## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>4</td>
</tr>
<tr>
<td>Purpose</td>
<td>4</td>
</tr>
<tr>
<td>Background</td>
<td>4</td>
</tr>
<tr>
<td>Scope</td>
<td>4</td>
</tr>
<tr>
<td>Compliance</td>
<td>5</td>
</tr>
<tr>
<td>Reference</td>
<td>5</td>
</tr>
<tr>
<td>Contact Officer</td>
<td>5</td>
</tr>
<tr>
<td>Responsibilities</td>
<td>6</td>
</tr>
<tr>
<td>Information Security</td>
<td>8</td>
</tr>
<tr>
<td>Acceptable use of ICT resources</td>
<td>8</td>
</tr>
<tr>
<td>Information classification</td>
<td>8</td>
</tr>
<tr>
<td>Personal information</td>
<td>9</td>
</tr>
<tr>
<td>Physical security of ICT resources</td>
<td>9</td>
</tr>
<tr>
<td>Stolen, lost or damaged ICT resources</td>
<td>10</td>
</tr>
<tr>
<td>Security training and communication</td>
<td>10</td>
</tr>
<tr>
<td>Identity and access management</td>
<td>17</td>
</tr>
<tr>
<td>Identification of users</td>
<td>17</td>
</tr>
<tr>
<td>Identity management federation</td>
<td>17</td>
</tr>
<tr>
<td>Authentication of users</td>
<td>17</td>
</tr>
<tr>
<td>Authorisation to use ICT resources</td>
<td>18</td>
</tr>
<tr>
<td>Access to ICT systems and information</td>
<td>18</td>
</tr>
<tr>
<td>Privileged access</td>
<td>19</td>
</tr>
<tr>
<td>Working offsite – employee remote access</td>
<td>19</td>
</tr>
<tr>
<td>Vendor access to ICT systems</td>
<td>20</td>
</tr>
<tr>
<td>Logging and monitoring</td>
<td>21</td>
</tr>
<tr>
<td>Auditing</td>
<td>21</td>
</tr>
<tr>
<td>Governance, compliance and risk management</td>
<td>12</td>
</tr>
<tr>
<td>Registration and inventory of ICT systems</td>
<td>12</td>
</tr>
<tr>
<td>Ownership of ICT systems</td>
<td>13</td>
</tr>
<tr>
<td>Risk management of ICT systems</td>
<td>13</td>
</tr>
<tr>
<td>Risk triage of ICT systems</td>
<td>14</td>
</tr>
<tr>
<td>Shadow ICT systems</td>
<td>14</td>
</tr>
<tr>
<td>Exemption from security assessment</td>
<td>15</td>
</tr>
<tr>
<td>Compliance with ICT Security policies</td>
<td>15</td>
</tr>
<tr>
<td>Policy waivers</td>
<td>16</td>
</tr>
<tr>
<td>Storage</td>
<td>17</td>
</tr>
<tr>
<td>Network drives and Storage Area Network (SAN)</td>
<td>23</td>
</tr>
<tr>
<td>Local drives</td>
<td>23</td>
</tr>
<tr>
<td>Removable devices</td>
<td>23</td>
</tr>
<tr>
<td>Storage in outsourced or cloud arrangements</td>
<td>23</td>
</tr>
<tr>
<td>Sanitisation and Disposal</td>
<td>24</td>
</tr>
<tr>
<td>Availability and resilience</td>
<td>25</td>
</tr>
<tr>
<td>Criticality and availability</td>
<td>25</td>
</tr>
<tr>
<td>Data backup and restore</td>
<td>25</td>
</tr>
<tr>
<td>Disaster recovery</td>
<td>25</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>--------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Business continuity</td>
<td>26</td>
</tr>
<tr>
<td>Operational security</td>
<td>27</td>
</tr>
<tr>
<td>Network segregation</td>
<td>27</td>
</tr>
<tr>
<td>Production information in non-production environments</td>
<td>27</td>
</tr>
<tr>
<td>Gateway security</td>
<td>28</td>
</tr>
<tr>
<td>Use of web presence for delivery of ACT services</td>
<td>29</td>
</tr>
<tr>
<td>Configuration of email services</td>
<td>29</td>
</tr>
<tr>
<td>Secure programming</td>
<td>30</td>
</tr>
<tr>
<td>Secure platforms</td>
<td>30</td>
</tr>
<tr>
<td>Secure data transfers</td>
<td>30</td>
</tr>
<tr>
<td>Secure desktops</td>
<td>31</td>
</tr>
<tr>
<td>Vulnerability Management</td>
<td>31</td>
</tr>
<tr>
<td>Reporting and disclosure of vulnerabilities</td>
<td>32</td>
</tr>
<tr>
<td>Incident response and investigations</td>
<td>32</td>
</tr>
<tr>
<td>Notification of data breaches</td>
<td>33</td>
</tr>
<tr>
<td>Associated documents</td>
<td>35</td>
</tr>
</tbody>
</table>
Introduction

Purpose
This policy establishes the Information Security regulatory framework for information being processed in electronic form for the ACT Government.

