



Information Security

INFOSEC-3:

Robust technology and information systems



Contents

About this document	3
Definitions and shortened terms	5
Context	9
Guidance	11
Introduction	11
Required action: Apply Tasmanian Government cyber security principles	13
Required action: Manage information on authorised systems	14
Required action: Ensure processes for audit trails and activity logging	16
Required action: Develop and test a business continuity plan	17
Required action: Own and be accountable for security risk in ICT systems	19
Required action: Ensure effective physical controls and secure zones	20
Required action: Consider supply chain security	21
References and resources	27

Author: Resilience and Recovery Tasmania
Publisher: Department of Premier and Cabinet
Date: April 2023

© Crown in Right of the State of Tasmania April 2023

About this document

This document – INFOSEC-3: Robust technology and information systems – is part of a suite of policies and guidance developed to assist Tasmanian Government agencies to meet requirements under Tasmania's Protective Security Policy Framework (TAS-PSPF).

The TAS-PSPF is a whole-of-government approach to the protection of Tasmanian Government information, people and assets from compromise and harm. It establishes minimum protective security standards and makes clear that to continue ensuring the security of our people and assets, Tasmanian Government agencies need to:

- understand the security environment in which they operate
- identify and understand the most critical assets they must protect
- mitigate security vulnerabilities on a prioritised security-risk basis
- anticipate and prepare for emerging security trends which threaten their ability to effectively undertake government business functions
- continue to improve protective security practices through accountability and governance.

The TAS-PSF sets out 14 core requirements – with each accompanied by supplementary requirements – that define what must be addressed in order to protect our information, people and assets.

The suite of policies and guidance, including those found in this document, ensures that the TAS-PSPF will be applied across Tasmanian Government agencies in a consistent way. It will also assist agencies to achieve the expected outcomes of the following protective security domains under the TAS-PSPF:

- security governance
- information security
- people security
- physical security.

The table below lists all 14 core requirements of the TAS-PSPF and their corresponding policies. The name of the policy and guidance provided in this document is [highlighted](#).

Protective security outcome	Core requirement	Relevant policies and guidance
Security governance	1	GOVSEC-1: Establish security governance
	2	GOVSEC-2: Security advice and responsibilities
	3	GOVSEC-3: Security awareness
	4	GOVSEC-4: Annual reporting
	5	GOVSEC-5: Security planning
	6	GOVSEC-6: Reporting incidents and security investigations
Information security	7	INFOSEC-1: Access to, and management of, official information
	8	INFOSEC-2: Protecting official information
	9	INFOSEC-3: Robust technology and information systems
People security	10	PESEC-1: Recruiting the right people
	11	PESEC-2: Ongoing suitability assessment
	12	PESEC-3: Managing separating people
Physical security	13	PHYSEC-1: Protecting assets
	14	PHYSEC-2: Agency facilities

Definitions and shortened terms

Guiding term	What this means in the context of the TAS-PSPF
must/will/required/responsible for	Any of these terms refer to an essential action that all agencies and Accountable Authorities must take.
must not	This term refers to an action that is prohibited – agencies and Accountable Authorities must NOT take this action.
should/recommended	Either of these terms refer to an action that agencies and Accountable Authorities ought to take as best practice, unless justifiable circumstances exist.
should not	This term refers to an action that agencies and Accountable Authorities ought to avoid, unless justifiable circumstances prevent an alternative action.
may	This term refers to an action that is optional to agencies and Accountable Authorities.

Term	What this means in the context of the TAS-PSPF
Accountable Authority/ies	The person or people responsible for, and with control over, a Tasmanian Government public authority. This includes, but is not limited to, agencies (as defined in the <i>State Service Act 2000</i>), administrative units, bodies corporate, statutory authorities, and instrumentalities of the Crown.
agency/ies	A Tasmanian Government agency/department or sub-entity.
Agency Security Advisor	Person/people nominated to perform security functions or specialist services related to security within an agency. This role supports the Accountable Authority in security monitoring and compliance.
ASIO Outreach	ASIO's public-facing website, which provides advice to government, industry and academia on current and emerging security threats and security policy, available by subscription.
asset	An agency's people, information, and physical items, including ICT systems, technology and information infrastructure.
availability	Ensuring that authorised users have access to information and associated assets when required.
classification	A process that determines and stipulates the extent of protection required to prevent information from compromise and harm.

