ACT Government

# ACT Government Cyber Security Policy

Version: 3.5

Updated: 10 November 2025

Approved by: ACT Government Chief Information Security Officer

## Contents

# 1. INTRODUCTION

## 1.1 Purpose

This Policy establishes the ACT Government framework for cyber security for official *territory records*, information, or data being processed or stored in electronic form.

The Cyber Security Policy derives its authority from the *ACT Government Protective Security Framework* (ACT PSF) and supplements the ACT PSF with guidance to:

- develop cyber security awareness, culture and practices in the ACT Public Service.
- ensure information and communication technology (ICT) resources and infrastructure protect official information up to the OFFICIAL: Sensitive classification, including its Information Management Markers (IMM) such as OFFICIAL: Sensitive – Personal Privacy.
- ensure all information assets when in electronic form are continuously available and protected to a level commensurate with the assessed risk and sensitivity/classification of the asset.
- define standards for the defence against unauthorised access, use, modification, disclosure, damage, or destruction of information assets (see Appendix A: Associated Documents).
- mandate processes to minimise risks associated with disruption or failure of ICT systems.

## 1.2 Background

In fulfilling its commitment to the community, the ACT Government collects, receives, and develops official information.

If official information is lost, inappropriately changed, or disclosed to unauthorised parties, it has the potential to harm members of the general public, harm the reputation of the ACT Government, disrupt the business functions of administrative units, the delivery of justice, and the national security of the ACT and Australian Governments.

The ACT Attorney-General, through the ACT PSF, instructs administrative units to:

- protect official information by achieving the mandatory requirements of the ACT PSF and Cyber Security Policy.
- identify vulnerabilities and assess their security risks for the protection of information.
- develop an appropriate security culture and proportionate measures to securely meet their business goals.
- meet the expectations for the secure conduct of government business.

The Cyber Security Policy was developed to guide administrative units and to set a baseline of mandatory cyber security standards and practices for ICT systems based on national and international standards (see Appendix B: Mapping to standards).

## 1.3 Scope

This Policy must be observed by all ACT Government employees and contractors, agents of the ACT Government, and incorporated bodies.

It applies to all ICT assets including, but not limited, to physical or logical computing devices either owned, leased, or used by the ACT Government to hold or process ACT Government electronic information, and any electronic information held on those assets.

It also applies to all ICT systems including common ICT infrastructure and strategic platforms, cloud services, and outsourced services with an ICT component.

This Policy excludes non-electronic information.

## 1.4 Compliance

The conventions used in this Policy include:

- MUST, or the terms "REQUIRED" or "SHALL", mean that the policy is an absolute requirement of the ACT Government. A policy waiver must be approved to proceed without complying.
- MUST NOT, or the phrase "SHALL NOT", mean that the policy is an absolute prohibition of the ACT Government.
- SHOULD, or the adjective "RECOMMENDED", mean 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, or the phrase "NOT RECOMMENDED", mean that there may exist valid reasons in particular circumstances when the behaviour is acceptable or even useful, but the full implications should be understood and carefully weighed before implementing.
- MAY, or the adjective "OPTIONAL", mean that an item is truly optional.

**Failure to comply with this Policy will result in disciplinary action under the terms and conditions of the contract of employment or engagement, or prosecution under the appropriate Act.**

**In some circumstances non-compliance with this Policy may also expose individuals to penalties under law, for example if they commit an offense under the *Information Privacy Act 2014*. Penalties for committing an offense include fines and/or imprisonment[1].**

## 1.5 Reference

This Policy provides a whole-of-government (WhoG) information security regulatory framework to ensure the ACT Government meets its obligations to protect and safeguard official information assets.

Applicable legislation, policies, and standards include, but are not limited to, those referenced in Appendix A: Associated Documents.

Directorates may have complementary policies and legislation that must also be complied with.

## 1.6 Contact

For any queries about this Policy, contact the ACT Government Cyber Security Centre (ACT CSC) via cyber.security@act.gov.au.

# 2. RESPONSIBILITIES

| Role | Responsibilities |
|---|---|
| **ACT Chief Digital Officer (CDO)** | Responsible for driving the ACT's digital agenda and leading the whole of government strategic direction for ICT. |
| **ACT Government Chief Information Security Officer (CISO)** | The position of ACT Government Chief Information Security Officer (CISO). A WhoG role that manages the strategic direction of cyber security for ACT Government and the implementation and operation of WhoG cyber security measures. |
| **ACT Govt staff** | Comply with the Cyber Security Policy and Acceptable Use Policy. |

[1] *Information Privacy Act 2014*, s 53 (Offence—use or divulge protected information)

| Role | Responsibilities |
|---|---|
| **Agency Security Advisors (ASAs)** | Responsible for day-to-day management of the protective security measures within the administrative unit. Develops, implements, and monitors administrative unit security procedures and systems. Analyses the administrative unit's security environment and posture, and plans measures to manage security risks. |
| **Agency Security Executives (ASEs)** | The delegate of the Director-General or agency head with authority to approve protective security programs for their administrative unit. |
| **Business System Administrator** | An ACTPS officer with access privileges, knowledge, and skills necessary to administer the day-to-day operation of the ICT system. Applies access levels, manages system configuration, and adds/changes/removes/suspends user access. |
| **Business System Manager** | An ACTPS officer who is responsible for the integrity and operation of the ICT system; negotiates service levels; authorises access levels and access for all new users including staff, contractors, vendors and volunteers; and reviews audit logs. |
| **Business System Owner** | Person at executive or senior executive level within an administrative unit who has the authority to make binding financial and operational decisions regarding an ICT system, and to accept residual risk on behalf of the Director-General. |
| **Chief Information Officers (CIOs)** | Executives in each administrative unit responsible for ICT services. May also be Business System Owners of administrative unit ICT systems and infrastructure. |
| **Database Administrator** | An officer with access privileges, knowledge, and skills necessary to administer the data in the system and is typically able to view and manipulate data in aggregate, develop and modify queries and perform extract/transform/load (ETL) activities. |
| **ACT Government Cyber Security Centre (ACT CSC)** | DCBR team responsible for developing WhoG Cyber Security Policy, standards and strategies. Comprised of the CISO, security engineers, security analysts and investigators who provide cyber security advice; implement and operate WhoG security measures; and lead cyber security incident response. |
| **Digital Canberra (DCBR)** | Digital Canberra leads the ACT Government's technology, digital, data, and cyber security services It leads the implementation of the ACT Digital Strategy and ACT Digital Health Strategy, manages ICT infrastructure for our hospitals, schools, and public service, and represents the ACT at national digital, data, and cyber security forums. |
| **Directors-General and agency heads** | Responsible under the ACT PSF for the security of the information and ICT systems in their administrative unit. These responsibilities are often delegated to a Senior Executive Responsible for Business Integrity and Risk (SERBIR). |
| **Business Partners (DCBR)** | DCBR staff embedded in administrative units who are responsible for liaison and assisting administrative units with DCBR solutions. They perform a broad range of functions including collecting business system information and advising administrative units about business system criticality. |
| **Information Owner** | The Information Owner is the originator of a piece of information. They are responsible for classifying the information and ensuring it is stored with security controls commensurate to the information's classification. |
| **JACS Security & Emergency Management Division (SEMD)** | SEMD is responsible for developing WhoG policy on public sector protective security. |
| **Records Manager** | Responsible for education and assisting their administrative unit in meeting their records, information, and data management responsibilities. |

# 3. CYBER SECURITY PROGRAM

## 3.1 Security Operations

The CISO is responsible for developing and maintaining the ACT Government's operational cyber security capabilities, including workforce, processes, and technologies, to:

- Identify cyber security threats, vulnerabilities, and risks.
- Protect identified ICT assets by implementing appropriate management, operational, and technical controls.
- Monitor for and detect cyber security events.
- Respond to events that become cyber security incidents.
- Recover ICT assets impacted by cyber security incidents and plan for resilience.

## 3.2 Security risk management

Administrative units should adopt an organisational risk register to manage cyber security risks. Risk registers must align with the ACT Government Risk Management Policy, and should follow a consistent framework to ensure coordination of risks between whole-of-government, administrative unit and per-system strata.

The risk register will provide:

- Executive visibility of information security risk across government.
- Identification of ICT assets to be protected (including information assets and services).
- Risk mitigation recommendations from security advisors.
- Reporting to relevant stakeholders.
- Monitoring of risk treatments and their effectiveness.
- Informed advice for cyber and information security strategies.

## 3.3 Security communications

The ACT Government CISO is responsible for ensuring the ACT Government establishes and maintains security information channels with appropriate security authorities, and for communicating relevant cyber security information (particularly regarding emerging threats, security incidents and new technologies) to ASEs, ASAs and CIOs.

External contact and security information is exchanged with:

- The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC).
- Other government jurisdiction CISOs including Australian states and territories.
- Vendors of ACT Government Strategic Platforms (for example Microsoft, AWS, Oracle, Salesforce).

Internal contact and security information is exchanged with (but not limited to):

- JACS Security and Emergency Management Division (SEMD)
- The Chief Digital Officer (CDO)
- ACT Government Solicitor (ACTGS)
- ACT Auditor-General's Office (AGO)
- Territory Records Office (TRO)
- Agency Security Executives (ASEs) and Agency Security Advisors (ASAs)
- Senior Executive Responsible for Security
- Chief Information Officers (CIOs)

- System administrators and executive staff within DCBR

### Instructions

The ACT Government CISO or their delegate will:

1. Convey security advice to ASAs, ASEs and CIOs as needed to respond to external and internal cyber security developments.
2. Develop cyber security advice for users, administrative units, or WhoG as needed and will communicate with these audiences as authorised by the ACT Government CISO.
3. Represent DCBR or participate as an advisor or observer as needed on government deliberations requiring cyber security advice.
4. Produce cyber security posture reporting for WhoG and administrative units.
5. Publish and maintain ACT Government's Cyber Security Framework.

# 4. INFORMATION SECURITY

## 4.1 Protecting records, information and data

ACT Government organisations must take steps to protect their records, information, and data from misuse, interference, loss, unauthorised access, modification and disclosure.

The principles relevant to the security of information are described in the *Territory Records (Records, Information and Data) Standard 2016 (No 1)*, which is a mandatory standard issued under the *Territory Records Act 2002*.

### Instructions

1. Understand and remain aware of the *Territory Records (Records, Information and Data) Standard 2016 (No 1)* and principles.
2. Ensure all official Territory records, information, and data are:
    a. registered as a record in an approved Electronic Digital Records Management Systems (EDRMS), or
    b. managed in a system that:
        i. is registered with DCBR
        ii. is identified in the administrative unit's Records Management Plan
        iii. has undergone, in consultation with the TRO, a Business Systems and Digital Recordkeeping Functionality Assessment, including a records, information, and data risk assessment.
3. Do not delete original Territory records, information, and/or data without approval of the Information Owner, and Records Manager.
4. When starting a new ICT initiative, perform an assessment to determine any records, information, or data it may hold.
5. Information Owners should use the Business Systems and Digital Recordkeeping Functionality Assessment tool to assist with determining their records, information, and data requirements.

## 4.2 Information classification

For information security purposes, there are three types of official Territory information:

- information that does not need increased protection (public or OFFICIAL information).

- information that needs increased security (any information with an Information Management Marker (IMM)).
- information requiring significantly increased security (any information classified PROTECTED or higher per the ACT Government PSF).

Most official Territory information is likely to be classified at the IMM level or lower. If you believe the information you are handling should be classified at the PROTECTED level or higher, contact your ASA.

All ACT Government employees and contractors are responsible for making this decision about the Territory information they own and handle, using a process called **information classification**. The information classification is then used to determine how the data must be handled and protected.