The ICT Security Policy derives its authority from the ACT Government Protective Security Policy Framework (PSPF) and supplements the PSPF with policies to support Information Security.

The policy will:

- provide a secure and effective Information and Communications Technology (ICT) based Information Security environment
- ensure all information assets when in electronic form are continuously available and protected to a level commensurate with the assessed risk and value/classification of the asset
- define standards for the defence against unauthorised access, use, modification, disclosure, damage or destruction of information assets
- mandate processes to minimise risks associated with disruption or failure of ICT systems.

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

If information assets are lost, inappropriately changed, or disclosed to unauthorised parties, it has the potential to harm the reputation of the ACT Government and disrupt the business functions of directorates, the delivery of justice, and the national security of the Australian Government.

The ACT Attorney-General through the Protective Security Policy Framework instructs directorates and agencies to:

- identify vulnerabilities and their levels of security risk;
- achieve the mandatory requirements for protective security expected by government;
- develop an appropriate security culture and proportionate measures to securely meet their business goals; and
- meet the expectations for the secure conduct of government business.

The ICT Security Policy was developed to assist directorates and agencies with a baseline of mandatory cybersecurity rules and practices for ICT systems.

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.
- cloud services and outsourced ICT solutions, and
- ICT hardware, software and operating systems
- any electronic information held on those assets.

This policy excludes non-electronic information.
Compliance
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.

Reference
This policy provides a whole of government Information security regulatory framework to ensure the ACT Government meets its obligations to protect and safeguard official information assets as set out in, but not limited to, the following legislation and authorities:

- ACT Criminal Code 2002
- ACT Information Privacy Act 2014
- ACT Workplace Privacy Act 2011
- ACT Freedom of Information Act 2016
- ACT Public Sector Management Act 1994 (PSMA), including Public Sector Management Standards
- Electronic Transactions Act 2001
- Australian Government Information Security Manual (ISM) 2017
- Australian Government Protective Security Policy Framework
- ACT Protective Security Policy Framework (ACT PSPF) 2017
- Shared Services processes, directions and procedures
- ISO/IEC 27002 – Code of Practice for Information Security Practice
- ISO/IEC 31000 - Risk Management
- HB 171 – Guidelines for the Management of IT Evidence

Contact Officer
For all queries about this policy, staff should contact ICT Security.
## Responsibilities

