts to gain access to information for which they are not authorised.

   f. Relocate ICT equipment without proper authorisation and expressed permission of the system owner.

5. Staff must not use unsigned macros [10] [13] in any Microsoft program.

6. Staff must not use legacy (MS Office 97 or earlier) file types for any Microsoft program, including but not limited to:

   a. .doc – Legacy Word Document.

   b. .xls – Legacy Excel Workbook.

   c. .ppt – Legacy PowerPoint Presentation.

7. Unauthorised devices must not be connected to the agency network. Only devices that fulfil the criteria laid out in the Acceptable Use section are authorised devices. Any unauthorised devices that

connect or attempt to connect to the agency network will be blocked, may be deactivated or otherwise rendered inoperable, and may become damaged. Connecting or attempting to connect an unauthorised device to the agency network constitutes a breach of agency policy. A previously authorised device that has been reported as stolen, or has been altered or otherwise has had its software or hardware modified without the correct authority, is considered an unauthorised device.

8. Staff must not make alterations to the hardware configuration of their computer device (for example: RAM, Hard Disks, or internal expansion cards). Agency whitelisted peripherals (for example: Keyboard, Mouse, Monitors or Audio Devices) may be added/removed as required [34] [36].
9. Staff must ensure that they do not under any circumstances allow another individual to use their account, or themselves use the account of another individual.

7.3 Email and Messaging

1. Staff must ensure that email and messaging services are used securely as outlined by the Staff Email and Messaging Policy [7].
2. Staff must not use non-agency web-based email services using the agency's ICT facilities.
3. Staff must not forward or send any agency information to a a private email or messaging service (except for their own personal details, for example their payslip [21]).
4. Staff must not use the agency's email services to foster commercial interests or individual profit.
5. Staff must not forward chain emails, spam, large attachments or material likely to degrade the system and/or its performance. Staff must not search for, retrieve or email material that is offensive or may offend.
6. Staff must ensure that they do not open suspicious attachments or URLs.
7. Staff must ensure that they report spam and suspected spam [11].
8. Staff must ensure that they do not use peer-to-peer applications such as messaging platforms to communicate sensitive or security classified information [28] to external recipients.
9. In communicating with internal recipients, staff should not use peer-to-peer applications such as messaging platforms - including screen sharing - to communicate sensitive or security classified information [28] that may increase the risk of compromise to agency systems and/or information. Staff should use internal email as the preferred communication method.
10. Where business reasons dictate the necessity to transmit data via messaging platforms rather than email, the sender must ensure that the recipients have a business need and relevant security clearance to receive the information. This requirement is applicable to individual or group audiences who are participating in or facilitating screen-sharing sessions.
11. Staff must not use any agency issued email address as a credential on the internet without prior approval from their Line Manager.
12. Transfer of information from the Protected Enclave (PE) environment to Official/Official: Sensitive (Unclassified) environment is a controlled activity within the agency. Staff must obtain approval from an authorised officer to facilitate the transfer of appropriate, unclassified information from the PE environment [37].

Email and electronic messaging channels for communication are also potential channels to introduce threats into the agency's ICT environment through attachments, embedded links and malicious software. By following these controls and the controls outlined in the Staff Emailing and Messaging Policy [7], staff are able to use email with the assurance that they are compliant with best practice behaviours and processes.

7.4 Malicious Software and Viruses

1. Staff must ensure that they report the installation of malicious software and viruses to the cyber security function [5] as soon as they become aware of it.

2. Staff must ensure that they seek advice from the cyber security function [5] pending the rebuild of a compromised device.
3. Staff must ensure that compromised devices are disconnected (but not powered down) from the agency's network, pending advice from the cyber security function [5].
4. Staff must not engage in any action or inaction that could cause damage, destruction, alteration, loss or disclosure of information or that could cause a malicious cyber intrusion.
5. Staff must ensure that any suspicious activity, malicious code or perceived compromise to the agency's ICT facilities is reported promptly to cyber security function [5]

Staff are encouraged to report suspected instances of malicious software and viruses to the cyber security function [38] before engaging in a rebuild of their system. By reporting malicious software and viruses, mitigations can be implemented which reduce the vulnerability of agency systems.