The ACT Government information classification scheme and protection requirements are defined in the ACT Government *Protective Security Framework* (ACT PSF).

### Instructions

1. Understand and remain aware of the ACT PSF Information Security requirements.
2. Ensure all Territory information is classified correctly.
3. Do not change the classification of information (including removing IMMs) without approval of the Information Owner.
4. Information Owners should use the Information Security Assessment template to assist with determining information security requirements.

## 4.3 Personal information

The ACT Government collects, holds, uses and discloses *personal information* to effectively carry out functions or activities under the *Public Sector Management Act 1994*, the *Territory Records Act 2002*, the *Freedom of Information Act 1989*, the *Information Privacy Act 2014*, the *Health Records (Privacy and Access) Act 1997* and other legislation relating to government functions.

All ACT Government employees and contractors are responsible for complying with applicable legislation. Staff should remain aware of and apply the Territory Privacy Principles (TPPs) and comply with the *Information Privacy Act 2014* when handling personal information in an ICT system. Specific instructions relating to ICT usage are described below.

### Instructions

1. When starting a new ICT initiative, perform a privacy threshold assessment to determine the presence and sensitivity of *personal information*.
2. Information Owners should use the Information Security Assessment template or similar mechanism to assist with performing a privacy threshold assessment and PIA.
3. When indicated by a privacy threshold assessment, perform a Privacy Impact Assessment (PIA) to determine the handling requirements of *personal information*.
4. When *sensitive information* is present (including *personal health information*), engage the ACT CSC to determine the protective measures required through risk management of ICT Systems.
5. Cloud services that handle OFFICIAL: Sensitive - Personal Privacy information should be hosted in Australia unless treatments are applied to ensure security and privacy of the information from third parties (including vendors) and any residual risk is known and accepted by the business system owner.

# 5. CYBER SECURITY AWARENESS AND TRAINING

## 5.1 Cyber Security awareness

The environment in which we work demands a culture of security to protect against information security breaches. Human error is the biggest risk to protecting electronic information.

Cyber Security policies and procedures in themselves do not minimise the ability of intruders to compromise information. As human engagement is critical in implementing an effective and robust cyber security framework, cyber security awareness is crucial to prevent security incidents.

The ACT Government cyber security training and awareness program:

- increases user awareness on the importance of securing information efficiently.
- helps users understand the different types of threats, risks and vulnerabilities that exist in ICT and physical environments.
- teaches users about effective ways to mitigate security risks, and how to use security management practices and tools to increase information security.

### Instructions

1. Cyber Security awareness training must be conducted within each administrative unit in formal staff induction sessions and refresher training on a regular basis.
2. It is the administrative unit's responsibility to ensure that this training is relevant to the administrative unit's work environment.
3. Administrative units' cyber security awareness training must include topics about information security, including privacy and procedures relating to system and records, information and data access
4. On commencement of employment, staff must agree that they will not divulge ACT Government official information. Staff must also agree that they will not seek access to records, information, and data that is not required as part of their normal duties.
5. System Administrators should be properly trained in all aspects of system security prior to supporting their business systems and should work in partnership with the administrative unit's Records
6. Manager to ensure the protection of records, information, and data in their systems.

## 5.2 Acceptable use of ICT resources

ACT Government provides ICT resources to its employees to serve the ACT community. These resources must only be used for approved purposes to ensure the community gets the best value from its investment. The ACT CSC logs and monitors use of ACT Government ICT resources (e.g. Internet, email, instant messaging) in compliance with the *Workplace Privacy Act 2011* and may use this as evidence in disciplinary matters.

### Instructions

1. When using ACT Government ICT resources, all ACT Government employees and contractors must comply with all laws of the ACT and Australia and comply with the ACT Government Acceptable Use Policy.

# 6. PERSONNEL SECURITY

## 6.1 Security Clearances

Staff with access to sensitive information or critical systems may require a security clearance provided by an appropriate vetting process before commencement of duties.

### Instructions

1. All ACT Government employees and contractors must have a criminal record check performed and satisfy other pre-employment requirements determined by each administrative unit prior to appointment.
2. The *ACT Government Protective Security Framework* (ACT PSF) Personnel Security requirements must be satisfied as relevant to the identified eligibility requirements of the position held by an employee or contractor.
3. The ACT Government *Security Clearance Policy* must be followed as relevant to the identified eligibility requirements of the position held by an employee or contractor.
4. Employees and contractors with directorates who hold a position with **administrator access** to government critical or business critical systems, or the ability to change health or sensitive human resources (HR) records, must satisfy the *Security Clearance Policy* and *the ACT Government Protective Security Framework*.
    a. Where these systems are hosted on DCBR managed infrastructure, the ACT Government Chief Information Security Officer will have discretionary power to require additional security vetting, including DCBR's Personnel Vetting Program (PVP) or AGSVA clearance processes.
5. In addition to point four:
    a. Employees and contractors with Digital Canberra (DCBR) specifically who hold a position with **administrator access** to government critical systems or business critical systems, or the ability to change health or sensitive human resources (HR) records, must obtain and maintain through the ACT Government Cyber Security Centre, DCBR's PVP certificate OR have an active AGSVA security clearance (of any level).
    b. Employees and contractors with DCBR specifically who hold a position with **Super User administrator access**, must be an Australian citizen and obtain and maintain a Negative Vetting 1 (NV1) Australian Government Security Vetting Agency (AGSVA) security clearance. For the policy statement, 'Super User' is defined as privileges of Domain Administrator or Global Administrator, or their reasonable equivalence, in the Test or Production networks of CIT, Education or ACTGOV.
6. Employees and contractors with a security clearance suspension or removal must have their **administrator access** removed immediately.
7. Requests made for waiver consideration for short-term employee and contractor placement in positions with **Super User administrator access** will be determined by the ACT Government Chief Information Security Officer (CISO).

# 7. PHYSICAL AND ENVIRONMENTAL PROTECTION

## 7.1 Physical security of ICT resources

All ICT Systems or ICT Assets identified as critical must be physically protected in secure areas from unauthorised access, damage and interference using security controls advised by DCBR Security on a risk-assessed basis.

Controls typically include physical isolation of assets in a **secure area**, protected by a defined security perimeter, with appropriate security barriers and entry controls.

Secure areas include but are not limited to computer rooms, Private Automatic Branch Exchange (PABX) rooms, network equipment rooms, and associated facilities.

### Instructions

1. Access to secure areas is restricted to authorised ACT Government personnel. Access must be controlled using passwords, locks, and/or other access-control devices.
2. Third-party access to secure areas must be restricted to authorised personnel with an equivalent level of personnel security vetting to the ACT Government and a need-to-access.
3. Secure areas must be monitored on a risk-assessed basis using access control logs and CCTV surveillance.
4. All wiring closets must be secured to prevent damage, unauthorised attempts to connect to data outlets, and interception of records, information and data.
5. Access to network connection points located in public areas, conference rooms and other high-risk environments must restrict access only to trusted devices.

# 8. MAINTENANCE OF ICT ASSETS

Maintenance of ICT assets, from replacement of failed media (supporting a system's continued availability) to updating firmware and software (protecting a system from bugs and vulnerabilities), is vital to the security of information assets and government functions.

## 8.1 Maintenance of ICT infrastructure

ACT Government engages DCBR to develop and maintain its ICT infrastructure. For technical systems with a Criticality of Essential Infrastructure, DCBR should develop, document, and disseminate to support personnel:

1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among technical teams, administrative units and vendors; and
2. Procedures for the implementation of the system maintenance policy and associated system maintenance controls.

## 8.2 Maintenance of business systems

ACT Government engages DCBR and a range of cloud service providers to develop and maintain business systems. For each business system with a System Security Plan (SSP), the system maintenance policy and procedures described above should be documented in or attached to the SSP.

## 8.3 Stolen, lost or damaged ICT resources

ACT Government stores official information locally on ICT resources such as servers, laptops, smartphones and removable media devices. Theft, loss, or damage to these resources may indicate a security incident related to the information.

### Instructions

1. Report all incidents of lost, stolen, or damaged ACT Government ICT equipment as soon as possible to the DCBR Asset Team using the Report lost or stolen ICT devices form or the Report damaged ICT devices form.

2. Refer all incidents of lost, stolen or damaged ICT equipment to the embedded ICT team or DCBR Service Desk for recording and escalation for investigation to the ASA.
3. Information such as the value of the missing or damaged item(s) must be recorded and any information stored on such items must be identified and reported to the administrative unit's Records Manager.
4. Where the incident is considered a significant cyber security incident, ASAs, embedded ICT teams or Service Desk must escalate it to the ACT CSC for investigation. The ACT CSC will prepare an incident report to the ASA including the findings of the investigation.
5. ASAs should file a copy of the report in their approved system of record.

# 9. SYSTEMS AND SERVICES ACQUISITION

Administrative units using external service providers to process, store or communicate official information or manage business systems on their behalf must ensure service providers meet the same security requirements that administrative units must meet, as described in the Cyber Security Framework.

## 9.1 Procurement of ICT systems

Administrative units must identify and agree upon security requirements prior to developing or procuring ICT systems including cloud services. Providers of ICT systems should support administrative unit compliance with the requirements of the Cyber Security Policy.

When procuring ICT systems including cloud services that handle information classified with any IMM or higher, administrative units must follow all procurement policies and should follow due diligence guidelines, including a review of contract terms, prior to entering any agreement.

### Instructions

1. Administrative units should consult with DCBR to determine if an ICT system already exists to perform the required service that suits the information security requirements of the business.
2. Administrative units should choose ICT systems that are already approved for WhoG use (where they are fit for purpose) in preference to unsanctioned ICT systems.
3. Administrative units should use the Secure Technology Procurement Toolkit - Digital Canberra when preparing an approach to market for ICT services and/or providers, noting these are not a one-size-fits-all solution and further procurement and security advice may be required.
4. Administrative units should consult with Procurement ACT and/or ACTGS to leverage existing, reviewed contractual clauses designed to address cyber security requirements during ICT procurements. Note these are not a one-size-fits-all solution and adjustments requiring additional legal and security advice may be necessary.
5. Administrative units should not agree to contract terms that compromise the confidentiality or integrity of official information, or the availability of business systems. Administrative units should seek support from the ACT CSC and/or ACTGS if such terms are identified in a draft or existing contract.
6. Administrative units should not release official information to third parties who are not already contracted to the Territory or do not have a need to know.
7. Administrative units should consult with their Records Manager or the TRO to determine any records, information, or data management requirements.

## 9.2 Management of ICT systems

Administrative units must manage ICT systems, to ensure contract management, access control, auditing, patching, change control and other system governance activities are performed.

### Instructions

1. The System Owner of a critical business system, WhoG system, or strategic platform must delegate a System Manager to oversee the day to day running of the system.
2. The System Manager and their contact details must be identified in the system record managed by DCBR and registered as a record in the administrative unit's EDRMS or appropriate system of record.
3. The System Manager is responsible for at least the following:
    a. Negotiating associated changes and/or upgrades.
    b. Authorising access levels, periodically reviewing access levels.
    c. Running the audit log analysis, approving analysis results.
4. The System Manager should not have System Administrator privileges, to ensure separation of duties.

# 10. GOVERNANCE, RISK AND COMPLIANCE

## 10.1 Governance of cyber security

All administrative units have an obligation to manage the security risk of their information assets.

### Instructions

1. Administrative units must follow an agreed whole of government framework to:
    a. Establish the ownership and governance of ICT systems.
    b. Register ICT systems.
    c. Perform a security risk assessment of ICT systems.
    d. Ensure ICT systems have appropriate disaster recovery and business continuity plans.
    e. Decommission ICT systems no longer in use.
    f. Report on compliance with the Cyber Security Framework and ACT PSF.