Term	What this means in the context of the TAS-PSPF
compromise	May include exposure to loss and unintended or unauthorised access, misuse, information disclosure and intrusion of business activities and information. Compromise is a risk and hindrance to business delivery, safety and security.
confidentiality	Ensuring that information is accessible only to those authorised to have access and a 'need to know'.
consequence	The outcome, or expected outcome, of any compromise of information or a security incident.
contractor	External or third party contracted to provide services to an agency. For the purpose of the TAS-PSPF, contractor includes sub-contractor and service provider.
core requirement	A requirement that agencies must meet to achieve the government's desired protective security outcomes. Each of the 14 TAS-PSPF policies includes a core requirement (as well as supplementary requirements).
employees	All people conducting work on an agency premises, including contractors. See also, people.
function	The purpose or role of an agency.
handling	Any processes for accessing, transmitting, transferring, storing or disposing of protected information.
integrity	Safeguarding the accuracy and completeness of information and processing methods, i.e. information has been created, modified or deleted by the intended authorised means and is correct and valid.
official information	All Tasmanian Government documents, intellectual property and information that is held, transmitted or obtained by an agency.
originator	The instigating individual (or agency) responsible for producing information.
outcomes	The protective security 'end-state' aims of the Tasmanian Government relating to 4 security domains: governance, information, people and physical.
people	Employees and contractors, including secondees and any service providers that an agency engages. It also includes anyone who is given access to Tasmanian Government assets.

Term	What this means in the context of the TAS-PSPF
principles	<p>Fundamental values that guide decision-making. There are 5 principles that inform protective security settings in the TAS-PSPF.</p> <ol style="list-style-type: none"> 1. Security is a responsibility of government, its agencies and its people. 2. Each agency is accountable and owns its security risks. 3. Security will be guided by a risk management approach. 4. Strong governance ensures protective security is reflected in agency planning. 5. A positive security culture is critical.
protected information	Information which has been assessed and classified as requiring protective markings and protection.
protection	The processes and procedures applied to ensure the confidentiality, integrity and availability of information and assets.
protective marking	The level of classification applied to information, and any other handling instructions or protections the information requires due to the level of harm should it be compromised.
PSPF maturity rating	The level to which an agency has addressed and implemented the core and supplementary requirements in the TAS-PSPF.
risk appetite	The risk an agency or Accountable Authority is willing to accept.
risk tolerance	The level of risk an agency is comfortable taking after risk treatments have been applied to achieve an objective or manage a security risk.
security culture	The characteristics, attitudes and habits within an organisation that establish and maintain security.
security incident	<p>A security incident is:</p> <ul style="list-style-type: none"> • an action, whether deliberate, reckless, negligent or accidental, that fails to meet protective security requirements or agency-specific protective security practices and procedures which results, or may result in, the loss, damage, corruption or disclosure of information or assets • an approach from anybody seeking unauthorised access to protected assets • an observable occurrence or event (including natural or man-made events) that could harm Tasmanian Government information, people or assets.
security maturity	The measure of an agency's ability to manage their security risks within their risk environment and aligned to their risk tolerances.

Term	What this means in the context of the TAS-PSPF
security plan	Central document detailing how an agency plans to manage and address their security risks.
security risk	Something that could result in compromise, loss, unavailability or damage to information or assets, or cause harm to people.
security risk management	Managing risks related to an agency's information, people and assets.
security vetting	An authorised vetting agency's assessment of a clearance subject's suitability to hold a security clearance.
sensitive	Information classified as sensitive is not protected information; however, this information requires some protections on a 'needs to know' basis.
supplementary requirements	The actions needed to implement the TAS-PSPF core requirements and attain the government's desired protective security outcomes. Each of the 14 core requirements includes supplementary requirements to help implement the TAS-PSPF.
threat	The intent and capability of an adversary.
threat actor/adversary	An entity that is partially or wholly responsible for an incident that impacts – or has the potential to impact – an agency's security.
visitor	Any person who attends an agency and/or has access to its assets, who is not employed or otherwise engaged by that agency.
vetting	The evaluation of a person's suitability to obtain and maintain a security clearance and access sensitive and protected assets.
zone	The physical locality, workspaces, and design of areas within an agency that store assets and information, specifically where information is produced, accessed, handled and stored. Security zoned areas range from 1-5, where the security requirements increase with the applicable zone number allocation.

Acronym/abbreviation	Meaning
ASA	Agency Security Advisor
IRAP	Infosec Registered Assessors Program
RE	Responsible Executive

Context

The **INFOSEC-3: Robust technology and information systems** policy and guidance will assist agencies to achieve an effective protective security outcome within the information security domain of the TAS-PSPF. They address core requirement 9 and its supplementary requirements.