7.5 Internet Usage

Internet browsing and visits to websites can easily expose a user to various risks of compromise, especially to sites that have unsecured connections. Doing so from an agency networked device therefore increases the vulnerability of agency systems. Accordingly staff are expected to exercise care in any use of workplace Internet access outside of business use.

1. Staff must ensure that, where possible, they avoid visiting websites which use an unsecured (http rather than https) connection.
2. Staff must not visit websites that have an invalid or out of date security certificate as identified by the web browser.
3. Staff must not attempt to enable or access sites that use Active Content (for example, Java or Flash).
4. Staff must limit their personal web browsing activities using work devices to a reasonable level.
5. Staff and users must not use agency ICT facilities and/or the Services Australia network in an attempt to conceal their IP address and/or install The Onion Router browser (TOR browser) or similar technology to gain access to the dark web.
6. Staff must not use their Virtual Desktop Infrastructure or any interface used for developmental, testing or administrative use (such as Servers, Jump Boxes/Servers, Sandboxes, etc.) as means to access the internet or connect to any network external to the agency network.
7. Staff should avoid visiting websites outside of acceptable use guidelines.
8. Staff should ensure that they avoid posting personal information that identifies them as a Services Australia employee on websites, as the information posted in the public domain may make staff the target of cyber-attacks.
9. Staff should ensure that they report to the cyber security function [5] any sites that are accessed that they suspect should be blocked as per the agency Internet Restriction Policy [35].
10. Our agency will inspect all external websites traffic, except those on the authorised exemption list (such as Australian banking websites).
11. Staff must not use their universal password (LAN password) to access services on the internet.

8. Related Policies

This policy is supported by the following policies:

1. Internet Restriction Policy [35]
2. Staff Email and Messaging Policy [7]
3. Use of Removable Storage Devices Directive [25]

4. User Access Control for ICT Systems Policy [17]
5. Staff Identity and Access Management Policy [39]

9. Australian Government Security Guidance

The Protective Security Policy Framework (PSPF) and Information Security Manual (ISM) provide the security controls relevant to this policy and must be applied by all staff in execution of their roles and responsibilities. Any questions regarding the policy and these security controls should be directed to the cyber security function [5].

9.1 Australian Government Protective Security Policy Framework (PSPF) requirements

The PSPF [1] outlines governance and information security requirements to manage cyber security risks, and to ensure the confidentiality, integrity and availability of the agency's information.

PSPF Control	Core Requirement Description Core requirements articulate what entities must do to achieve the government's desired protective security outcomes. It is the responsibility of each System Owner to ensure compliance with the relevant requirements.
GOVSEC 01 **Role of accountable authority**	The accountable authority is answerable to their minister and the government for the security of their entity. The accountable authority of each entity must: a. determine their entity's tolerance for security risks a. manage the security risks of their entity b. consider the implications their risk management decisions have for other entities, and share information on risks where appropriate The accountable authority of a lead security entity must: a. provide other entities with advice, guidance and services related to government security b. ensure that the security support it provides helps relevant entities achieve and maintain an acceptable level of security c. establish and document responsibilities and accountabilities for partnerships or security service arrangements with other entities.
GOVSEC 02 Management Structures and Responsibilities	The accountable authority is answerable to their minister and the government for the security of their entity. The accountable authority of each entity must: a. determine their entity's tolerance for security risks b. manage the security risks of their entity c. consider the implications their risk management decisions have for other entities, and share information on risks where appropriate The accountable authority of a lead security entity must: a. provide other entities with advice, guidance and services related to government security b. ensure that the security support it provides helps relevant entities achieve and maintain an acceptable level of security

	c. establish and document responsibilities and accountabilities for partnerships or security service arrangements with other entities.
INFOSEC 10 Safeguarding information from cyber threats	Each entity must mitigate common and emerging cyber threats by: a. implementing the following mitigation strategies from the Strategies to Mitigate Cyber Security Incidents: i. application control ii. patching applications iii. restricting administrative privileges iv. patching operating systems. b. Considering which of the remaining mitigation strategies from the Strategies to Mitigate Cyber Security Incidents you need to implement to protect your entity.

9.2 Australian Government Information Security Manual (ISM)

The ISM [40] controls are designed to protect the agency's systems and information from cyber threats and data loss. All staff must apply these controls in the execution of their roles and responsibilities.