## 10.2 Ownership of ICT systems

All ICT systems including cloud services must have an identified Business System Owner, who is accountable for the operation and security of ICT systems.

### Instructions

1. Business System Owners must be a member of the ACT Public Service Senior Executive Service with the delegation to accept security risk on behalf of the Director-General.
2. Administrative units must name the Business System Owner when registering an ICT system.
3. Administrative units must advise DCBR when the Business System Owner changes.

## 10.3 Registration and inventory of ICT systems

When procuring, migrating or transferring Territory information to ICT systems (including cloud services) administrative units must register each system with DCBR. Information about registered systems must be stored and maintained in an authoritative inventory to enable visibility and risk management.

### Instructions

1. Administrative units must register all ICT systems, public websites, and cloud services with DCBR.
2. DCBR will assist administrative units to discover unregistered ICT systems.
3. DCBR will maintain an inventory of ICT systems including external systems such as cloud services.
4. The ICT system inventory should include at least the:
    a. system name and type.
    b. business criticality of the system.
    c. classification of the information handled by the system.
    d. host and location of ACT Government information assets.
    e. products and vendors used, including third party service providers.
    f. Security Point of Contact (SPOC) of the vendor, including contact details.
    g. Business System Owner and Business System Manager (who acts as the system SPOC).
5. Administrative units must notify DCBR of changes to these details during the life of the system.

## 10.4 Criteria for security risk assessment

System Owners must manage the security risk of their ICT systems. The ACT CSC provides a Risk Management Standard, processes and templates to ensure consistency.

**NOTE:** A security assessment is not a vulnerability assessment or penetration test. This requirement is described in Vulnerability management.

### Mandatory Assessment

It is **mandatory** to assess the security risks of an ICT system if it:

- is a business system with criticality of Government Critical, OR
- is a strategic platform for whole-of-government or multiple administrative units, OR
- hosts a public website of ACT Government on a unique or otherwise unassessed platform, OR
- is a cloud service handling official information with an Information Management Marker (IMM).

The ACT Government CISO or their delegate may determine that any ICT system requires security risk assessment if it presents risk to common ACT Government ICT infrastructure or information assets.

Exemptions may only be granted in writing by the ACT Government CISO or their delegate.

### Recommended Assessment

It is **recommended** to assess the security risks of an ICT system if it:

- is a business system with criticality of Business Critical, OR
- is a technical system with criticality of Essential Infrastructure, OR
- any business or technical system that handles official information with an Information Management Marker (IMM).

### No Assessment Required

It is **not required** to assess the security risks of an ICT system if it meets **exemption** criteria:

- criticality of Business Operational, Administrative or Non-essential Infrastructure, AND
- handles official information that is classified Public or OFFICIAL (no IMM), AND
- is not a public website of the ACT Government, AND
- is hosted by DCBR on-premises or in a strategic platform.

Exemptions may only be granted in writing by the CISO or their delegate.

## 10.5 Performing security risk assessments

The Business System Owner of an ICT system that meets the criteria for assessment is responsible for ensuring a security risk assessment is performed. The ACT CSC provides tools and processes that enable administrative units to self-assess the security risks of DCBR-hosted ICT systems.

### Instructions

1. Administrative units must identify and assess security risks to information and ICT systems and advise on appropriate security controls to implement the risk treatments.
2. The ACTIA risk matrix must be used to provide common definitions of likelihood, consequence and risk and must cover the baseline elements of the System Security template provided by the ACT CSC.
3. Additional risks may be identified by the assessor, the client or the ACT CSC.

## 10.6 Security authorisation

Security authorisation is performed at several levels and must be based on understood and accepted security risk:

| System Type | What role is responsible for security authorisation |
|---|---|
| **Administrative Unit ICT infrastructure** | Administrative Unit ASE |
| **Business systems** | Business System Owners |

### Instructions

1. The CISO reviews and **endorses** the security assessment. Endorsement of a security assessment demonstrates that it identifies all known security risks and recommends appropriate controls to bring risk to an acceptable level.
2. The Business System Owner **approves** the security assessment after endorsement. Approval constitutes acceptance of residual risk levels and commitment to implement the documented security controls and advised risk treatments.
3. The security assessment should be approved before Territory information is transferred to an ICT system or cloud service.

4. Administrative units must review security assessments every three years, or when a significant change has occurred in the business, technology or security environment.
5. Administrative units should incorporate High and Extreme risks from security assessments into their wider organisational risk management plan.

## 10.7 Unregistered Cloud systems

Unregistered cloud services (also known as Shadow ICT) present potentially unacceptable levels of security risk to administrative units. Directorates must remain aware of the level of unregistered cloud services in use in their administrative units and the security risks to enable an informed risk management approach.

### Instructions

1. Administrative units are responsible for understanding the security risks of cloud services.
2. Administrative units should review cloud service usage, identify System Owners, contacts and other service management details that enable visibility and management of their cloud services used for Official purposes.
3. DCBR provides content filtering services to manage access to high-risk services that can be tailored to directorate requirements.

## 10.8 Security assessment review for change activities

When a major change to an ICT system occurs, the security assessment must be reviewed to ensure accuracy. The ACT CSC may exempt a change from further assessment activity if it meets the criteria below.

### Exemption from security assessment review

At the discretion of the ACT Government CISO or their delegate, changes to ICT systems may be exempt from security assessment if one or more of the following applies:

1. The ICT system does not meet the criteria for a mandatory security assessment.
2. The ICT system has a valid SSP and the change does not materially impact security risks.
3. The system is a subsystem and is included in another SSP, and the change does not impact security risks in the system or related systems.
4. The security assessment has not been approved but has been reviewed by the ACT CSC and is close to completion. The Business System Owner commits to completion within 30 working days.
5. The change is for work that will be carried out in a non-production environment only.
6. The change is to install software into production for Pre-Prod testing, i.e. the Exemption is for Tech Review only – the security assessment must be completed before go-live.
7. The change relates to the implementation of infrastructure only, e.g.:
    - non-Essential Infrastructure; or
    - physical infrastructure (e.g. network infrastructure for a new building); or
    - upgrade to an existing component of the SOE or server system software.
8. The Change is simple remedial work to a Production system (e.g. to clear files cached on assets) unrelated to a change to an application.
9. Minor Changes (operating system patching, NMP hardware changes, etc.).

## 10.9 Compliance with Cyber Security policies

Administrative units must comply with this Cyber Security Policy and related Standards.

### Instructions

1. The ACT Government CISO or their delegate should periodically audit ACT Government ICT systems for compliance with this policy.
2. Cloud service providers who are independently assessed as compliant with controls of the ASD Information Security Manual, ISO 27000 or SOC 2 Type II standards and/or Cloud Security Alliance *Cloud Controls Matrix* (CCM) are compliant with many aspects of this policy.
3. Agreements with cloud service providers should, on a risk-assessed basis, include clauses to permit the ACT CSC or an independent third-party engaged by the ACT CSC to conduct:
    a. security investigations.
    b. compliance audits.
    c. vulnerability assessments.
    d. penetration testing.
4. Such agreements must include clauses requiring service providers to implement corrective action identified by investigation, audits and vulnerability testing.

## 10.10 Policy waivers

Policy waivers exist to accommodate exceptional circumstances where administrative units have a strong case for implementing ICT systems or services that are non-compliant with an existing policy.

### Instructions

Policy waivers are to comply with the *ICT Policy Waiver Procedure* and, where applicable, documented in the security assessment of ICT systems.

## 10.11 Compliance with other standards

Administrative units may be required to comply with other ACT, national or international standards for ICT systems and information security.

## 10.12 Payment Card Industry – Data Security Standard compliance

The Payment Card Industry – Data Security Standard (PCI-DSS) is a global standard that provides a baseline of technical and operational requirements to protect payment data. ACT Government is considered a Merchant for the purposes of compliance with the standard.

### Instructions

1. Administrative units must understand their compliance level and comply with the appropriate PCI-DSS requirements when handling payment data.
2. Administrative units must provide information to support PCI Qualified Security Assessors (QSAs) when audits are performed.
3. Payment card information is considered sensitive and is to be to be classified with an appropriate information management marker and protected in accordance with its classification and the PCI-DSS requirements.
4. Payment data must not be handled by systems that are not explicitly assessed as meeting the PCI-DSS requirements.

5. Administrative units must develop and maintain a security plan for any ICT system handling payment data.
6. Administrative units must develop operating procedures to manage payment data in accordance with the PCI-DSS requirements.

# 11. CONFIGURATION MANAGEMENT

## 11.1 Configuration management database (CMDB)

DCBR must maintain a CMDB to provide the central, complete and accurate inventory of components in the ACT Government ICT environment.

The CMDB is a database to record IT components, known as Configuration Items (CIs), and track them through stages of Change Management such as Architecture Design Review.

Any change, or reversal of a change, to a CI on ACT Government's infrastructure, will be performed exclusively through the Change Management Process.

## 11.2 Configuration management policy and procedures

Configuration Management provides a framework for:

- Documenting and maintaining the baseline configuration of ICT systems.
- Managing and tracking agreed system configuration as well as the integrity, availability and maintainability of the system.
- Planning to ensure the ability to reverse a deployment or implementation.
- Tracking system changes made, including installation of patches, to hardware, software, firmware, and documentation, through development, approval, testing, and controlled implementation of changes delivered into Production environments.

Given the geographic spread, delegated administration, and distributed ownership of ICT systems and services, ACT Government must centralise its Configuration Management information.

### Instructions

1. DCBR should formally document and maintain a configuration management plan that defines the purpose, scope, objectives, policies and procedures, and organisational and technical context for Configuration Management.
2. DCBR shall select and identify the physical, functional and structural characteristics of Configuration Items (CIs) including their owner, relationships and documentation. This includes allocation of identifiers and version numbers for CIs and updating the CMDB.
3. DCBR including the ACT CSC shall evaluate Major change requests and change proposals and provide approval or disapproval.

## 11.3 Baseline configurations and standards

DCBR shall maintain Baseline configuration documents for common infrastructure and environments including:

- Technology Reference Manual, guiding business system development to best practice to support and inform architectural decisions that are suitable for common ICT environments.
- Standard Operating Environment.
- Network Architecture.
- Security Architecture.

- Cloud Architecture, describing the design of Strategic Platforms chosen by DCBR to deliver common capabilities to WhoG.
- Other references as needed such as Integration Architecture.

All baseline documents shall be stored by DCBR in a secure, central location with appropriate access and version controls.

## 11.4 Configuration items to be managed

The CMDB is a central source of information for ICT roles such as Incident Management, Problem Management, Release Management, Change Management, Design Changes, Project Management, Security Governance, Risk Management and Compliance.

To ensure effective governance of the most relevant and important components of the ACT Government ICT environment, a subset of components are managed as CIs.

The following CIs should be managed in the CMDB:

- Business Systems (or Business Services and Applications) and Websites.
- Cloud Services (including IaaS, PaaS and SaaS).
- Servers – physical (Windows, Unix, Linux etc) and virtual.
- Network Devices, Data Storage, Chassis Components, and Datacentre Facilities.
- Workstations, Displays and Accessories.
- Duplication Machines – Multi Function Devices (Photocopiers), Printers, Faxes etc.

## 11.5 Security review of changes

All ACT Government change mechanisms must include security impact analysis of proposed changes which includes the consideration of security risk to the system and to its shared infrastructure.

## 11.6 Software licensing and usage

The ACT Government desktop environment provides a base level of software install for office productivity. Administrative units may use additional software but must ensure they are appropriately licensed.

### Instructions

In all cases, Administrative units must:

1. Manage software and if applicable license management.
2. Ensure software is package for the ACT Government desktop SOE.
3. Support the costs of lifecycle management including packaging, patching and upgrading.