Core requirement 9

The Accountable Authority must ensure the security of technology and information assets to safeguard data, information and privacy, and to ensure continuous delivery of government business during all stages of the asset life cycle.

Supplementary requirements

To achieve this, the Accountable Authority will:

- a) ensure application of the Tasmanian Government Cyber Security Policy cyber security principles providing safeguarded maintenance of the confidentiality, integrity and availability of information¹
- b) only process, store or communicate information on ICT systems that the Accountable Authority has authorised to operate, based on acceptance of residual security risk associated with its operation
- c) ensure ICT systems incorporate processes for audit trails and activity logging in applications to ensure the accuracy and integrity of data captured or held
- d) develop and regularly test a Business Continuity Plan to manage the assessed risks and business impact associated with loss of critical information, personnel, facilities and ICT infrastructure
- e) ensure ownership of, and accountability for, information security risk in ICT systems, including cloud and outsourced services, by nominating a business risk owner for every system, who is responsible for ensuring the secure operation of their system.²

¹For access to the Tasmanian Government Cyber Security Policy – cybersecurity principles, refer to www.dpac.tas.gov.au/_data/assets/pdf_file/0024/103839/Tasmanian_Government_Cybersecurity_Policy.pdf

² The business risk owner may be the same for various (or all) systems.

- f) in combination with the *'People Core Requirements'*, ensure the effectiveness of physical controls and application of secure zones at any location where storage of information (in any form) is performed.
- g) ensure consideration of supply chain security is applied at all stages of contracted supply.

Access to information, particularly protected information, requires access controls to ensure that confidentiality and the integrity of Tasmanian Government information, assets and business operations are maintained. As the business operations and environment of each agency vary, levels of access and associated controls will be based on agency-specific security planning and risk assessments.

Limiting unintended or unauthorised access to protectively marked information relies on robust and validated technology, information and infrastructure systems, complemented by enhanced security governance.



Guidance

Introduction

The Tasmanian Government owns, manages and delivers various technology and information infrastructure, services and systems on behalf of the Tasmanian community in order to process, store and communicate information. Protecting these systems strengthens community confidence and supports secure and continuous delivery of Tasmanian Government operations and services.

Robust technology and information systems help your agency to:

- maintain the trust and confidence of the public, clients and partners
- keep agency information safe and available to those who need it
- reduce the risks of your agency's information being lost, damaged, or compromised
- avoid the costs of recovery after an incident, as well as costs of downtime and lost productivity
- comply with regulation and legislation.

An ICT system is the related set of hardware and software used to process, store or communicate information and data, and the governance framework in which it operates.

This policy (INFOSEC-3) requires your agency to ensure the security of technology and information assets that you operate or outsource during all stages of the asset life cycle.

The phases of an ICT system's life cycle are outlined in the following table.

Phase	Detail
Define	<ul style="list-style-type: none">• Determine the type, value and objectives for your ICT system and the information it processes, stores or communicates based on the business impact of loss or compromise.
Design	<ul style="list-style-type: none">• Assess the risks to your information and supporting ICT systems within your network.• Adopt suitable security controls which are proportionate to the identified risks and in line with your agency's risk appetite.• Your agency's Responsible Executive (RE) must assess the proposed security controls for appropriateness and then accept the security design, if deemed fit-for-purpose. Should the security controls not be accepted, further risk reduction must be considered and adopted in the design.
Implement	<ul style="list-style-type: none">• Implement the agreed security controls for the system and its operating environment, including supporting policies and procedures.
Assess	<ul style="list-style-type: none">• Evaluate your security controls for the system and its operating environment.• Certify – the Chief Information Officer³ accepts that due diligence and consideration has been given to risk, security, functionality and business requirements.
Authorise	<ul style="list-style-type: none">• Authorise – the RE gives approval for the system to operate based on the acceptance of the residual security risks.• System goes live.• Maintain and ensure that the security controls for your operating environment are up-to-date. Remaining secure is crucial and requires ongoing activity to stay up-to-date with evolving security environments, threats, vulnerabilities and mitigations.
Monitor	<ul style="list-style-type: none">• Undertake regular reviews to ensure your security controls remain fit-for-purpose.• Identify changes in your information use, your agency or the threat environment.• Use this information to inform improvements and return to the Define or Design phase where significant improvements are necessary.