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACT Government employees and contractors</td>
<td>Comply with the policy and adopt the password standard.</td>
</tr>
<tr>
<td>JACS Security &amp; Emergency Management Branch</td>
<td>Responsible for developing whole-of-government policy on public sector protective security.</td>
</tr>
<tr>
<td>ICT Security</td>
<td>Responsible for developing whole-of-government ICT security policy, standards and strategies. A team comprised of the ITSA, ITSMs, security analysts and investigators who provide ICT security advice and implement and operate whole-of-government security measures.</td>
</tr>
<tr>
<td>Agency Security Advisors</td>
<td>Responsible for day-to-day management of the protective security measures within the directorate or agency. Develops, implements and monitors directorate or agency security procedures and systems. Analyses the directorate or agency’s security environment and posture, and plans measures to manage security risks.</td>
</tr>
<tr>
<td>Agency Security Executives</td>
<td>The delegate of the Director-General or CEO with authority to approve protective security programs for their directorate or agency.</td>
</tr>
<tr>
<td>Shared Services</td>
<td>Responsible for the security of ACT Government ICT infrastructure and Whole-of-Government ICT systems.</td>
</tr>
<tr>
<td>Directors-General and agency heads</td>
<td>Referred to as <strong>Business Owners</strong>. Responsible under the PSPF for the security of their information and ICT systems.</td>
</tr>
<tr>
<td>System Owner</td>
<td>Person within an ACT Government directorate who has the authority to make binding financial and operational decisions regarding an ICT system, and accepting the risks associated with the system on behalf of the Director General. This person is at executive or senior executive level. A System Owner owns an ICT system at the business unit or directorate level. An Enterprise System Owner owns a Whole of Government or multi-directorate system.</td>
</tr>
<tr>
<td>Senior Executive Responsible for Security</td>
<td>A role performed by the Chief Technology Officer, Shared Services. <strong>System Owner</strong> of Shared Services ICT infrastructure. Provides executive oversight of the ICT Security function.</td>
</tr>
<tr>
<td>Information Technology Security Advisor (ITSA)</td>
<td>Also referred to as the <strong>Chief Information Security Officer (CISO)</strong>. A Whole-of-Government role that manages the strategic direction of ICT security for ACT Government and the implementation and operation of Whole-of-Government security measures.</td>
</tr>
<tr>
<td>Information Technology Security Manager (ITSM)</td>
<td>A delegate of the ITSA responsible for a specialist discipline in ICT security.</td>
</tr>
<tr>
<td>Role</td>
<td>Responsibilities</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ICT Managers</td>
<td>Responsible for assisting directorates with SSICT solutions. Broad range of activities including collecting business system information and advising directorates about <strong>business system criticality</strong>.</td>
</tr>
<tr>
<td>Chief Information Officers</td>
<td>Responsible for ICT services on behalf of directorates. <strong>System Owners</strong> of directorate ICT infrastructure.</td>
</tr>
<tr>
<td>System manager</td>
<td>A directorate officer who is responsible for the integrity and operation of the ICT system; negotiates service levels; authorises access levels and access; and reviews audit logs.</td>
</tr>
<tr>
<td>Information owner</td>
<td>The ACT Government owns all information it develops and generates; however, the ACT Government is a nebulous concept from the point of identifying ownership. As such, the owner of the information is defined as the originator of the information.</td>
</tr>
</tbody>
</table>
Information Security

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. ICT Security logs and monitors your use of ACT Government ICT resources (e.g. Internet, email, instant messaging) and may use this data as evidence in any disciplinary matter.

Instructions

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.

Reference

Acceptable Use Policy

Information classification

There are two types of official Territory information:

- information that does not need increased security (public or UNCLASSIFIED information); and
- information that needs increased security to protect its confidentiality (any information with a Dissemination Limiting Marker or DLM such as Sensitive: Personal or For Official Use Only).

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 Protective Security Policy Framework (PSPF).

Instructions

1. Understand and remain aware of the ACT Information Security guidelines.
2. Ensure all official Territory information is classified correctly.
3. Do not change the classification of Territory information without approval of the information owner.
4. Information owners should use the Information Security Assessment template to assist with determining information security requirements.

Reference

ACT Protective Security Policy Framework
ACT Information Security Guidelines
Territory Records Standards for Records Management
Corporate Fact Sheet: Information Classification
ACT Government Information Security Assessment template
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, Health Records (Privacy and Access) Act 1997 and several other pieces of legislation relating to our functions.

All ACT Government employees and contractors are responsible for complying with the Information Privacy Act and the Territory Privacy Principles. Specific instructions relating to ICT usage are described below.

Instructions

1. When starting a new ICT initiative, perform a threshold assessment to determine the presence and sensitivity of personal information.
2. When indicated by a threshold assessment, perform a privacy impact assessment (PIA) to determine the handling requirements of personal information.
3. Information owners should use the Information Security Assessment template or similar mechanism to assist with performing a threshold assessment and PIA.
4. When sensitive personal information including personal health information is present, engage ICT Security to determine the protective measures required through the Risk Management of ICT Systems instructions.
5. Cloud services that will handle sensitive personal information should be hosted in Australia unless there are mitigations preventing vendor and third party access to the data.

References

Guide to undertaking privacy impact assessments, Office of the Australian Information Commissioner
ACT Government Information Security Assessment template
Information Privacy Act 2014 (ACT)
Territory Privacy Principles
Directorate Privacy Policies
Health Records (Privacy and Access) Act 1997

Physical security of ICT resources

All Information Systems or Information Assets classified as “critical” must be physically protected in secure areas from unauthorised access, damage and interference using security controls advised by ICT 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 computer rooms, PABX rooms, network equipment rooms and any associated service facilities.

Instructions

1. Access to secure areas is restricted to authorised ACT Government personnel. Access must be controlled using passwords, locks or access-control devices.
2. Access to information systems and assets in an outsourced arrangement must be restricted to authorised vendor personnel with an equivalent level of personnel security vetting to the ACT Government.

3. Secure areas should be monitored on a risk-assessed basis using access control logs and CCTV surveillance.

4. All wiring closets must be secured to prevent any damage and to stop unauthorised attempts to connect to data outlets and to prevent interception of data.