## 11.7 User-installed software

Staff are not permitted to install software on workstations or servers without the express consent of DCBR. Such authorisation will be captured in the ServiceNow ITSM system or be captured in the OneGov Portal.

# 12. IDENTIFICATION AND AUTHENTICATION

## 12.1 Identification of users

Unique identification of ICT users ensures accountability and integrity. If users cannot be uniquely identified, access to information, modification and deletion of data, and inappropriate usage cannot be attributed to an individual. By uniquely identifying each user, the ACT Government reduces the likelihood of fraud, personal harm and harm to government reputation.

### Instructions

1. Business System Owners must ensure that all users are uniquely identifiable, and their identity is authenticated each time they access ACT Government ICT resources.
2. Business System Owners must ensure employees and contractors are positively identified before being authorised to access ACT Government ICT resources.
3. ACT Government will issue each employee and contractor with a unique user identity in accordance with the User Identity and Authentication Standard.
4. Business System Owners should ensure applications leverage the unique user identities provided by ACT Government to enable single sign-on and consistent security activities such as authentication, access control, and auditing.

## 12.2 Authorisation to use ICT resources

Employees and contractors may only be authorised to use ACT Government ICT resources while they are in the service of the ACT Government and have a need to know the information.

### Instructions

1. Business System Owners are the authority for approving access by any user to a business system. This authority may be delegated to the Business System Manager.
2. Business System Owners or their delegate must ensure that a user's access to ICT resources is removed when they no longer require access to a system, for example when employment is terminated, contract expired, the user is on leave for greater than 90 days or the user transfers to a different business area.
3. Business System Owners or their delegate should ensure ICT systems are configured to suspend a user's access after 90 days of inactivity. Exemption from this is by prior written approval of the Directorate CIO.
4. Proactive management of accounts is achieved by:
    a. Managers notifying DCBR when a staff member ceases employment.
    b. Administrative units ensuring that a similar process is applied to any cloud services which are not centrally managed via the ACT Government identity management services.
5. Administrative units should regularly review accounts created for use by vendors or for generic accounts, shared mailboxes etc.

## 12.3 Identity management federation

Cloud services that will be used by large numbers of users will be difficult for administrative units to manage identities, including provisioning and deprovisioning user accounts. Further, internal users may be tempted to re-use their ACT Government ICT credentials in an external system, which if compromised could expose ACT Government internal systems to attack.

### Instructions

1. Cloud services must, on a risk-assessed basis, leverage DCBR AD via identity management federation.
2. Cloud services should leverage DCBR AD via identity management federation when more than 50 users are present or when the service is shared across multiple administrative units.
3. Cloud services should leverage ACT Government's "Digital Account" Customer Identity and Access Management (CIAM) service when providing services to the public.
4. Cloud services which contain Sensitive Information must provide Multi-Factor Authentication.

## 12.4 Authentication of users

ICT systems that use weak methods of authenticating the identity of users are vulnerable to compromise.

### Instructions

1. ICT systems must enforce the password length and complexity, reset and re-use requirements of the Password Standard for all users.
2. ICT systems should not send authentication information including temporary passwords in clear text.
3. ICT systems should protect authentication information using ASD Approved Cryptographic Algorithms.
4. ICT systems should not store authentication information including temporary passwords in clear text, for example hard coded into an application or script.
5. Where passwords are stored in clear text, passwords must be changed on a frequent basis.
6. External systems (cloud services and ACT Government websites) should reset passwords using a tokenised reset mechanism.

## 12.5 Multi-factor authentication

Sensitive information requires extra levels of protection not provided by single-factor (password-based) authentication methods. Multi-factor authentication (MFA) provides this protection by strengthening authentication processes and reducing the impact of compromised credentials.

### Instructions

1. Multi-factor authentication must be used for remote access that provides access to any sensitive information or administrative capability.
2. Multi-factor authentication must be used for access to cloud services that provides access to any sensitive information or administrative capability.
3. Multi-factor authentication should be used for:
    a. system and database administrators
    b. privileged users
    c. positions of trust.
4. Multi-factor authentication for ACT Government infrastructure may be suspended temporarily by DCBR if the service is degraded or unavailable, when authorised by the ACT Government CISO (or delegate).

# 13. ACCESS CONTROL

## 13.1 Access to ICT systems and information

Access to ICT systems and information is granted in a manner that balances the business need for appropriate access to information with controls that prevent unauthorised access.

Access controls ensure the confidentiality, integrity, and availability of information and ICT resources for authorised personnel in a way that meets both business and security requirements.

### Instructions

1. Access to information and ICT resources must only be granted to employees and contractors who have been identified according to the requirements of the User Identity and Authentication Standard, and in accordance with the Acceptable Use Policy.
2. Access to information stored on or processed in application systems or storage devices will be based on the **need-to-know** principle.
3. Access to information and ICT resources must only be granted to employees and contractors who have been positively identified and deemed suitable to have access appropriate to their role.
4. ICT systems must have a formal user registration and de-registration procedure for granting and removing access to employees and contractors. The procedure should:
    a. cover all stages in the life cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services; and
    b. designate an appropriate agency officer to authorise the issuing of passwords and the creation of new accounts.
5. ICT systems must have access control rules and rights clearly documented for each user or group of users, and include the minimum provisions outlined in the User Identity and Authentication Standard, Password Standard, and Monitoring and Logging Standard.
6. User access rights to ICT systems should be reviewed at regular intervals and at least annually.
7. All detected unauthorised access to ACT Government information assets must be reported to the ACT CSC.
8. Unauthorised access to information is strictly prohibited and failure to comply with this policy will render the offender subject to disciplinary sanctions under the PSMA and other legislative instruments.

## 13.2 Privileged access

Privileged access is any level of access to ICT systems and information that grants permissions above ordinary users, e.g., to create, change, suspend or revoke other users' access.

Security controls for accounts with privileged access must be stronger than those for ordinary users.

### Instructions

1. Privileged access to ICT systems handling IMM information or higher must only be granted to employees and contractors who have a Baseline security clearance or equivalent.
2. Privileged access to ICT systems handling OFFICIAL (no IMM) information should only be granted to employees and contractors who have been vetted with a criminal record check. The ACT CSC may, on a risk-assessed basis, recommend security clearance at a higher level for sensitive and critical systems.

3. Business System Owners must ensure they, and anyone they delegate, can suspend or revoke privileges.
4. Privileged user access rights to ICT systems should be reviewed at regular intervals and at least every six months.
5. Privilege allocations must also be checked to ensure that unauthorised privileges have not been obtained.

## 13.3 Working offsite – employee remote access

ACT Government employees while performing their duties may be required to access the information assets of the ACT Government from home, remote locations, or while travelling. When working offsite, employees must continue to protect Territory information according to this policy.

### Instructions

1. ACT Government employees shall use only approved remote access facilities that have been authorised and/or provided by the ACT Government.
2. The use of non-approved methods of connectivity to the ACT Government ICT infrastructure will be deemed a violation of security with the offender being sanctioned under the PSMA and other appropriate legislation.
3. Employee authentication to the ACT Government network must comply with the User Identity and Authentication Standard.
4. If information is transferred to the remote device, then the remote device shall be secured in accordance with the ACT PSF.
5. Data in transit (wired or wireless communications) between the remote device and the ACT Government network must be protected according to Section 19 – Guidelines for Cryptography.

## 13.4 Vendor access to ICT systems

DCBR provides facilities for vendors to access the production environment to undertake emergency break fix support. These facilities are provided in accordance with least privileged access, with access to test and production environments strictly limited.

### Instructions

1. Only remote access methods endorsed by the ACT Government CISO shall be used to connect to ACT Government domains.
2. Authentication to the ACT Government network must comply with the User Identity and Authentication Standard.
3. Applications being accessed shall reside on server(s) owned exclusively by an administrative unit or the server(s) shall only support the application being accessed by multiple administrative units.
4. Vendor access must be supported by a Contract Agreement for services and include non-disclosure and confidentiality agreements that any support staff and subcontracting parties shall be bound by.
5. Directorates must ensure DCBR is notified when vendor access should be updated or terminated.
6. Vendor access requests must be requested through DCBR' Vendor Remote Access Request Form to ensure compliance with policy and security requirements.
7. Data in transit (wired or wireless communications) between the remote device and the ACT Government network must be protected according to Section 19 – Guidelines for Cryptography.

# 14. MONITORING, AUDITING AND ACCOUNTABILITY

## 14.1 Logging and monitoring

The purpose of logging and monitoring is to protect the operation of the ACT Government network and other assets, and to ensure compliance with the *ACT Public Sector Management Act 1994,* and ACT Government ICT policies.

Authorised users shall have no expectation of privacy in respect to their personal use of Internet, email, Instant Messaging (IM), social media and other ICT facilities and devices; however, using ICT facilities to collect, use or disclose personal information of others is subject to privacy laws and regulations.

### Instructions

1. DCBR must log and monitor the use of ACT Government ICT facilities and devices; non-ACT Government ICT facilities and devices when they connect to an ACT Government network; and the use of ACT Government ICT resources to access the Internet, email, IM, social media etc.
2. New technologies and facilities adopted by ACT Government must be risk-assessed to determine their monitoring and logging requirements.
3. Business systems should support ingestion of their logs into ACT Government security tools (i.e., ACT Government's Security Information and Event Management software).
4. Business System Owners are accountable for ensuring ICT system user and administrator activities are logged and that system alerts and network security events are logged by their service provider.
5. Activities that should be logged include:
    a. authorised access
    b. privileged access
    c. unauthorised access attempts
    d. system alerts or failures
    e. network security events.
6. Activities that must not be logged include:
    a. passwords
    b. sensitive information such as bank accounts or tax file numbers.
7. Logs for critical and Internet-facing systems should be centralised or forwarded to a secure central location for faster response to cyber security incidents.

## 14.2 Auditing

Non-compliance with the Cyber Security Policy puts the confidentiality, integrity, and availability of ACT Government ICT services, systems, and electronic information at risk. ACT Government uses compliance checking and auditing to identify non-compliance and reduce future incidents. Reducing non-compliance will reduce the risks to the environment.

The following audits are performed at regular intervals:

- Privileged access (conducted by the ACT CSC).
- Generic user accounts (facilitated by ICT teams and conducted by administrative units).

Other audits performed on an ad hoc or on demand basis include, but are not limited to:

- password complexity
- domain access – success and failure
- Internet/cloud service usage
- email usage
- network storage
- installed software.

Requests for audits and compliance investigations can be made by submitting a request in accordance with the Cyber Security Incident Response Plan.

### Instructions

1. Business System Owners are accountable for ICT system user and administrator activities and should - as determined by risk assessment - audit user access, access levels, and data changes to their ICT systems for anomalous behaviour indicating a security incident or decay in security posture.
2. The ACT Government CISO or their delegate shall:
    a. Provide security assurance reports to Directorates and the Security and Emergency Management Senior Officials Group (SEMSOG) on compliance across the ACT Government.
    b. Conduct authorised investigations into incidents of non-compliance with ICT policy.
    c. Assist authorised officers in the conduct of criminal and administrative investigations.
3. All audits will be conducted with due regard to the *Workplace Privacy Act 2011* (ACT).

# 15. MEDIA AND STORAGE

The storage of electronic records, information, or data is to be controlled. Some storage methods are unsuitable for Sensitive Information. The information classification scheme used by the ACT Government is defined in the ACT PSF, and its application is described in Information Security: Protective Markings.

The protection of classified records, information or data depending on the classification level is outlined in the ACT PSF.

## 15.1 Network drives and Storage Area Network (SAN)

Network drives such as your group drive (usually G: drive) and home drive (usually H: drive or OneDrive) are part of the publicly funded resources provided for official ACT Government business use.