³ Or appropriate delegate, in the absence of a Chief Information Officer.

Decommission	<ul style="list-style-type: none"> Archive, destroy, repurpose or dispose of information and supporting ICT systems in an appropriately secure way when they are no longer required.
---------------------	---

Table I – ICT system life cycle⁴

The Tasmanian Government relies on its ICT systems to protect information and data from compromise and ensure the secure and continuous delivery of its operations and services.

By considering and managing security risks during all stages of the system life cycle, you improve both the trustworthiness and resilience of these systems and their associated components.

Required action: Apply Tasmanian Government cyber security principles

The Tasmanian Government Cyber Security Policy⁵ is the one of the principal documents of the Tasmanian Government Information Management Framework.⁶ It provides a consistent, risk-based approach to protecting Tasmanian Government information, systems and services from cyber security threats.

The Tasmanian Government Cyber Security Policy is based on the following principles.

Awareness	Increased cyber security awareness enables staff at all levels to understand their responsibilities and identify and respond to cyber security risks.
Collaboration	Sharing cyber security knowledge across government improves cyber security capability and maturity.
Enablement	Cyber security is a key enabler for digital transformation.
Integration	Integrating cyber security into business risk management frameworks, policies and procedures improves planning for, and responses to, cyber security incidents.

⁴ For further information, please refer to Figure I in the Australian Government Protective Security Policy Framework policy 11: Robust ICT systems, available at www.protectivesecurity.gov.au/sites/default/files/2020-09/Policy11-Robust_ICT_systems-2018.3.DOCX#:~:text=This%20policy%20describes%20how%20entities,entities%20process%2C%20store%20and%20communicate

⁵ For access to the Tasmanian Government Cyber Security Policy, go to www.dpac.tas.gov.au/_data/assets/pdf_file/0023/254912/Tasmanian-Government-Cyber-Security-Policy-V1.1.pdf

⁶ The Tasmanian Government Information Management Framework is available on the website of the Office of the State Archivist at www.informationstrategy.tas.gov.au/Government-Information-Strategy

Privacy and security	Integrating cyber security into all digital systems and services improves privacy and security for consumers of Government services.
Risk	Adopting a risk-based approach allows the Tasmanian Government to adapt its cyber security risk management approach based on its risk tolerance.
Standards	<p>Aligning with national and international industry and Tasmanian Government standards provides a consistent, systematic and repeatable approach enabling collaboration across government and the private sector.</p> <p>Applicable international standards are:</p> <ul style="list-style-type: none"> • AS ISO/IEC 27001 for cyber security management requirements • AS/NZS ISO 31000 and AS/NZS ISO/IEC 27005 for risk management.

Table 2 – Tasmanian Government Cyber Security Policy Principles

Considering and applying the Tasmanian Government's principles will assist you as you work to safeguard your agency's ICT systems from cyber security threats.

For more information and guidance on how the Tasmanian Government Cyber Security Policy applies to your agency, contact your Agency Security Advisor (ASA).

Required action: Manage information on authorised systems

This policy (INFOSEC-3) requires each agency to authorise the ICT systems, making sure that an appropriate level of security is applied and that the relevant authority has considered and accepted residual security risks.⁷ Authorisation helps in providing confidence that your agency's ICT system/s meet security requirements, address known security vulnerabilities, and remain secure. For more information about the authorisation of ICT systems, please refer to Annexure I.

It is important to understand the operating environment of your agency's ICT system/s, as risks of compromise to a system or systems increase where the operating environment is complex.

The interconnection of ICT systems creates a potential path for adversaries to target the system/s via third parties, particularly where other systems are external and outside of your agency's control, for example, another agency's ICT system or industry partners' systems. For this reason,

⁷ Where identified necessary, an impartial (and in some cases, independent) security assessment can be a valuable tool in authorisation decisions.



as part of your security assessment and authorisation process, it's important to consider security risks and security protection required between the systems. This includes making sure that before any interconnection takes place, information about security risks is shared to ensure that any shared security risks are accepted by all parties.

It is a requirement that your agency's ICT system/s be authorised to the highest assessed sensitivity or security-classified information and data it will process, store or communicate. Authorisation to operate is usually ongoing; however, during the life cycle of an ICT system, it is a requirement to review that system (as described above in Table 1 – ICT system life cycle).