5. Access to network connection points located in public areas, conference rooms and other high-risk environments also require extra security controls to mitigate such risks.

Reference
ACT Government Physical Security Policy

Stolen, lost or damaged ICT resources

Report all incidents of lost, stolen or damaged ACT Government ICT equipment as soon as possible to the Shared Services ICT Central Asset Service Team using the Lost, Stolen or Damaged Assets Report form.

Instructions

1. Refer all incidents of lost, stolen or damaged ICT equipment to the Directorate ICT team for investigation.

2. Issues such as the value of the missing item/s and any information stored on such items must be identified.

3. Where the incident is considered significant, Directorate ICT teams must escalate it to ICT Security for investigation. ICT Security will prepare an incident report including the findings of the investigation. A copy of the report will be kept in Security and a copy will be delivered to the ACT Audit Office.

Reference
Acceptable Use of ICT Resources Policy

Security training and communication

The current environment in which we live and operate in demands a “culture of security” to protect ICT users from information security breaches. Even with the faster propagation and sophistication of new attack techniques, the biggest risk to protecting digital information remains human error.

Security policies and procedures in the workplace or additional security controls at home in themselves do not minimise the ability of intruders to compromise information. It is the human component that is critical in any effective and robust security framework, hence initiatives to improve security awareness of ICT users has a mitigating effect on information security incidents.

The ACT Government 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. Security awareness training must be conducted within each directorate. It is the directorate’s responsibility to ensure that this training is relevant to the directorate’s work environment. ICT Security can assist in development of training and can conduct training seminars on request.

2. Directorates must include topics about information security, including confidentiality, privacy and procedures relating to system access, in formal staff induction sessions and refresh the awareness of existing staff on a regular basis.

3. Each employee, on commencement of employment, must agree that they will not divulge any official information that they may have access to in the normal course of their employment. Staff must also agree that they will not seek access to data that is not required as part of their normal duties.

4. System Administrators should be properly trained in all aspects of system security prior to supporting these systems.

5. Directorates should conduct annual refresher training on the ICT Security Policy and security awareness to ensure that all staff are familiar with changes in policy and security practices.
Governance, compliance and risk management

Procurement of ICT systems
When procuring ICT systems including cloud services that handles information classified with any Sensitive DLM, directorates should engage legal advice to review the contract terms with the vendor prior to entering any agreement.

Instructions
1. Directorates should use the Recommended Sample Clauses for Cloud Security developed by the GSO and ICT Security when negotiating contracts with cloud vendors.
2. Directorates must not agree to contract terms that compromise privacy, the confidentiality of sensitive information, the availability of critical services or the ability of the Territory to investigate security incidents or vulnerabilities in the ICT system.
3. Directorates should not release official information to third parties who are not already contracted to the Territory.
4. Directorates should consult with Shared Services to determine if an ICT system already exists to perform the required service that suits the information security requirements of the business.

Reference
Recommended Sample Clauses for Cloud Security

Registration and inventory of ICT systems
When procuring, migrating or transferring Territory information to ICT systems including cloud services, directorates must register each system with Shared Services. Information about registered systems must be stored and maintained in an inventory to enable visibility and risk management.

Instructions
5. Directorates must register ICT systems including cloud services with Shared Services ICT.
6. Shared Services will assist directorates to discover unregistered ICT systems and cloud services.
7. Shared Services ICT will maintain an inventory of ICT systems including cloud services.
8. 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. products used and vendors;
   e. Security Point of Contact (SPOC) of the vendor, including contact details; and
   f. System Owner and the directorate SPOC (typically the Business System Manager).
9. Directorates must notify Shared Services of changes to these details during the life of the system.

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

Instructions
1. System Owners must be a member of the ACT Public Service with the delegation to accept security risk on behalf of the Director-General.
2. Directorates must name the System Owner when registering an ICT system.
3. Directorates must advise Shared Services ICT when the System Owner changes.

Reference
ACT Protective Security Policy Framework

Risk management of ICT systems
Directorates must manage the security risk of their ICT systems including cloud services. Directorates must assess security risks of an ICT system by performing a high assurance assessment (developing a Security Risk Management Plan (SRMP)) if it:

- is a business system with criticality of Government Critical or a strategic platform with criticality of Essential Infrastructure; and/or
- handles Territory information classified with any Sensitive Distribution Limiting Marker (DLM).

The criteria for low, medium and high assurance assessments are described in greater detail in the ICT Security Assurance Model.