Staff must not save unofficial information including software or large personal files to any network drive. These drives are monitored, and images, videos, music files, and executable files are reported to the ACT CSC.

Network and local drives, as well as Storage Area Networks (SAN), are not endorsed recordkeeping systems.

The appropriate use of network drives is described in the Acceptable Use Policy.

## 15.2 Local drives

Storing official information on local drives can place it at risk of being lost or inaccessible over time, because local drives are not regularly backed up like network drives and only the user can access the content. If the information is deleted, corrupted, or modified in an unwanted way, it cannot be recovered

to its previous “known good” state resulting in potential loss of corporate information and evidence of business.

Storing sensitive records, information and data on a local drive is discouraged and should only be done on occasions where there is a short-term working need. Users should not temporarily store sensitive information on a local drive without additional protection.

Storing Sensitive Information on the local drive of a mobile device like a laptop computer places it at higher risk. If the device is lost or stolen, someone who finds the device can potentially access the information.

## 15.3 Removable media

Users are discouraged from storing official information on removable media. If a user needs to store content temporarily for working purposes, they are responsible for its safekeeping and transfer to the administrative unit’s EDRMS.

Alternative data storage media options may be used for official business records once the content has been identified as records and captured in the current records management system. It is important to realise that once electronic records are transferred to another storage media it is no longer backed up or secured. The secure physical storage of alternative media is essential, particularly for data of a sensitive nature and should be disposed or deleted by an endorsed sanitisation and disposal method once the copy is no longer required.

Storing sensitive records, information and data on a removable media is discouraged and should only be done on occasions where there is a short-term working need. Users should not temporarily store Sensitive Information on removable media without additional protection.

Encryption of removable media may be required to protect Sensitive Information in certain circumstances. Encryption must be performed using an approved method that complies with Section 19 – Guidelines for Cryptography.

Only removable media from trusted sources should be used in ACT Government devices. Media from unknown sources must not be connected to ACT Government devices.

## 15.4 Storage in outsourced or cloud arrangements

The use of third parties to process, communicate, or store official information shall be treated as placing information into an untrusted environment. Examples of external environments include but are not limited to cloud services; externally hosted or maintained data centres; and personal devices either corporate or privately owned.

### Instructions

1. Official information may only be stored in outsourced arrangements including cloud services after a security risk assessment has been performed and the assessment has determined the outsourced arrangement both has a need to store this information and is appropriately secured for this storage.
2. Security risk assessments must comply with the Cyber Security Risk Management Standard.
3. The administrative unit’s Records Manager must be consulted to discuss records, information and data risks, before an outsourced storage arrangement is made.
4. The System Owner must approve the arrangement (accept residual risks) before official information is transferred from ACT Government.

## 15.5 Sanitisation and Disposal

ICT resources including mobile devices, laptops, workstations, servers, SANs, network devices, disposable media and portable media must be sanitised and disposed of in an appropriate manner to ensure that the

confidentiality of official information is not compromised. Sanitisation removes data from storage media, so that there is complete confidence the data will not be retrieved and reconstructed.

### Instructions

1. DCBR and administrative units must follow approved processes when ICT resources are no longer required. Contact the Service Assurance team for details.
2. Storage media must be sanitised according to Destruction of Data on Storage Media before it is reused for another purpose or disposed of.
3. Storage media must be destroyed on all assets being disposed of, in accordance with Destruction of Data on Storage Media.

# 16. CONTINGENCY PLANNING

## 16.1 Criticality and availability

ICT systems must be designed and maintained to provide a level of availability that supports the system's criticality to the business. Critical business systems and essential infrastructure must be designed and tested according to high availability principles.

### Instructions

1. Unplanned outages in ICT systems must be reported to Business System Owners and the DCBR ICT Service Desk.
2. Availability must be measured and reported to Business System Owners for critical business systems and essential infrastructure, including outsourced solutions and cloud services.

## 16.2 Data backup and restore

Electronic information is volatile in nature and to ensure that information is available in the event of disaster regular backups of the source information is needed.

To ensure the effectiveness of any backup regime, periodic restores of the backups are required. Failing to do so may result in critical data loss for ACT Government in the event of an erroneous or faulty backup.

Note: Backups are a disaster recovery mechanism and are not recognised as an archive under the *Territory Records Act 2002* (ACT).

### Instructions

1. All ICT systems handling official information must be backed up at least every business day, or more frequently on a risk-assessed basis
2. Backed up official information shall be restored and reviewed for completeness at pre-set intervals based on the criticality of the information and as detailed in the SSP.
3. All official information stored on backup media shall be restored in accordance with the Data Backup and Restore Standard.

## 16.3 Disaster recovery

Administrative units **must** prepare a Disaster Recovery Plan (DRP) for each critical ICT system to ensure it is able to recover from disasters ranging from physical (fire, flood, etc.) to logical (infrastructure failure, virus outbreak, etc.). Administrative units should prepare a DRP for each non-critical ICT system.

### Instructions

1. DCBR assists administrative units with developing DRPs for the critical business systems it hosts as part of the solution design process. DCBR must meet the requirements of the ACT PSF for the protection of ACT Government ICT resources in providing this service.
2. Administrative units should use a methodology and template provided by DCBR to prepare DRPs for non-DCBR systems.
3. Business System Owners should test their DRPs before a system goes into production, and annually thereafter.
4. Business System Owners must file their DRPs in their administrative unit's recordkeeping system.
5. DCBR should keep a copy of DRPs in a central offsite location such as the ICT inventory system.
6. DCBR should keep a copy of DRPs in an alternate onsite location.

## 16.4 Business continuity

The ACT Government must address business continuity and disaster recovery to minimise the impact of incidents on the operations of ACT Government information management systems.

Administrative units including DCBR must develop and regularly test a Business Continuity Plan (BCP) to reduce the organisation's exposure to threats and hence reduce the risks associated with loss of critical information, personnel, facilities, and ICT infrastructure.

### Instructions

1. Administrative units must establish procedures to develop and maintain BCPs that include:
    a. a continuity strategy consistent with business objectives and priorities.
    b. a relationship to ICT system SSPs and DRPs.
    c. a continuous improvement cycle for BCPs.
    d. incorporation of the BCP process within administrative units.
2. At a minimum, BCPs must cover critical ICT systems used by the administrative unit, including those shared with other administrative units.
3. BCPs should also cover non-critical ICT systems, on a risk-assessed basis.
4. Administrative units must file BCPs as a record in their administrative unit's recordkeeping system.
5. ASAs should keep a copy of current BCPs in an alternate offsite location.

# 17. SYSTEM AND COMMUNICATIONS PROTECTION

## 17.1 Network segregation

Non-production ICT environments used for software development, etc. are characterised by flexible access control, patch levels and other security controls. They are more vulnerable to malicious code and insider threats and must be segregated from the production environment.

### Instructions

1. Non-production ICT environments must be segregated from production ICT environments using approved methods and technologies.
2. New development and modification of software should only take place in a development environment.

3. Non-production environments must be commensurate to the same level of security as the production environment if they are to handle Sensitive Information.

## 17.2 Production data release

Sensitive data should only be stored or transmitted in production environments. DCBR Cyber Security acknowledges that there are a range of scenarios where production data is used in non-production environments to achieve optimal outcomes for business.

Once the data is no longer required in the non-production environment, it must be destroyed.

### Instructions

1. Official information should not be handled by non-production ICT environments unless explicitly permitted by the Business System Owner. Business System Owners should provide this approval using the Production Data Release form in the Production Data Release Standard.
2. Development environments are inherently less secure and must not be used to handle personal or sensitive information.
3. Sanitised information may be used in lower environments when the sanitisation method used is endorsed by DCBR Cyber Security. Sanitisation methods are used to depersonalise personal details and/or reduce the sensitivity/classification of official information to OFFICIAL (no IMM).
    a. DCBR Cyber Security does not endorse sanitisation methods based on “shuffling” real data. Research has established that this method is insecure, as the moved data can easily be reassociated by inference, probability, matching against other datasets, etc.
4. Dummy data should be used in lower environments in preference to official or personal information. Dummy data is mock information (fictitious names, contact details, etc) that does not contain any real data but serves to reserve space or enable functionality where real data would nominally be present.
5. When engaging external ICT and cloud service providers, Business System Owners should ensure they are prohibited by written agreement from using official information in non-production ICT environments outside the direct control of ACT Government.
6. Business System Owners must satisfy themselves that they are in compliance with legislation such as the *Information Privacy Act 2014* (ACT) and other enactments of secrecy, and should seek legal advice where legislation applies to their intended re-use of production data.

## 17.3 Gateway security

The interface between the ACT Government network and the Internet (including all other external network connecting services) will be protected by a gateway. A gateway is a network point that acts as an entrance to another network.

The gateway environment includes demilitarized zones (DMZs). A DMZ is a perimeter network to house public services that is maintained outside of the internal/protected network. Since a DMZ is usually open to allow public access to services, it is exposed to more threats than the internal/protected network.

DCBR will manage all activity within the gateway so as not to breach security and allow unauthorised access between the Internet and the internal network.

### Instructions

1. All ACT government internet gateways must be secured using controls that comply with the ISM Gateway guidance.
2. All servers deployed to the gateway environment must be built in accordance with the Server Build Policy.

3. All applications must undergo Security vulnerability assessment or be formally exempted prior to entering production.
4. All changes to gateways are to be authorised prior to implementation by Change Management.

## 17.4 Secure data transfers

Data transfers between ACT Government and external systems such as cloud services must be performed securely, according to the sensitivity of information transferred and the criticality of the system.

### Instructions

1. Use secure data transfer methods that comply with Section 19 – Guidelines for Cryptography.
2. Physical transfer via encrypted media or physical safehand if encryption to Section 19 – Guidelines for Cryptography is not possible.
3. Use Application Programming Interfaces (API) that meet security standards approved by DCBR Cyber Security.
4. API-led data transfers between internal systems should be handled by a centrally governed and administered API Gateway.
5. API-led transfers between internal and external systems, or between external systems, should be handled by a centrally governed and administered API Gateway.

## 17.5 Use of web presence for delivery of ACT services

ACT Government domain names are typically those ending with .act.gov.au, but may also include .act.edu.au and others. DCBR administers .act.gov.au domain names on behalf of ACT Government administrative units.

### Instructions

1. Domain name registration requests must be approved by the administrative unit's Director-General or Executive Delegate.
2. Domain names must be registered with a Registrant Contact Position (an employee of the administrative unit).
3. DCBR as the Domain Provider reserves the right to remove the domain from the registry if it is in breach of .gov.au policies or the Registrant Agreement.
4. DCBR has the right to reject an application for a domain name.
5. Domain name registrations must be reviewed by system owners in accordance with the Australian Government Domain Name Policy (every 2 years as at 17 February 2022).

## 17.6 Configuration of email services

ACT Government relies on email to correspond internally and externally. Some areas of business are highly reliant on email to deliver critical services. The common email service provided by DCBR must be protected according to the highest level of sensitivity and criticality required by administrative units. Business systems must be integrated with ACT Government email in a way that does not reduce this security posture.

Administrative units should comply with best practice security controls for email services, including:

- Sender Policy Framework (SPF) – a DNS name record that advertises the authorised mail senders for a specific mail domain.

- DomainKeys Identified Mail (DKIM) – a method of cryptographic signing of emails that a recipient mail server interrogates to determine the trust in the message origin or proving tampering of a message.
- Domain-based Message Authentication, Reporting, & Conformance (DMARC) – an extension of SPF and DKIM which provides for additional policy control, where an organisation can assert how they wish SPF and DKIM failures to be handled and enables reporting on deliverability of messages from a domain.