ISM Control	Definition When writing this policy, the tabled controls were sourced from the most recently published ISM. System owners must use the latest ISM controls published by the Australian Cyber Security Centre (ACSC).
0252	Security Control: 0252; Revision: 6; Updated: Jun-20; Applicability: All Cyber security awareness training is undertaken annually by all personnel and covers: ▪ the purpose of the cyber security awareness training ▪ security appointments and contacts within the organisation ▪ authorised use of systems and their resources ▪ protection of systems and their resources ▪ reporting of cyber security incidents and suspected compromises of systems and their resources.
0462	Security Control: 0462; Revision: 6; Updated: Jun-21; Applicability: All When a user authenticates to encryption functionality for ICT equipment or media storing encrypted data, it is treated in accordance with its original sensitivity or classification until such a time that the user deauthenticates from the encryption functionality
0631	Security Control: 0631; Revision: 6; Updated: Jun-20; Applicability: All Gateways: ▪ are the only communications paths into and out of internal networks ▪ allow only explicitly authorised connections ▪ are managed via a secure path isolated from all connected networks (physically at the gateway or on a dedicated administration network) ▪ log all physical and logical access to their components ▪ are configured to save logs to a secure logging facility

ISM Control	Definition When writing this policy, the tabled controls were sourced from the most recently published ISM. System owners must use the latest ISM controls published by the Australian Cyber Security Centre (ACSC).
	▪ have all security controls tested to verify their effectiveness after any changes to their configuration
0817	Security Control: 0817; Revision: 4; Updated: Jan-20; Applicability: All Personnel are advised of what suspicious contact via online services is and how to report it.
0820	Security Control: 0820; Revision: 5; Updated: Jan-20; Applicability: All Personnel are advised to not post work information to unauthorised online services and to report cases where such information is posted.
0821	Security Control: 0821; Revision: 3; Updated: Oct-19; Applicability: All Personnel are advised of security risks associated with posting personal information to online services and are encouraged to use any available privacy settings to restrict who can view such information.
0824	Control: 0824; Revision: 2; Updated: Sep-18; Applicability: All Personnel are advised not to send or receive files via unauthorised online services.
0869	Security Control: 0869; Revision: 5; Updated: Dec-21; Applicability: All Mobile devices encrypt their internal storage and any removable media.
1146	Control: 1146; Revision: 2; Updated: Sep-18; Applicability: All Personnel are advised to maintain separate work and personal accounts for online services.
1284	Security Control: 1284; Revision: 2; Updated: Oct-19; Applicability: All Content validation is performed on all data passing through a content filter with content which fails content validation blocked.
1286	Security Control: 1286; Revision: 1; Updated: Sep-18; Applicability: All Content conversion is performed for all ingress or egress data transiting a security domain boundary.
1289	Control: 1289; Revision: 1; Updated: Sep-18; Applicability: All The contents from archive/container files are extracted and subjected to content filter checks.
1290	Control: 1290; Revision: 1; Updated: Sep-18; Applicability: All Controlled inspection of archive/container files is performed to ensure that content filter performance or availability is not adversely affected.
1291	Control: 1291; Revision: 1; Updated: Sep-18; Applicability: All Files that cannot be inspected are blocked and generate an alert or notification.
1293	Security Control: 1293; Revision: 1; Updated: Sep-18; Applicability: All All encrypted content, traffic and data is decrypted and inspected to allow content filtering.
1671	Control: ISM-1671; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3 Microsoft Office macros are disabled for users that do not have a demonstrated business requirement.

10. References

[1] Protective Security Policy Framework (PSPF), available externally, Protective Security Policy Framework website, Attorney-General's Department.

[2] Agency's Protective Security Control Plan, available internally Services Australia Intranet, Security policies page.

[3] Information Security Management Framework (ISMF), available internally, Services Australia intranet, Cyber security policies page.

[4] Conduct and Behaviour Policy, Available internally, Services Australia Intranet, Ethics - What is expected of me page.

[5] To contact the cyber security function, s47E(d) .

[6] Users can email s47E(d) @servicesaustralia.gov.au for any enquiries related to this policy.

[7] Staff Email and Messaging Policy, available internally, Services Australia intranet, Cyber security policies page.

[8] Mobile Computing and Use of Mobile Devices Policy, available internally, Services Australia intranet, Cyber security policies page.