Security assessment must be consistent across all directorates and comply with the ACTIA Risk Management Framework and the ACT PSPF.

As the provider of strategic security advice, ICT Security provides templates, tools and supporting processes to help directorates perform security assessments.

A sample of directorate SRMPs are audited by ICT Security annually and may also be examined by directorate internal auditors or the ACT Auditor-General.

Instructions
1. The System Owner of an ICT system needing a high-assurance assessment must ensure a SRMP is developed that documents the security risks and treatments recommended to protect it.
2. ICT Security will develop SRMPs for Whole-of-Government business systems and strategic platforms (including cloud services).
3. ICT Security will help directorates identify and assess security risks to information and ICT systems and advise on appropriate security controls to implement the risk treatments.
4. Security controls are derived from the Australian Government Information Security Manual (ISM) in the first instance. Security controls should also be drawn from relevant international standards and industry advice, such as ISO 27001 and Cloud Security Alliance Cloud Controls Matrix (CCM).
5. The CISO **endorses** the SRMP. Endorsement of a SRMP demonstrates that it identifies all known security risks and recommends appropriate controls to bring risk to an acceptable level.

6. The SSICT Security Executive also endorses the SRMP for any cloud services.

7. The System Owner **approves** the SRMP after endorsement. Approval constitutes acceptance of residual risk levels and commitment to implement the advised risk treatments and security controls.

8. ICT Security **holds and publishes** (to approved viewers) approved SRMPs on a secure repository.

9. The SRMP must be approved before Territory information is transferred to an ICT system or cloud service.

10. Directorates must review SRMPs every three years, or when a significant change has occurred in the business, technology or security environment.

11. SRMPs for Whole-of-Government business systems and strategic platforms should be audited before the system goes into production, and bi-annually thereafter.

12. Directorates should incorporate Extreme and High risks from SRMPs into their wider directorate risk management plan.

**Reference**

ACTIA Risk Management Framework

ICT Security Risk Management Standard


Cloud Security Alliance *Cloud Controls Matrix* (CCM)

**Risk triage of ICT systems**

ICT systems do not require formal assessment of security risks if they:

- have a criticality of Business Operational, Administrative or Nonessential Infrastructure
- handle official information classified public or unclassified (no DLM), **AND**
- are not public websites of the ACT Government.

However, the CISO at their discretion may determine that any ICT system requires security assessment or vulnerability assessment.

**Instructions**

1. ICT Security provide self-assessment tools and processes to directorates that enable triaging of ICT systems.

2. Directorates must still register triaged ICT systems including cloud services.

3. Directorates must still name the System Owner.

**Shadow ICT systems**

Shadow ICT (unregistered ICT systems and cloud services) presents potentially extreme levels of security risk to directorates. ICT Security provides reporting about cloud services in use across ACT Government. Directors-General and their delegates must remain aware of the level of shadow ICT present in their directorates and the security risks presented to enable a targeted approach to bringing these systems into formal risk management.
Instructions

1. Directorates must manage the security risk of shadow ICT.

2. Directorates should review ICT Security reporting of shadow ICT monthly and, in conjunction with Shared Services, identify system owners, contacts and other service management details that enable visibility of their ICT systems including cloud services.

3. ICT Security will add high risk cloud services to a list of unsanctioned services.

4. Directorates should block unsanctioned services.

Exemption from security assessment

Changes to an ICT system will prompt a check or review of security assessment status. ICT Security may exempt a Change from further assessment activity if it meets the criteria below. Standard Changes (operating system patching, NMP hardware changes, etc.) are covered by general exemptions and do not need individual exemptions.

Instructions

At the discretion of the CISO or their delegate, changes to ICT systems may be exempt from security assessment if:

1. The system meets the triage criteria for Low Assurance in the Security Assurance Model.

2. The system already has a valid SRMP, and the change does not materially impact security risks.

3. The system is a subsystem and is included in a larger SRMP, and the change does not impact security risks in the system or related systems.

4. The SRMP has not been approved but has been reviewed by ICT Security and is close to completion. The Change 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 (e.g. Create a Private DMZ in DTE Test).

6. The Change is to install software into production for Pre-Prod testing, i.e. the Exemption is for Tech Review only – the SRMP must be completed before go-live.

7. The Change relates to the implementation of infrastructure only, e.g.:
   - physical infrastructure (e.g. network infrastructure for a new building);
   - upgrade to an existing component of the SOE or server system software; or
   - a product classed as “Infrastructure” (like AD, FIM, SCCM, or SCOM).