### Instructions

1. All parties sending email from a registered act.gov.au domain or subdomain must:
    a. Provide support for SPF or DKIM or both.
    b. Comply with publishing a DMARC record, which DCBR will provide.
    c. When unable to comply, seek a waiver when using a subdomain dedicated to the system or business function.
2. DCBR Cyber Security and embedded ICT teams will assist third parties to correctly use email authentication protocols, including making any necessary changes to DCBR managed systems.
3. Business System Owners should migrate to a dedicated mail subdomain if they cannot support email authentication.
4. DCBR will provide DMARC reporting and forensics capability to assist in SPF, DKIM, and alignment.
5. All domains that send no mail will have default SPF and DMARC records created that indicate no mail is expected from the domain and a policy of REJECT.

# 18. SYSTEM AND INFORMATION INTEGRITY

## 18.1 Source code management

Source code - like any information asset of the Territory - must be managed securely, not just for the protection of the code, but for the protection of other information assets handled by the code.

### Instructions

1. Repositories for ACT Government code or vendor code held in escrow must be registered with DCBR and recorded in the CMDB.
2. Repositories must be operated by the ACT Government or by a third party with which the ACT Government has a written agreement with. Written agreements must specify that no other party can be given access to the repository without written consent from the ACT Government.
3. Repositories operated by a third party must be governed under a written agreement that ensures the ACT Government has irrevocable access to the repository and its associated artefacts, as well as ownership of any records, information, or data.
4. Repositories must implement a mechanism to allow the ACT Government to have full control of the access levels in the repository.

## 18.2 Secure programming

ACT Government business systems that are exposed to the wider range of threats from the Internet should be developed using secure coding, code review, and testing practices provided by the Open Web Application Security Project (OWASP).

### Instructions

1. DCBR should adopt and promulgate OWASP standards for secure coding, code review and testing practices for all bespoke business systems.
2. DCBR Cyber Security will reduce the likelihood of relevant security risks when assessing websites, cloud services, and mobile applications that comply with OWASP standards.

## 18.3 Secure platforms

ICT platforms (e.g., web servers, application servers, databases) must be configured securely according to the controls of the ASD Information Security Manual and should also be configured in accordance with the advice of the platform vendor and industry sources of best practices such as the Centre for Internet Security (CIS) Security Benchmarks.

### Instructions

1. DCBR should adopt and promulgate CIS Security Benchmarks for all server builds.
2. DCBR Security will take into account CIS compliance when assessing relevant security risks of ICT platforms.

## 18.4 Secure desktops

While no single mitigation strategy is guaranteed to prevent cyber security incidents, ACT Government implements eight essential mitigation strategies recommended by the ASD as a baseline. This baseline, known as the Essential Eight - makes it much harder for adversaries to compromise systems. Furthermore, implementing the Essential Eight pro-actively is more cost-effective than responding to a large-scale cyber security incident.

DCBR configures ACT Government desktops (including laptops and cloud services providing “desktop as a service”) securely using the Essential Eight and in accordance with the advice of the platform vendor. The attack surface and accumulation of vulnerabilities of the ACT Government desktop is also limited by central management of non-standard applications by DCBR.

### Instructions

1. ACT Government should adopt and promulgate Windows security baselines for all desktop builds.
2. ACT Government must implement centrally managed, automatically updated malware protection on corporate devices including workstations, laptops and mobile devices.
3. ACT Government must implement standard desktops on behalf of administrative units that support the ASD’s “Essential 8” mitigations, particularly regarding:
    a. Office macro security.
    b. Application whitelisting.
    c. Removal or hardening of Java, Flash, and other programs that weaken desktop security
    d. Restrict administrative privileges.
4. End users must not install non-standard applications without prior written approval from an appropriate governance body that includes DCBR Cyber Security.
5. Technical staff should not be able to install non-standard applications without central deployment.

## 18.5 Patch management

Business System Owners are accountable for the patching of ICT systems in accordance with the recommendations of software vendors.

### Instructions

1. Business System Owners must ensure patches or alternative remediations are compliant with Essential 8 maturity level 1 for 'patch applications' and 'patch operating systems' for all ICT systems. Essential Eight Maturity Model | Cyber.gov.au
2. DCBR will assist Business System Owners with a patch management framework for hosted ICT systems.
3. Business System Owners must gain assurance, determined by risk assessment and enforced by contract terms, that cloud service providers patch their applications and underlying ICT systems throughout the life of a cloud service through the governance, risk management, and compliance auditing process.

## 18.6 Vulnerability management

The ACT Government will - according to an ICT system's assurance level, perform - VAs to identify security weaknesses caused by misconfiguration, bugs, age or design flaws.

### Instructions

1. Externally hosted or externally exposed business systems, including cloud services and websites, must be vulnerability assessed if they meet the criteria for security risk assessment.
2. A VA or penetration test by an independent third party may meet the requirement to undertake a VA, subject to the provision of suitable evidence and a quality assurance review by DCBR Cyber Security.
3. Initial VAs must be completed, and any extreme-risk vulnerabilities identified, must be remediated before the system goes live, and before any official information is transferred to the system.
4. DCBR Cyber Security will monitor new information from a variety of government and industry sources on emerging security vulnerabilities and threats to ICT resources.
5. Ongoing vulnerability management in the form of automated vulnerability scanning and/or patching may be performed throughout the life of DCBR-hosted ICT systems to maintain security in the face of emerging vulnerabilities and threats.
6. Externally facing DCBR managed websites must be automatically audited at least daily by DCBR as they are historically more vulnerable to compromise.
7. DCBR Cyber Security will analyse identified vulnerabilities to determine their potential impact and advise Business System Owners of appropriate treatments.
8. Business System Owners must ensure the advised treatments are implemented on a risk-assessed basis agreed with the CISO or their delegate.

## 18.7 Reporting and disclosure of vulnerabilities

ACT Public Service staff and contractors must report identified security vulnerabilities directly to DCBR Cyber Security. Security researchers not employed or contracted to ACT Government are encouraged to report vulnerabilities in government systems to DCBR Cyber Security or through the Business System Owner or delegate who is then required to report this to DCBR Cyber Security.

### Instructions

1. Vulnerabilities should be reported to the ACT Government following the process outlined at Report a system security vulnerability - ACT Government.
2. Reports should include:

a. date the vulnerability was observed

b. location of the vulnerability (e.g. URL, domain etc)
c. an explanation of the potential security vulnerability
d. a list of products and services that may be affected (where possible)
e. steps to reproduce the vulnerability
f. prior conditions (e.g. logged in, not logged in, previous actions etc) where applicable
g. proof-of-concept code (where applicable)
h. names of any files that were uploaded to our systems
i. the names of any test accounts you have created (where applicable)
j. if you would like public acknowledgement for your contribution and what name to publish.

3. Security researchers may make public (disclose) vulnerabilities 90 days after reporting to ACT Government, unless otherwise agreed by both parties.
4. ACT Government may acknowledge discovery of vulnerabilities but does not pay bug bounties.

# 19. GUIDELINES FOR CRYPTOGRAPHY

Cryptography is used to encrypt information and data to provide additional assurances to their security. When information is appropriately encrypted, the likelihood of the encrypted information being accessed by unauthorised parties is considered to be lower. This enables a reduction in handling, storage and transmission requirements.

The purpose of cryptography is to provide confidentiality, integrity, authentication and non-repudiation of data. In doing so:

- confidentiality protects data by making it unreadable to all but authorised entities,
- integrity protects data from accidental or deliberate manipulation by entities,
- authentication ensures that an entity is who they claim to be, and
- non-repudiation provides proof that an entity performed a particular action.

## 19.1 Cryptography Standards

The ACT Government aligns with the Australian Signals Directorate (ASD) Information Security Manual's (ISM) Guidelines for Cryptography. Business areas should ensure their suppliers are aware of, and compliant (preferably through contractual clauses) against, ISM controls for cryptography and supply updates in alignment with updates that are made in the ISM. Regularly check the ASD website to ensure they are aligned with the latest version of the ASD ISM cryptography control standards.

Instructions

1. All new systems will be required to meet the ASD ISM cryptography control standards.
2. All new systems will be assessed and managed through the ACT Government Vulnerability Management Standard and the ACT Government Change and Release Management Policy.

## 19.2 Life Cycle Management

Cryptography controls will be managed throughout the life cycle of a business system. Compliance with the national standards will vary throughout the life cycle of existing business systems. Management of the risks associated with this will be managed according to the level of risk and criticality.

Instructions

1. Where an existing business system has **secure** cryptography that is not currently in compliance with the national standards the risks will be managed within existing government guidelines and standards.
2. Where critical issues in cryptography are identified and require remediation these will be managed in line with the ACT Government Vulnerability Management Standard.
3. Existing systems that undergo significant change, in alignment with the ACT Government Change and Release Management Policy, will be required to update cryptography to meet the national standards.

## 19.3 Cryptographic Bill of Materials (CBOM)

Cryptographically relevant quantum computer (CRQC) refers to the expectation that quantum computing will have the capability to compromise current public-key encryption, threatening systems like HTTPS, digital signatures, and secure communications. Whilst projections for this type of computing becoming relevant are typically expected to be beyond 2035, additional risks exist today for "harvest now, decrypt later" attacks, where threat actors store encrypted data to decrypt it in the future when the capability exists.

A Cryptographic Bill of Materials (CBOM) is a structured inventory that describes all cryptographic assets in a software system and their relationships. By providing a detailed inventory of cryptographic assets, it enables better risk management, compliance and preparation for future cryptographic challenges, particular in the context of emerging threats such as quantum computing. The CBOM will help ensure identification and prioritisation of moving to safe, ASD approved post-quantum cryptography.

In line with recognised best practice, ACT Government will work towards developing a Cryptographic Bill of Materials.

Instructions

1. Directorates should include cryptography assets in design documents and include them in Configuration Management Database entries to assist in the future development of a CBOM.

## 19.4 Application of Cryptography

Cryptographic controls are applied to systems according to the classification of the information they handle, their operating context, and the protective environment of the data ‘at rest’ or ‘in transit’. Systems **must** comply with the controls (indicated in red) or **should** comply with the controls on a risk-assessed basis (indicated in amber), depending on the combination

***Table 1: Application of ASD Approved Cryptographic Algorithms (AACA) and ASD Approved Cryptographic Protocol (AACP) controls.***

| **Data Category** | 1. **External location (for example public facing DMZ networks) or**<br>2. **portable device, or**<br>3. **Mixed vendor ACT Government networks (BMS, MED-DEV) etc** | **Trusted ACT Government internal networks** |
|---|---|---|
| Public data | SHOULD COMPLY | SHOULD COMPLY |
| OFFICIAL | SHOULD COMPLY | SHOULD COMPLY |
| Aggregated OFFICIAL | SHOULD COMPLY | SHOULD COMPLY |

| | | |
|---|---|---|
| IMM (e.g. Sensitive) | MUST COMPLY | SHOULD COMPLY |
| Aggregated IMM | MUST COMPLY | SHOULD COMPLY |

# 20. INCIDENT RESPONSE

For the purposes of the ACT Government Cyber Security Framework:

- **Cyber Security Event** is an identified occurrence of a system, service or network state indicating a possible breach of the Cyber Security Policy, or a failure of controls, or a previously unknown situation that may be relevant to security.
- **Cyber Security Incident** is a single or series of unwanted to unexpected cyber security events that have a significant probability of compromising business operations and threatening information security.

## 20.1 Incident response and investigations

The purpose of establishing critical response and incident reporting processes is to ensure that the government has critical services available to withstand, or quickly recover from, incidents.

Administrative units must have in place Critical Response and Incident Reporting procedures to manage incidents occurring within critical ICT systems. Administrative units should consider applying this policy to non-critical ICT systems on a risk-assessed basis.