[9] Services Australia Social Media Policy for Staff, Available internally, Services Australia intranet.

[10] s47E(d) Article: Digital Signing of Microsoft Office Macros, Available internally on s47E(d) application.

[11] s47E(d) t Article: What to do when you receive spam or phishing emails, available internally on s47E(d) application.

[12] s47E(d) Article: Report a Cyber Security Incident, available internally on the s47E(d) application.

[13] Windows Standard Operating Environment (SOE) Policy, available internally, Services Australia intranet, cyber security policies page.

[14] T. Schreider, Building Effective Cybersecurity Programs: A Security Manager's Handbook, Brookfield: Rothstein, 2017, chapter 5.

[15] Services Australia Enviromental Sustainability Policy, section 3.4 (agency officials responsibilites and actions), Available internally, Services Australia Intranet, 2014.

[16] For detailled figures & business advice see "Energy consumption at work: leaving your Monitors on costs money", Available Externally, online media May 2018.

[17] User Access Control for ICT Systems, available internally, Services Australia intranet, Cyber security policies page.

[18] s47E(d) s47E(d) .

[19] External Electronic Data Exchange Policy and Standard, Available internally, Services Australia Intranet, Cyber security policies page.

[20] Data Aggregation Policy, available internally, Services Australia intranet, cyber security policies page.

[21] Staff Personal details, Available internally, Services Australia Intranet.

[22] Control of Customer Information Outside Core Systems Policy, Available Internally, Services Australia intranet, go to s47E(d)

[23] Data Loss Prevention Policy, available internally, Services Australia intranet, cyber security policies page.

[24] Foreign Government Information Exchange and Storage Policy, Available internally, Services Australia Intranet, Cyber Security Policy page.

[25] Use of Removable Storage Devices Policy, Available internally, Services Australia Intranet, Cyber security policies page.

[26] Information Security intranet page, see the security hub on the Services Australia intranet.

[27] Customer Information Exchange Policy Statement, available internally, Services Australia intranet.

[28] Services Australia Information Security Policy, available internally, Services Australia intranet.

[29] ICT Asset and Media Sanitisation Policy, available internally, Services Australia intranet, cyber security policies page.

[30] Services Australia Cloud Policy, s47E(d)

[31] Refer to s47E(d) article: ICT Hardware Asset Request and Asset Return, s47E(d)

[32] submit a Non-standard ICT asset form, s47E(d)

[33] Asset Management Policy and Procedures Guide, available internally, Services Australia Intranet, Asset Policy and Guidance page.

[34] s47E(d) Article: Use of external devices - Cyber security requirements, s47E(d)

[35] Internet Restriction Policy, available internally, Services Australia intranet, Cyber security policies page.

[36] Ergonomic Equipment Guidelines, available internally, Services Australia Intranet, HR Policy Hub.

[37] Protected Enclave Policy, available internally, Services Australia intranet, cyber security policies page.

[38] Report a cyber security event or incident, available internally, Services Australia Intranet, Cyber Central Page.

[39] Staff Identity and Access Management Policy, available internally, Services Australia intranet, Cyber security policies page.

[40] Australian Government Information Security Manual (ISM), Available Externally, the Australian Signals Directorate's Australian Cyber Security Centre (ACSC) website.

[41] Cyber Security Governance Framework, Available internally Services Australia intranet, Cyber Central page.