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.

Compliance with ICT Security policies

ICT systems and cloud services must comply with ICT Security policies including this ICT Security Policy.

Instructions

1. The CISO or their delegate 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 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 ICT Security to conduct:
   a. security investigations
   b. compliance audits, and
   c. vulnerability testing.

4. Such agreements must include clauses requiring service providers to implement corrective action identified by investigation, audits and vulnerability testing.

**Policy waivers**

Policy waivers exist to accommodate those unique and rare circumstances where directorates have a strong business case for implementing information technology components that are non-compliant with an existing policy.

**Instructions**

Policy waivers are to comply with the ACT Government *Policy Waiver Procedure*.

**Reference**

ACT Government Policy Waiver Procedure
Identity and access management

Identification of users

Unique identification of ICT users ensures accountability and integrity of information. 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 severe consequences such as fraud, personal harm and harm to government reputation.

Instructions

1. System Owners must ensure that all users are uniquely identifiable, and their identity is authenticated each time they access ACT Government ICT resources.
2. 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 Standard.
4. System Owners should ensure service providers 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.
5. System Owners of WhoG systems should ensure ICT service providers leverage the unique user identities provided by ACT Government to enable single sign-on and related security activities.

Identity management federation

Cloud services that will be used by large numbers of users will be difficult for directorates 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 Shared Services ICT Active Directory via identity management federation.
2. Cloud services should leverage Shared Services ICT Active Directory via identity management federation when more than 50 users are present or when the service is shared across multiple directorates.
3. Cloud services should leverage ACT Government's iConnect Customer Identity and Access Management (CIAM) service when providing services to the public.

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 requirements of the Password Standard for all users.
2. Multi-factor authentication must be used for remote access that provides access to any DLM level 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 Shared Services if the service is degraded or unavailable, when authorised by the SSICT Security Executive (or delegate) on advice from the CISO (or delegate).

5. ICT systems must not send authentication information including temporary passwords in clear text.

6. ICT systems should not store authentication information including temporary passwords in clear text, for example hard coded into an application or script.

7. Where passwords are stored in clear text, passwords must be changed on a frequent basis.

8. External systems (cloud services and ACT Government websites) should reset passwords using a tokenised reset mechanism.

9. Reset passwords must meet the requirements for re-use of passwords as defined in the Password Standard.

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. System Owners are the authority for approving access by any user to a business system.

2. System Owners 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 or the user transfers to a different business area.

3. System Owners should ensure ICT systems are configured to suspend a user’s access after 90 days of inactivity.
   a. Directorates must ensure that Shared Services receives separation notification within 3 weeks of a staff member leaving. Shared Services will ensure the account is disabled within one week after this notification.
   b. Directorates must ensure that a similar process is applied to any cloud services which are not centrally managed via the ACT Government identity management services.
   c. Exemption from this policy is by prior written approval of the user’s manager.

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 authorized personnel in a way that meets both business and security requirements.
Instructions

1. 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.

2. 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 Standard.

3. Access to information stored on or processed in application systems or storage devices will be based on the need-to-know principle according to the requirements of the Access Control Policy.

4. Access to information and ICT resources must only be granted to employees and contractors who have been deemed suitable to have access appropriate to their role.

5. All detected unauthorised access to ACT Government information assets must be reported to ICT Security.

Reference

Acceptable Use of ICT Resources Policy
User Identity Standard
Access Control Policy
Public Sector Management Act and Standards

Privileged access

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. Privileged access to Shared Services hosted ICT resources handling DLM information must only be granted to employees and contractors who have been vetted to a personnel security clearance of at least Baseline.

2. Privileged access to ICT resources handling UNCLASSIFIED (no DLM) information should only be granted to employees and contractors who have been vetted with a criminal record check. ICT Security may on a risk-assessed basis recommend security clearance at a higher level for sensitive and critical systems.

3. System Owners must ensure they can suspend or revoke privileges.

Working offsite – employee remote access

The ACT Government promotes a family friendly work environment for its employees; as such Home-Based work and flexible working arrangements are provided for the staff of the ACT government. In addition, ACT government employees while performing their duties may be required to access the information assets of the ACT government while in remote locations or 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 any other method 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. For Home-Based work: Approved requests will be assessed for security risk by the IT Security Advisor or their delegate prior to home-based work commencing.

4. Employee authentication to the ACT Government network shall comply with the User Identity Standard.

5. If information is transferred to the remote device, then the remote device shall be secured in accordance with the ACT PSPF.