The ACT CSC provides investigation and digital forensic services to ensure only qualified investigators are involved and ensures that any chain of evidence is maintained.

### Instructions

1. Business System Owners must establish an incident reporting procedure for their ICT systems.
2. Critical response and incident reporting must comply with established administrative unit procedures, e.g. fraud control.
3. Where the incident involves a government system, the ACT CSC must be notified, kept informed of developments, and involved with resolution of the incident.
4. Incident response and reporting must comply with the Cyber Security Incident Response Plan.
5. The logging of system and security events for all ICT systems must comply with the Monitoring and Logging Standard.
6. Investigations and forensic analysis will only be conducted by the ACT CSC.

## 20.2 Notification of data breaches

ACT Government is not an APP Entity under the *Privacy Act 1988* (Cth) and is governed by the *Information Privacy Act 2014* (ACT) and *Health Records (Privacy and Access) Act 1997* (ACT). These laws do not require mandatory data breach notifications, although other Commonwealth laws such as the *Taxation Administration Act 1953* (Cth) (re Tax File Numbers) require compliance.

From 1 July 2024, the ACT Human Rights Commission includes the ACT Information Privacy Commissioner who administers the ACT Information Privacy Act

The ACT Information Privacy Commissioner has a number of functions under the *Information Privacy Act 2014* (ACT), including handling privacy complaints against Territory agencies and providing guidance about compliance with Territory Privacy Principles.

The information privacy functions will complement other complaint handling functions of the ACT Human Rights Commission, which from June 2024 include handling complaints regarding breaches of human rights by public authorities, including the right to privacy.

The ACT Human Rights Commission is the contact for ACT agencies seeking guidance about the *Information Privacy Act 2014* and the obligations of Government under this Act.

The ACT Government is committed to transparency and protection of the public interest and should provide notification of data breaches. Administrative units may develop their own data breach plans to implement this policy including voluntary notification of data breaches to the ACT Information Privacy Commissioner.

**Instructions**

1. Data breaches must be reported as security incidents to the ASA and data breaches in ICT systems and cloud service providers must be reported to ACT Cyber Security Centre.
2. Business System Owners are responsible for assessing a suspected data breach to determine its likely impacts. Privacy officers or ACT Cyber Security Centre can provide technical assistance on request.
3. Business System Owners must make the Director-General completely aware of all information in relation to the breach via their delegated Executive Data Lead.
4. With the approval of the relevant Director-General, the administrative unit should notify any individuals whose personal information is involved in a data breach of their ICT systems, where the breach may result in harm including (but not limited to):
    a. Physical
    b. Psychological
    b. Reputational
    c. Financial.
5. With the approval of the relevant Director-General, Business System Owners should provide guidance to affected individuals about the steps they should take in response to the breach, such as:
    a. Identity protection measures
    b. Advice to financial institutions, customers, etc.
6. With the approval of the relevant Director-General, Business System Owners should notify the ACT Human Rights Commissioner using the Make a Complaint Form or via email to hrcintake@act.gov.au. Statements must include:
    a. the System Owner of the ICT system and contact details
    b. a description of the data breach
    c. the kinds of information concerned, and
    d. the guidance provided to affected individuals in response to the data breach.
7. The ACT Information Privacy Commissioner is empowered to request information from Business System Owners if there is a reasonable belief that a government system (including cloud services) is involved in a data breach.

8. Any breaches of privacy under the Commonwealth *Privacy Act 1988,* such as data breaches involving tax file numbers, should be directed to the OAIC. Information on notifiable data breaches under the Commonwealth *Privacy Act 1988* can be found on the OAIC website here.

## 20.3 Payment of ransomware demands

Ransomware attacks involve Cyber criminals encrypting files and demanding payment for their release. Ransomware is a popular form of attack by Cybercriminals which can disrupt operations, breach sensitive information, and cause reputational damage. Cybercriminals using ransomware pose a significant risk to Australia, ACT Government, and Canberrans.

ACT Government does not condone the payment of a ransom to Cybercriminals. Payment does not offer a guarantee that data encrypted in ransomware will be decrypted by the attacker and is likely to attract further attacks from cybercriminals seeing a soft target. Administrative units are best protected by ensuring their ICT systems comply with the Cyber Security Policy, keeping regular offline backups of critical data, and implementing the ASD Essential 8 security controls.

### Instructions

1. Ransomware attacks must be reported as security incidents to the ASA, Directorate CIO, and the ACT CSC.
2. Business System Owners must forward reports of ransomware attacks from service providers entrusted with official information to the ACT CSC so that the security incident can be assessed.
3. Ransomware attacks may exfiltrate personal information which constitutes a notifiable data breach and must be assessed and reported as such by the Business System Owner to the ACT CSC.
4. The ACT Government position is to not pay ransomware.
5. Business System Owners must not communicate with the purported cyber-criminals responsible for the ransomware. If there are any extraneous circumstances that would justify contact, any intended communications must be brokered between the ACT CSC, the Directorate, and a law enforcement agency.
6. Administrative units should take steps to build workforce awareness of ransomware and other malware threats as awareness is an important line of defence.
7. For DCBR managed environments/cloud applications, the ACT CSC must notify the ACSC of ransomware attacks and seek assistance if required. For customer managed environments/cloud applications, the ACT CSC will advise the directorate CIO and Business System Owner on ACSC incident reporting protocol, as this may be performed by the Business System Owner's service provider.
8. Restoration of external services from backup and other mechanisms should occur under guidance from the ACT CSC to validate the suitability of remediation, incident resolution, and cyber safety of resuming operations.

**NOTE:** The ACT CSC, the ACSC, and most cyber security providers, will **not** be able to provide you with a decryption key.

# APPENDIX A: ASSOCIATED DOCUMENTS

The following ACT Government documents are part of the Cyber Security Framework that supports this Cyber Security Policy:

| Reference | Policy Section |
|---|---|
| ACT Protective Security Framework | Information Classification; Physical security of ICT resources; Ownership of ICT systems |
| Risk Management Tools | Security risk management |
| **ACT Government ICT Technology Reference Manual** | Network segregation |
| Acceptable Use Policy | Acceptable use of ICT resources; Stolen, lost or damaged ICT resources; Access to ICT systems and information |
| ACTPS Recordkeeping Maturity Model and Compliance Checklist | Protecting records, information and data |
| API-led Connectivity Standard | Secure data transfers |
| Service Assurance | Sanitisation and Disposal |
| Records by Design | Protecting records, information and data |
| Security Clearances | Security Clearances |
| Cyber Security Incident Response Plan | Security Operations; Auditing; Incident response and investigations |
| Destruction of Data on Storage Media | Sanitisation and Disposal |
| DCBR Change and Release Process | Configuration management policy and procedures |
| ICT Incident Management Fact Sheet | Incident response and investigations |
| ICT System Criticality Standard | Physical security of ICT resources; Registration and inventory of ICT systems; Criticality and availability |
| ICT Policy Waiver Procedure | Policy waivers |
| Information Classification Scheme | Information Classification; Registration and inventory of ICT systems |
| Information Privacy (CMTEDD Intranet) | Personal information |
| Information Security Assessment **template** | Information Classification; Personal information |
| Report lost or stolen ICT devices - Digital Canberra<br>Report damaged ICT devices - Digital Canberra | Stolen, lost or damaged ICT resources |
| Monitoring and Logging Standard | Access to ICT systems and information; Logging and monitoring; Auditing; Incident response and investigations |
| Password Standard | Authentication of users; Access to ICT systems and information |
| Privileged Accounts Policy | Privileged access |

| | |
|---|---|
| Production Data Release Standard | Production data release |
| Procuring ICT Services - Digital Canberra | Procurement of ICT systems |
| Secure Technology Procurement Toolkit - Digital Canberra | Procurement of ICT systems |
| Cyber Security Risk Management Standard - Digital Canberra | Criteria for security risk assessment; Security authorisation; Storage in outsourced or cloud arrangements |
| Vulnerability Management Standard<br>Vulnerability Management Plan – Microsoft Windows Server | Vulnerability management |
| Server Build Policy | Gateway security |
| Source Code Management Policy | Source code management |
| Add or update a business application or website in the CMDB - Digital Canberra | Registration and inventory of ICT systems |
| User Identity and Authentication Standard | Identification of users; Access to ICT systems and information; Working offsite – employee remote access; Vendor access to ICT systems |
| Vendor Remote Access Request Form | Vendor access to ICT systems |

Applicable legislation includes, but is not limited to:

| Reference | Policy Section |
|---|---|
| *Criminal Code 2002* (ACT) | *General references* |
| *Electronic Transactions Act 2001* (ACT) | *General references* |
| *Freedom of Information Act 2016* (ACT) | *General references* |
| *Health Records (Privacy and Access) Act 1997* (ACT) | Protecting records, information and data; Personal information; Notification of data breaches |
| *Information Privacy Act 2014* (ACT) | Personal information; Logging and monitoring; Production data release; Notification of data breaches |
| *Insurance Authority Act 2005* (ACT) | *General references* |
| *Public Sector Management Act 1994* (ACT) **(PSMA), including** Public Sector Management Standards | *General references* |
| Security of Critical Infrastructure Act 2018 - Federal Register of Legislation | *General references* |
| *Taxation Administration Act 1953* (Cth) | Notification of data breaches |
| Territory Privacy Principles<br>Territory Privacy Principles Quick Reference - HRC | Personal information |

| | |
|---|---|
| ***Territory Records Act 2002* (ACT)** | Protecting records, information and data |
| ***Workplace Privacy Act 2011* (ACT)** | Acceptable use of ICT resources; Logging and monitoring; Auditing |

The following non-ACT Government documents support our Cyber Security Framework:

| Reference | Policy Section |
|---|---|
| **Australian Government Domain Name Policy** | Use of web presence for delivery of ACT services |
| **Australian Government Information Security Manual** | Gateway security; *General references* |
| **Australian Government Ransomware Action Plan 2021** | Payment of ransomware demands |
| **Centre for Internet Security (CIS) Security Benchmarks** | Secure platforms |
| **ISO/IEC 27001 – Information Security Management** | *General references* |
| **NIST Cyber Security Framework** | *General references* |
| | |
| **Ransomware \| Cyber.gov.au** | Payment of ransomware demands |
| **What is personal information? (OAIC)** | Personal information |
| **Windows security baselines** | Secure desktops |
| **Payment Card Industry Data Security Standard** | PCI-DSS compliance |

# APPENDIX B: MAPPING TO STANDARDS

| Policy chapter | NIST 800-53 families | ACSC ISM guidelines | ISO 27001 domains |
|---|---|---|---|
| **Responsibilities** | PM - Program Management | Cyber Security Roles | Organisation of information security |
| **ICT security program** | PM - Program Management | Cyber Security Principles | Information security policies |
| **Information security** | No applicable advice | No applicable advice | Compliance |
| **Security awareness and training** | AT - Awareness and Training | Personnel Security | Human resource security |
| **Personnel security** | PS - Personnel Security | Personnel Security | Human resource security |
| **Physical and environmental protection** | PE - Physical and Environmental Protection<br>MA - Maintenance | Physical Security | Physical and environmental security |
| **System and services acquisition** | SA - System and Services Acquisition | Evaluated Products<br>ICT Equipment Management | System acquisition, development and maintenance |
| **Governance, compliance and risk management** | PL – Planning<br>RA - Risk Assessment<br>CA - Security Assessment and Authorization | Outsourcing<br>Security Documentation | Supplier relationships |
| **Configuration and change management** | CM - Configuration Management | System Management | Asset management |
| **Identification and authentication** | IA - Identification and Authentication | System Management | Access control |
| **Access control** | AC - Access Control | Personnel Security | Access control |
| **Monitoring, auditing and accountability** | AU - Audit and Accountability | System Monitoring | Operations security |
| **Media and storage** | MP - Media Protection | Media Management | Asset management |
| **Contingency planning** | CP - Contingency Planning | System Management | Information security aspects of business continuity management |
| **System and communications protection** | SC - System and Communications Protection | Communications Infrastructure<br>Communications Systems<br>Network Management<br>Enterprise Mobility<br>Using Cryptography<br>Gateway Management<br>Data Transfers and Content Filtering | Operations security<br>Communications security<br>Cryptography |
| **System and information integrity** | SI - System and Information Integrity | System Hardening<br>Software Development<br>Database Systems Management<br>Email Management | System acquisition, development and maintenance |
| **Incident response** | IR - Incident Response | Cyber Security Incidents | Information security incident management |