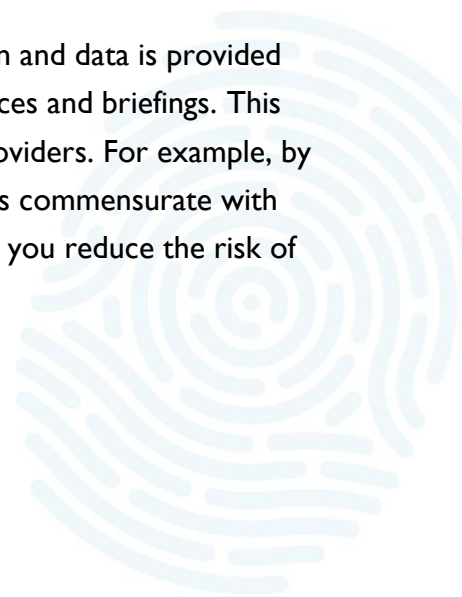
Any review may require a reassessment of the system, including its capacity to continue operation, or it may be approaching time for decommissioning. Examples of events that may trigger additional risk management activities for an ICT system include:

- changes in security policies relating to the system
- detection of new or emerging cyber threats to the system or its operating environment
- the discovery that security controls for the system are not as effective as planned
- a cyber security incident involving the system
- major architectural changes to the system.

Outsourced managed services and cloud services

Your agency's obligation to protect information doesn't stop at its internal system/s. You are also obliged to protect any Tasmanian Government information and data which is processed, stored or communicated via outsourced managed service providers and/or cloud service providers. You can achieve this by applying the same authorisation process you apply to internal systems.

You must ensure that access to sensitive and security-classified information and data is provided on a 'need to know' basis, in accordance with appropriate security clearances and briefings. This includes the use of any outsourced managed services and cloud service providers. For example, by using a service provider whose employees hold national security clearances commensurate with the information and data you require them to store, process and transmit, you reduce the risk of compromise from unauthorised access and inappropriate handling.



Required action: Ensure processes for audit trails and activity logging

Your agency must ensure ICT systems incorporate an audit trail and activity logging in applications. Putting measures in place to monitor the accuracy and integrity of information and data captured or held will help you to respond to incidents and to detect unusual, unauthorised or malicious activity.


The Tasmanian Government has a suite of Cyber Security Standards, which support the Tasmanian Government Cyber Security Policy.⁸ These standards are applicable to all Tasmanian Government agencies and do include some audit and access requirements. Applying these requirements increases the likelihood of detection and appropriate response to any unusual, unauthorised or malicious activity.

The following requirements are taken from the suite of standards:

- Any action taken to create, delete, remove or update a user account is logged for auditing purposes and the logs are maintained in accordance with the agency disposal schedules⁹
 - A record is to be maintained that contains the approvals to perform the logged actions.
- Audit logs are maintained in accordance with agency disposal schedule for all system or application authentication.
 - Logs are to include successful and unsuccessful authentications.
- Additions, modifications or removals of privileged and highly privileged accounts and/or the associated permissions are to be reviewed monthly.
- Anonymous access to systems is to be logged and the following access information logged at a minimum:
 - information accessed
 - time and date of access
 - connection source of access.

⁸ For further information, please visit the Department of Premier and Cabinet website at www.dpac.tas.gov.au/divisions/digital_strategy_and_services/cybersecurity#:~:text=The%20Tasmanian%20Government%27s%20Cybersecurity%20Policy%20%282018%29%20provides%20a,of%20cybersecurity%20standards%20to%20improve%20agencies%27%20baseline%20security.

⁹ For further information, please refer to TAS-PSPF policy: Protecting official information (INFOSEC-2).



The Australian Government Information Security Manual includes Guidelines for System Monitoring¹⁰ which detail the process for event logging and monitoring. According to these guidelines, when you are determining the audit and activity logging capacity of your agency's ICT systems, you should consider the details of events to be logged, event logging facilities to be used, how event logs will be monitored and how long to retain event logs. Doing this will also assist you when you're developing policy/ies regarding auditing and activity logging.

The Australian Government Information Security Manual also includes Guidelines for System Hardening¹¹ which suggest that you log the following events:

- application and operating system crashes and error messages
- changes to security policies and system configurations
- successful user logons and logoffs, failed user logons and account lockouts
- failures, restarts and changes to important processes and services
- requests to access internet resources
- security product-related events
- system startups and shutdowns.

Logging these details of operating systems will add an additional layer to your agency's ability to monitor and understand activities within your ICT system/s. You should record all of your monitoring and auditing activities and store these details in a centrally available location to increase the visibility and identification of events which might trigger investigation.