6. The communications link (wired or wireless) between the remote device and the ACT Government network shall be an appropriately secured connection in accordance with the ACT PSPF.

Reference

Remote Access Policy
Remote Connection Standard
User Identity Standard
Encryption Policy

Vendor access to ICT systems

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

Instructions

1. Only remote access methods endorsed by the CISO shall be used to connect to ACT Government domains.

2. Authentication to the ACT Government network shall comply with the ACT Government User Authentication Standard.

3. Applications being accessed shall reside on a server or servers owned exclusively by a Directorate or the server or servers shall only support the application being accessed by multiple Agencies.

4. A contract for services shall include a non-disclosure and confidentiality agreement and any support staff and subcontracting parties be bound by the conditions of the contract. Shared Services has a template agreement from "remote access agreement" form, which is the preferred document to ensure compliance with policy and security requirements. Copies of such contracts or deeds of agreement must be lodged with the SS ICT Security Manager Operations or their delegate.

5. The communications link (wired or wireless) between the remote device and the ACT Government network shall be a secure connection in accordance with the ISM.

Reference

Remote Vendor Access Policy
Remote Connection Standard
User Authentication Standards

Encryption Policy

**Logging and monitoring**

The ACT Government logs and monitors the use of Internet, email, IM and other ICT facilities and devices. For new technologies adopted by the ACT Government the need for controls and the level of monitoring and logging will be identified by a risk assessment.

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*, and ACT Government ICT policies.

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

**Instructions**

1. Activities that should be logged include:
   a. authorised access
   b. privileged access
   c. unauthorised access attempts
   d. system alerts or failures.

2. Activities that must not be logged include:
   a. passwords
   b. sensitive information such as bank accounts or tax file numbers.

3. The level of monitoring required for individual facilities should be determined by a risk assessment.

4. All logging and monitoring will be performed in accordance with the *Logging and Monitoring Standard* and be conducted with due regard to the *ACT Workplace Privacy Act 2011*.

**Auditing**

Non-compliance with the ICT Security Policy puts at risk the confidentiality, integrity and availability of ACT Government ICT services and systems, and electronic information. 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 ICT Security)
- Generic user accounts (facilitated by ICT teams and conducted by the Directorate)

Examples of other audits and checks performed on an ad hoc or on demand basis include but are not limited to:

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

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

Instructions

1. The CISO or their delegate shall:
   a. Undertake compliance audits across the ACT Government in accordance with the agreed ICT and Information Security audit program
   b. Provide reports to the security executive on compliance across the ACT Government
   c. Conduct authorised investigations into incidents of non-compliance with ICT policy
   d. Assist authorised officers in the conduct of criminal and administrative investigations.

2. All audits will be conducted with due regard to the ACT Workplace Privacy Act 2011.

Reference
Monitoring and Logging Standard
ICT Security Incident Response Policy
Storage

The storage of electronic data is to be controlled. Some storage methods are unsuitable for sensitive information (classified with a DLM). The information classification scheme used by the ACT Government is defined in the ACT PSPF, and its application is described in the fact sheet Information Classification Scheme.

The protection of classified data depending on the classification level is outlined in the ACT PSPF.

Network drives and Storage Area Network (SAN)

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

Do 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 ICT Security.

The use of network drives is contained in the Acceptable Use of ICT Resources Policy.

Local drives

Users storing official information on a local drive are responsible for its safekeeping.

Storing official information on local drives can place it at risk, because local drives are not regularly backed up like network drives. If the information is deleted, corrupted or modified in an unwanted way, it cannot be recovered to its previous “known good” state.

User should not store sensitive information on a local drive without additional protection.

Storing sensitive information (classified with a DLM) 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.

Removable devices

Users storing official information on removable media are responsible for its safekeeping.

Alternative data storage media options may be used for official business records once these records are captured in the current records management system. It is important to realise that once an electronic record is 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.

Users should not store sensitive information on removable media without additional protection.

Encryption of removable media may be required to protect sensitive information (classified with a DLM) in certain circumstances. Encryption must be performed using an approved method that complies with the ACT Government Encryption Standard.

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.

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.

2. Security risk assessments must comply with the *ICT Security Risk Management Standard*.

3. The System Owner must approve the arrangement (accept residual risks) before official information is transferred from ACT Government.

Reference

ICT Security Risk Management Standard

Sanitisation and Disposal

ICT resources including mobile devices, workstations, servers, Storage Area Networks (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. Shared Services and directorates must follow the approved Assets Disposal Process when ICT resources are no longer required.