# GLOSSARY

| Term | Definition |
|---|---|
| **Active Directory (AD)** | A Microsoft directory service for Windows domain networks but can refer to a broad range of directory-based, identity-related services. Provides authentication and authorisation capabilities for a Windows domain. |
| **Administrative unit** | Any ACT Government directorate, agency or statutory authority. |
| **Agency Security Advisor (ASA)** | Responsible for day-to-day management of the protective security measures within the administrative unit. Develops, implements, and monitors administrative unit security procedures and systems. Analyses the administrative unit's security environment and posture, and plans measures to manage security risks. |
| **Agency Security Executive (ASE)** | The delegate of the Director-General or agency head with authority to approve protective security programs for their administrative unit. |
| **Authentication** | The process of confirming the correctness of the claimed identity. |
| **Availability** | The state when data is in the location needed by the user, at the time the user needs them, and in the form needed by the user. |
| **Business Continuity Plan (BCP)** | A plan designed to allow continuity of function by a business area or ICT system in the event of interruption, failure, disaster etc. |
| **Business System Administrator** | An ACTPS officer with access privileges, knowledge, and skills necessary to administer the day-to-day operation of the ICT system. Applies access levels, manages system configuration, and adds/changes/removes/suspends user access. |
| **Business System Manager** | An ACTPS officer who is responsible for the integrity and operation of the ICT system; negotiates service levels; authorises access levels and access for all new users including staff, contractors, vendors and volunteers; and reviews audit logs. |
| **Business System Owner** | Person at executive or senior executive level within an administrative unit who has the authority to make binding financial and operational decisions regarding an ICT system, and to accept residual risk on behalf of the Director General. |
| **Chief Digital Officer (CDO)** | Responsible for driving the ACT's digital agenda and leading the whole of government strategic direction for ICT. |
| **Chief Information Officer (CIO)** | Executives in each administrative unit responsible for ICT services. May also be System Owners of administrative unit ICT systems and infrastructure. |
| **ACT Government Chief Information Security Officer (CISO)** | The position of ACT Government Chief Information Security Officer (CISO). A WhoG role that manages the strategic direction of cyber security for ACT Government and the implementation and operation of WhoG cyber security measures. |
| **Confidentiality** | Ensuring that information is accessible only to those authorised to have access. |

| | |
|---|---|
| **Configuration Item (CI)** | ICT components that are to be tracked in ACT Government's CMDB. Further information is available under 'configuration items to be managed'. |
| **Configuration Management Database (CMDB)** | A database of record for ICT components (CIs), used to track them through stages of change management, and over their lifecycle. |
| **Critical system** | A system that requires extra measures to protect is availability due to business impacts of an unplanned outage. |
| **Data integrity** | Information in a condition in which it has not been altered or destroyed in an unauthorised manner. |
| **Disaster Recovery Plan (DRP)** | A plan designed to allow recovery of a business area function or ICT system following a disaster. |
| **EDRMS** | Electronic Document Records Management System |
| **Encryption** | The process of transforming information using an algorithm or cipher to make it unreadable to anyone except those possessing the key. |
| **Personal Health Information** | From the *Health Records (Privacy and Access) Act 1997* (ACT) dictionary:<br>Personal Health information, of a consumer, means any personal information, whether or not recorded in a health record—<br>a. Relating to the health, an illness or a disability of the consumer; or<br>b. Collected by a health service provider in relation to the health, an illness or a disability of the consumer. |
| **ICT Asset** | Any physical or logical computing device either owned, leased, or used by the ACT Government to store, process or communicate ACT Government electronic information. |
| **ICT System** | Any system used by the ACT Government to store, process or communicate ACT Government electronic information. Includes, but is not limited to, DCBR hosted systems, external cloud services and outsourced ICT solutions. |
| **Information Owner** | The originator of a piece of information (i.e., the staff member who wrote an email or document). |
| **Penetration Test** | A test wherein a party (with permission) attempts to breach an ICT system. Aims to identify weaknesses and vulnerabilities in a system's defences. |
| **Permitted services** | ICT systems that have not been assessed for security risk, but access to them via ACT Government networks or corporate devices is still permitted. |
| **Personal Information** | From the *Information Privacy Act 2014* (ACT) s 8:<br>Means information or an opinion about an identified individual, or an individual who is reasonably identifiable—<br>i. Whether the information or opinion is true or not; and<br>ii. Whether the information or opinion is recorded in a material form or not; but |

| | |
|---|---|
| | Does not include personal health information about the individual. |
| **Remote access** | The ability to get access to a computer or a network from an external location. An external location being a premise not controlled or maintained by the ACT Government. |
| **Sanctioned services** | ICT systems that have been assessed for security risk and treated appropriately. |
| **Secure environment** | An environment the Information Owner assesses as not posing a significant risk to the confidentiality of the information. |
| **Secured** | Physically protected for example locked in a safe. Information can be logically protected by implementing encryption when physical controls are inadequate. |
| **Secured connection** | Encompasses a physical connection that provides the required level of protection for the information travelling across the connection and encryption in accordance with Section 19 Guidelines for Cryptography where the physical connection fails to provide the appropriate level of protection. |
| **Sensitive Information** | Official information that requires extra measures for protection, classified and marked with an Information Management Marker according to the ACT Government Information Security Guidelines. |
| **Sensitive Personal Information** | From the definition of 'sensitive information' in the *Information Privacy Act 2014* (ACT) s 14:<br>Sensitive information, in relation to an individual, means personal information that is—<br>c. About the individual's—<br>i. Racial or ethnic origin;<br>ii. Political opinions; or<br>iii. Membership of a political association; or<br>iv. Religious beliefs or affiliations; or<br>v. Philosophical beliefs; or<br>vi. Membership of a professional or trade association; or<br>vii. Membership of a trade union; or<br>viii. Sexual orientation or practices; or<br>ix. Criminal record; or<br>d. Genetic information about the individual; or<br>e. Biometric information about the individual that is to be used for the purpose of automated biometric verification or biometric identification; or<br>f. A biometric template that relates to the individual.<br>**Note:** Sensitive Personal Information *does not* include personal health information. |
| **Security and Emergency Management Senior Officials Group (SEMSOG)** | SEMSOG brings together and provides a liaison between Executives in relation to security and emergency management. |

| | |
|---|---|
| **Shadow ICT** | ICT systems that have not been registered with DCBR. |
| **SSP** | System Security Plan (previously a Security Risk Management Plan), the document used to assess security risk of an ICT system and its compliance with the Cyber Security Policy. |
| **Strategic platform** | ICT systems used for the delivery of business systems, e.g. Microsoft Azure, Salesforce. |
| **Technology Reference Manual** | Provides an authoritative reference to ACT Government's technology portfolio, and a standard language and classification scheme for technology in ACT Government. |
| **Unsanctioned services** | ICT systems that are not permitted from ACT Government networks or corporate devices. |
| **Vulnerability Assessment (VA)** | An assessment of an ICT system to determine if it is vulnerable to known attacks and Common Vulnerabilities and Exploitations. Note that this cannot provide an exhaustive assessment of the potential vulnerabilities of a system. If greater certainty is required, an independent Penetration Test should be undertaken. |
| **Whole-of-Government** | ICT systems for multiple administrative units or all administrative units, typically (but not always) provided by DCBR. |

# METADATA

| | |
|---|---|
| **Owner:** | ACT Government Chief Information Security Officer. |
| **Authority:** | DCBR ACT Cyber Security Centre |
| **Document location:** | Open Access Portal |
| **Review cycle:** | This document should be reviewed annually or when relevant change occurs to technology, business or the threat environment. |
| **Associations:** | ACT Protective Security Framework 2024 |

**Note:** This is a CONTROLLED document. Any documents appearing in paper form are not controlled and should be checked against the published (Open Access Portal) version prior to use.

# AMENDMENT HISTORY

| Version | Approved | Details | Author | Approval |
|---|---|---|---|---|
| Cyber Security Policy.0 | 11/2001 | Initial release. | ACTIM | ACTIS Management Board |
| 1.1 | 10/2006 | Minor revision | Policy Office | Endorsed by Policy Review Group |
| 2.0 | 11/2009 | Major revision and expansion to bring into line with current ACT Government infrastructure. | ICT Security | Approved by Shared Services Governing Committee |
| 2.5 | 11/2016 | Restructured for ease of reading. Added polices for governance, compliance and risk; network segregation; vulnerability management; cloud storage; user identification and authentication. Revised many other polices for cloud. | S Callahan | Executive Director, Shared Services ICT |
| 2.6 | 14/07/2017 | Requirement for security clauses with cloud service providers; revised Secure Data Transfers, Secure Desktops, and Sensitive Information in Non-production Environments | S Callahan | Executive Director, Shared Services ICT |
| 2.8 | 12/11/2018 | Notification of data breaches, email security, identity federation, domain name policy and change exemption policies added. | C Callahan J Owen | CTO, Shared Services ICT (Executive for ICT Security) |
| 2.9 | 08/01/2019 | Minor update to MFA rules and reference to data release standard. | C Callahan | ACT CISO |
| 2.10 | 06/06/2019 | Update to user account inactivity period, GRC triage criteria and shadow ICT reporting. | C Callahan | ACT CISO |

| Version | Approved | Details | Author | Approval |
|---|---|---|---|---|
| 3.0 | 28/10/2020 | Alignment with NIST 800-53 control families. Mapped to NIST, ACSC and ISO standards. Added Security Program, Personnel, Source Code and Config Management policies. Changed risk triage criteria and CISO authority to determine assessment. | C Callahan | ACT CISO |
| 3.0.6 | 17/02/2021 | Clarification of access control and vulnerability management policies. | C Callahan | ACT CISO |
| 3.1 | 21/09/2022 | New inclusions: PCI DSS and Payment of ransomware demands. Streamlined security authorisation processes.<br>Updates to DDTS Cyber Security team references and Chief Technology Officer to Senior Executive Responsible for Security.<br>Updates to linked references. | DDTS Cyber Security | ACT CISO |
| 3.2 | 30/06/2023 | Updated to new template. Updated or removed various references/links, and consolidated section references to Appendix A.<br>Clarification of *Unregistered Cloud Systems* (no change to intent). Clarified "must" as "should" in relation to API gateways. Incorporated certain clauses from the *Access Control Policy*, which has been retired. Clarified system eligibility for vulnerability assessments. | DDTS Cyber Security | ACT CISO |
| 3.3 | 15/01/2024 | Updates to Section 6 (Personnel Vetting) to include DDTS requirements for 'Super Users' and accounts with administrative privileges | Julian Valtas | Jeremy Hollis (A/G CISO) |
| 3.4 | 08/10/2025 | Minor updates to reflect new ACT Government directorate structure, update template, fix broken links and clarify Data Breach notification process | ACT CSC | ACT Government CISO |
| 3.5 | 10/11/2025 | Inclusion of Guidelines for Cryptography at Section 19, which replaces the Encryption Standard | ACT CSC | ACT Government CISO |

ACT Government

Digital Canberra

Date: 08 October 2025