11. Glossary of Terms

Definition or Acronym	Description
ACSC	Australian Cyber Security Centre
Agency	Services Australia is used in the first instance, and then refer as, 'the agency' (use lower case 'a') and personal pronouns 'we', 'our', 'us' thereafter.
Agency System	Information technology components, including software that processes data, which is owned and operated by Services Australia
Business Owner	The Business Owner is the agency's Senior Executive Service (SES) Officer who is accountable for the operation of a specific section of the Services Australia enterprise.
CISO	Chief Information Security Officer
Cyber Hygiene	Cyber hygiene refers to best practice and other activities that computer system users can undertake to improve their cybersecurity while engaging in common online activities, such as web browsing, emailing, texting, and so on.
Cyber security function	Within this document 'cyber security function' refers to either: the agency entity with primary responsibility for management and delivery of cyber security outcomes; or the activities themselves that constitute said management and delivery.
Defence-in-depth	An organisation's defence against cyber-attacks is designed in as many different layers as possible. Each layer consists of a technical or procedural method to defend the organisation; the idea is that if a single layer fails, the others take over.
Discriminatory Material	Material including any images, text or data which, if displayed in the workplace, would be unlawful according to the following legislation: Public Service Act 1999 Disability Discrimination Act 1992 Racial Discrimination Act 1975 Sex Discrimination Act 1984
ICT	Information Communication Technologies
ICT Assurance	The overall effort taken by the agency to ensure the availability, authentication, confidentiality, integrity, and non-repudiation of its sensitive data, information and ICT facilities
ICT Facilities	Information and communications technology facilities include; hardware and software that support the processing and communication of information and data that is owned, leased, managed, or operated by Services Australia or supplied by an external service provider for Services Australia use
ISM	Information Security Manual. The standard which governs the security of government ICT systems. Authored by Australian Signals Directorate (ASD)

ISMF	Information Security Management Framework. The standard which outlines how the agency complies with existing whole-of-government best practice as outlined within the Protective Security Policy Framework (PSPF)
Messaging platforms	Messaging platforms include (but are not limited to): Microsoft Teams, Skype for Business.
Offensive Material	Material including images, text, data or other material that: Offends community standards and includes images, data or other material that is humiliating, vulgar, discriminatory or racially biased against any person or group of persons Portrays violence, injuries or death of a person, people or animals or gratuitous destruction of property
PSPF	Protective Security Policy Framework
Security classified information	Information that has been classified as PROTECTED, SECRET or TOP SECRET [28].
Sensitive Information	Information that has been classified as OFFICIAL: Sensitive [28].
Sexually Orientated Material	Sexually oriented material including multimedia, images, text or data whose main focus is pornography. Pornography may include person/s engaged in sexual acts or images of partial or full nudity
Staff	Services Australia staff/employee of the agency, including contracted staff who have access to our agency ICT systems and applications (also see “user”).
System Owner	The system owner is the SES officer responsible for the secure operation of an information resource. See Roles and Responsibilities in Related Documentation
Unacceptable Material	Material including any images, text or data that: is offensive and/or sexually orientated material concerns terrorism, espionage, bomb or incendiary device making, theft or illegal drug use or similar material is defamatory, abusive, or likely to promote hatred or incite violence is harmful to Australia’s national interests or national security may harass, intimidate, threaten or offend another person.
User	Internal and external individuals, and foreign nationals, that have access to the agency’s ICT systems.
Mobile Device	Mobile phone / iOS or Android tablet device.
Portable Device	x86 portable laptop or workstation (running full desktop Windows, Linux or MacOS).

Australian Government
Services Australia

Business Integrity s47E(d) high level monitoring usage protocol

Summary

This document describes in detail the process Internal Fraud Directors will be required to follow to activate Dtex high level monitoring (screen and keystroke capture). The intent of this protocol is to provide a mechanism for using the advanced features of s47E(d) for fraud intelligence and investigation, whilst balancing the agency's need to adhere to Australian Privacy Principles.

Requirements to activate high level monitoring

For Dtex high level monitoring to be activated, Internal Fraud Directors must form a reasonable suspicion that fraudulent or highly inappropriate staff behaviour may be occurring. In addition, there needs to be a reasonable belief that the s47E(d) information gathered by high level monitoring may add value to the relevant intelligence case or investigation.

Administration of high level monitoring activation

In order for high level monitoring to be activated, an Internal Fraud Director must decide and document that;

1. the additional information collected by s47E(d) is relevant to the intelligence case or investigation
2. that the Australian Privacy Principles have been considered and the additional collection of information adheres to these principles

Internal Fraud Directors are defined as:

Director, Predictive Analytics and Fraud Detection

Director, Internal Fraud Intelligence

Director, Internal Investigations

s47E(d)

In all circumstances, the National Manager of Taskforce Integrity and Fraud Investigation and the other two Internal Fraud Director must be notified in writing within a reasonable timeframe.

Retention of Data

If during the course of intelligence analysis or during an investigation, the s47E(d) high level monitoring information is found to be not required for the case, this high-level monitoring data must be deleted as soon a reasonably possible.

Approved by:
General Manager, Business Integrity Division
Services Australia
XX/12/2020