Required action: Develop and test a business continuity plan

You can enhance your agency's resilience and strengthen your security measures with a business continuity plan. Business continuity is the ability of your agency to continue delivering services at acceptable operating levels in the event of a security incident or other disruption to your agency.

¹⁰ For further information, please visit the Australian Cyber Security Centre via www.cyber.gov.au/acsc/view-all-content/advice/guidelines-system-monitoring

¹¹ For further information, please visit the Australian Cyber Security Centre via www.cyber.gov.au/acsc/view-all-content/advice/guidelines-system-hardening





A disruption is anything that interrupts your business-as-usual operations. Disruptions can occur at any time, for any reason and their impact varies.

Maintaining a business continuity plan is crucial in ensuring your agency's critical functions can continue to operate to the fullest extent possible during, and post, a security incident or disruption. You must plan for continuity of the resources that support your agency's critical functions.

Before developing a business continuity plan, it is important that you understand the critical functions your agency performs and the assets which support these functions.¹² When you identify your agency's critical functions and relevant assets and/or services, you are supporting your criticality assessment by identifying and understanding what you need to protect.

The Tasmanian Government Incident Management Cybersecurity Standard¹³ requires you to maintain a register of critical business information regarding assets and/or services, which will support you to achieve the requirements of this policy (INFOSEC-3).

Having a business continuity plan can help your agency manage the impact of security incidents or disruptions, regardless of the cause. However, simply planning does not represent successful business continuity.

It is recommended your agency implements a business continuity program which includes continual planning and improvements, exercising/testing your business continuity plan to ensure you are prepared for security or disruptive incidents, and embedding business continuity into your agency's culture.

Ensuring your agency can provide access to information on a 'need to know' basis during a security or disruptive incident, while protecting it from unauthorised access, is crucial. The integrity of your ICT systems and associated services should be included in your business continuity planning and programs. Ensuring you have system and service recovery procedures will enhance your agency's ability to recover more broadly from any security or disruptive incidents.

For further information and assistance with business continuity plans and programs, please refer to ISO 22301:2019 – Security and resilience – Business continuity management systems – Requirements.

¹² Refer to TAS-PSPF policy: Security planning (GOVSEC-5) for further information on criticality assessments.

¹³ Available via the Department of Premier and Cabinet website at www.dpac.tas.gov.au/_data/assets/pdf_file/0010/123004/Tasmanian_Government_Incident_Management_Cybersecurity_Standard.pdf

Required action: Own and be accountable for security risk in ICT systems

All systems must have a business risk owner (system owner) to ensure ownership of and accountability for information security risk in ICT systems. As mentioned previously, it's important to remember that 'systems', in this context, include those operated by outsourced managed services and cloud service providers that process, store or communicate Tasmanian Government information and data. The system owner is responsible for ICT governance processes, ensuring secure operation and that business requirements are met. The owner may be the same for external systems utilised by your agency and for various (or all) internal systems.

It is recommended that system owners for large or critical systems are part of your agency's senior executive team or hold an equivalent management position.

System owners have an important role in the ongoing operation and monitoring of your agency's ICT system/s. Any monitoring activities should be conducted as specified by the system owner, which may include vulnerability assessments and penetration tests.

A system owner's responsibilities

System owners are responsible for the overall operation and maintenance of an ICT system, including the monitoring phase in the system's life cycle (as described above in Table I – ICT system life cycle). This includes any related support service or outsourced service, such as a cloud service.

System owners may delegate the day-to-day management and operation of the system to a system manager.

Operating the system and maintaining authorisation

It is recommended that system owners are responsible for ongoing compliance with your RE's authorisation, in accordance with your agency's operational requirements. This includes ensuring any system modifications are made correctly, in line with the system's controls and risk environment. Where necessary, due to modifications or ongoing monitoring activities, the system owner must ensure appropriate re-authorisation occurs.

Supporting documentation

System owners are also responsible for the development of documentation supporting the safe operation of the system. This documentation may include a security risk management plan and standard operating procedures. System owners must ensure the developed documentation remains current.

When developing any such documentation, the system owner should include the ASA to ensure a holistic understanding of both the agency's, and the system's, operational environment and security risks.

Required action: Ensure effective physical controls and secure zones

Protecting the confidentiality, integrity and availability of your agency information requires a layered approach to security measures, as no singular approach is a fully effective security measure. By adopting a layered approach, you reduce the likelihood of successful unauthorised or malicious attacks. In support of this policy, your agency must ensure effective physical controls and application of secure zones at any location where information (in any form) is stored.

Information, in any form, is valuable and must be protected according to its sensitivity or security classification. To achieve this, the system owner and the information originator must ensure the appropriate classification has been applied. This will then dictate how that system or information is to be stored, handled and transferred.

The TAS-PSPF supports risk-based decision-making, with the exception of required protections for sensitive and security classified information. However, your agency should apply sound risk management to the security of all technology and information assets, finding a balance between the extent of security measures and effective operation.

Please refer to TAS-PSPF policy: Protecting assets (PHYSEC-1) and TAS-PSPF policy: Agency facilities (PHYSEC-2) for detailed guidance on best practice physical security measures, including security zoning of work areas.

Required action: Consider supply chain security

Security risks can arise through the procurement of goods and services and effective risk management is required to reduce the likelihood and consequence of security issues or incidents. During procurement processes, your agency may engage multiple contractors, or a contractor may engage multiple subcontractors as part of the supply chain.

A supply chain is the network of developers, manufacturers, distribution centres and delivery means involved in the supply of goods and services to an agency, including ICT systems, cloud-based and outsourced services. Supply chains can be large and complex, involving many suppliers doing many different things. They may also span the globe, with goods potentially transiting many countries and being handled by multiple people before reaching your agency.

The more parties involved in a procurement or service provision, the greater or more complex the risk becomes. In addition, transparency of (and control over) operations is more challenging the further down a supply chain it is from government. For example, arrangements where resources are made, held or serviced outside of Australia (by the contractor or a subcontractor) may have additional risks because visibility is lower.

This policy (INFOSEC-3) requires your agency to ensure supply chain security is considered at all stages of contracted supply.

When procuring goods and services, it is recommended that you:

- consider the security risks of each service provider independently and holistically across their contracted and subcontracted partners
- reduce vulnerabilities and ensure security continuity to manage risks along the entire supply chain.

Understanding risks, threats or vulnerabilities in the supply chain

Identifying relevant threats and vulnerabilities associated with a procurement helps you to identify suitable security mitigations.

In conducting a supply chain risk assessment, it is recommended that you:

- identify the suppliers who make up the supply chain – check that the suppliers can articulate who and what they are connected to, and what dependencies they have
- determine the value and classification of the information that the supplier and their subcontractors will have access to
- identify vulnerabilities or recognise where they could be introduced and exploited.



If you do not conduct a risk assessment or understand the risks, threats or vulnerabilities associated with a procurement, you will be unable to identify appropriate risk mitigations.

When undertaking a procurement risk assessment, you should consider and seek to identify security risks that could affect or be caused by:

- the state or national interest
- critical infrastructure (agency-specific, Tasmanian and national critical infrastructure)
- people transacting with the agency via a contractor (or subcontractor)
- the ability to maintain control of information or resources in an outsourced, offshore or supply chain arrangement with potentially changing legal frameworks
- foreign involvement
- insider threat
- Tasmanian Government agencies or other entities
- agency security plans.

It is recommended that your agency consult experienced subject matter experts as part of assessing risk and designing mitigation strategies when the scale, scope and nature of the risk warrants it.

Reducing supply chain vulnerabilities and managing risks

Contract documentation

Relevant security provisions and associated protections should be included in procurement documents such as requests for tender, contracts, or service agreements. The benefit of ensuring security terms and conditions are identified is that they are then legally enforceable.

Where possible, you should include terms and conditions in procurement documents relating to:

- imposing appropriate information, physical and people security requirements
- identified security risks relevant to the procurement
- ongoing management of security risks and any proposed risk treatments.





It is recommended that you establish robust governance and assurance processes so that contracted providers implement applicable protective security requirements. These may include:

- identifying who is accountable for each security treatment or control in the contract
- establishing governance arrangements to manage ongoing protective security requirements (during the contract and at the completion or termination of the contract). This includes permission for your agency to:
 - amend (or terminate) a contract where issues of state or national interest arise (e.g. procedures to address actual or suspected security incidents or breaches, or when there is a change of ownership of supplier that is not approved)
 - monitor ongoing contracts (e.g. access to premises, records and equipment) through all levels of the supply chain/s, including subcontractors
 - manage changes to the provision of goods or services
 - approve or reject the engagement of individual subcontractors
 - terminate the contract if the provider fails to comply with provisions in the contract, including where there is unwillingness or inability to remedy or mitigate security incident/s.
- applying relevant information-handling controls and storage arrangements to protect sensitive or security-classified information (requiring contracted goods and service providers to protect Tasmanian Government information and assets in the same manner as your agency would)
- applying relevant people security provisions such as pre-employment screening and security clearance vetting requirements for people accessing security-classified Tasmanian Government information and assets (applying the same security measures to the contracted providers people as your agency would to its people)
- applying relevant physical security measures at facilities where Tasmanian Government information and assets are held and where goods are prepared for Tasmanian Government use
- addressing all hazards your agency may face in the protection of its information, people and assets (including requiring contracted goods and service providers to apply protections against threats to state and national security).



Common use contracts

Common-use contracts are established where a common requirement for goods or services across government agencies has been identified. The Tasmanian Government has established common-use contracts which must be used by agencies when procuring specific goods and services.

Using common-use contracts can help you reduce supply chain risk because the security and capability of the contracted supplier/s has already been scoped. A list of common-use contracts is available on the Tasmanian Government's purchasing website.¹⁴ Even when using common-use contracts, keep in mind that you still have a responsibility to perform due diligence, validation, and acceptance for supply chain services.

¹⁴ The Tasmanian Government's purchasing website is at www.purchasing.tas.gov.au/contracts/common-use-contracts-of-the-tasmanian-government



Annexure I: ICT systems and authorisation

Type of ICT system	TOP SECRET system	TOP SECRET sensitive compartmented information system	SECRET system	PROTECTED and OFFICIAL system (including OFFICIAL: Sensitive)	Multinational and multi-agency system	Outsourced information technology and cloud services (with the exception of a TOP SECRET system)	Gateways
<p>Security assessor – reviews the system architecture, including security documentation, and assesses the implementation and effectiveness of security controls.</p> <p>These assessments are typically undertaken by an Infosec Registered Assessors Program (IRAP) assessor or people within the agency who have appropriate capability.</p>	Australian Signals Directorate assessor (or their delegate)	Australian Signals Directorate assessor (or their delegate)	Agency assessor – IRAP assessor	Agency assessor or IRAP assessor	Determined by agreement between the parties involved	IRAP assessor	IRAP assessor





Authorising officer - reviews the authorisation package ¹⁵ and makes an informed risk-based decision as to whether the security risks associated with an ICT system's operation are acceptable or not, and grants authorisation for the system to operate.	Director-General Australian Signals Directorate (or their delegate)	Director-General Australian Signals Directorate (or their delegate)	Accountable Authority or Chief Security Officer (or their delegate)	Accountable Authority or Chief Security Officer (or their delegate)	Determined by formal agreement between the parties involved	Accountable Authority or Chief Security Officer (or their delegate)	Accountable Authority or Chief Security Officer (or their delegate)
--	---	---	---	---	---	---	---

¹⁵ The authorisation package includes the ICT system's system security plan, incident response plan, continuous monitoring plan, security assessment report, and plan of action and milestones.



References and resources

Australian Government, System Monitoring Guidelines, at www.cyber.gov.au/acsc/view-all-content/advice/guidelines-system-monitoring	
Australian Government, System Hardening Guidelines, at www.cyber.gov.au/acsc/view-all-content/advice/guidelines-system-hardening	
New Zealand Government, at	Supply chain protectivesecurity.govt.nz/governance/supply-chain-security/
	System ownership protectivesecurity.govt.nz/governance/protective-security-roles-and-responsibilities/roles-and-responsibilities-for-information-security/system-owners-maintain-and-operate-systems/
	Outsourcing and supply chains protectivesecurity.govt.nz/information-security/managing-specific-scenarios/outsourcing-offshoring-and-supply-chains/
Tasmanian Government, Cyber Security Policy, at www.dpac.tas.gov.au/_data/assets/pdf_file/0024/103839/Tasmanian_Government_Cybersecurity_Policy.pdf	
Tasmanian Government, Information Framework, at www.informationstrategy.tas.gov.au/Government-Information-Strategy	
Tasmanian Government, Common use contracts, at www.purchasing.tas.gov.au/contracts/common-use-contracts-of-the-tasmanian-government	
UK Government, Logging and protective monitoring, at www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/logging-and-protective-monitoring	



Department of Premier and Cabinet
Resilience and Recovery Tasmania

Phone:
(03) 6232 7979

Email:
sem@dpac.tas.gov.au