2. Storage media must be sanitised according to the Storage Media Sanitisation Standard 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 Fact Sheet.

Reference

Storage Media Sanitisation Standard
Assets Disposal Process
Destruction of Data on Storage Media Fact Sheet
Availability and resilience

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 System Owners and ICT Security.
2. Availability must be measured and reported to System Owners for critical business systems and essential infrastructure, including outsourced solutions and cloud services.

Reference

Business System Criticality Guideline
Availability Management Policy

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 will leave the directorate subject to critical data loss in the advent of an erroneous or faulty backup.

It must be noted that backups are a disaster recovery mechanism and are not recognised as an archive under the Territory Records Act.

Instructions

1. All ICT resources handling official information must be backed up in accordance with the Data Backup and Restore Standard.
2. All official information stored on backup media shall be restored and reviewed for completeness at pre-set intervals based on the criticality of the information and as detailed in the SRMP for the system.
3. All official information stored on backup media shall be restored in accordance with the Data Backup and Restore Standard.

Reference

Data Backup and Restore Standard
Fact Sheet - Restoring Files and Data

Disaster recovery

Directorates 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.). Directorates should prepare a DRP for each non-critical ICT system.
Instructions

1. Shared Services assists directorates with developing DRPs for the critical business systems it hosts as part of the solution design process. Shared Services must meet the requirements of the ACT PSPF for the protection of ACT Government ICT resources in providing this service.

2. Directorates should use a methodology and template provided by Shared Services to prepare DRPs for non-Shared Services systems.

3. System Owners should test their DRPs before a system goes into production, and annually thereafter.

4. Shared Services should keep a copy of DRPs in a central location such as the ICT inventory system.

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. To achieve this, business continuity and disaster recovery must comply with the ACT Government Business Continuity Management Policy.

Directorates and business units 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 business critical information, personnel, facilities and ICT infrastructure.

Instructions

1. Directorates 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 SRMPs and DRPs
   c. a continuous improvement cycle for BCPs
   d. incorporation of the BCP process within existing directorate processes.

2. At minimum BCPs must cover critical ICT systems used by the directorate, including those shared with other directorates.

3. BCPs should also cover non-critical ICT systems, on a risk-assessed basis.

4. Directorates should keep a copy of the current BCP in a central location.

Reference

Business Continuity Management Policy
Operational security

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 always 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 accredited to the same level of security as the production environment if they are to handle sensitive information.

References

Production information in non-production environments
Non-production environments should not contain personal or sensitive production information. Development environments must not contain personal or sensitive production information.

Instructions
1. Official information should not be handled by non-production ICT environments unless explicitly permitted by the system owner. This is usually provided in written form through approval of the system SRMP, or through approval of a Production Data Release form.
2. Personal information must not be handled by non-production ICT environments unless:
   a. ICT Security has approved that the lower environment is secured to the same standard as the production environment, and
   b. System Owner has approved that the purpose for which the data will be used meets the Appropriate Use under the Information Privacy Act.

If these conditions are not met, information with a DLM or classification must not be transferred to or accessed from within a non-production ICT environment without first being sanitised.
3. Approval to release Production data to Test is required and typically obtained as part of test planning. Use the Production Data Release Procedure and form.
4. Development environments are inherently insecure and must not be used to handle personal or sensitive information.
5. Sanitised information may be used in lower environments when the sanitisation method used is endorsed by ICT Security. Sanitisation methods are used to depersonalise personal information and/or reduce the sensitivity/classification of official information to UNCLASSIFIED (no DLM).
6. ICT 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.
7. 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.

8. When engaging external ICT and cloud service providers, 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.

9. System Owners must satisfy themselves that they are in compliance with legislation such as the Information Privacy Act and other enactments of secrecy, and should seek legal advice where legislation applies to their intended re-use of production data.

References
Fact Sheet: Production Information in non-production environments
Production Data Release Standard
Information Privacy Act (ACT) 2014

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.

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

Instructions
1. All ACT government internet gateways must be secured using controls that comply with the ACT Government Gateway Security Standard.
2. All activities within ACT Government internet gateways must comply with the ACT Government Gateway Environment Policy.
3. All servers deployed to the gateway environment must be built in accordance with the Shared Services server build standards.
4. All applications must undergo penetration testing in accordance with the Vulnerability Management policy before being promoted from the development environment into production.
5. All changes to network devices are to be authorised prior to implementation by Change Management and IT Security.

Reference
ACT Government Gateway Security Standard
ACT Government Gateway Environment Policy
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. Shared Services ICT administers act.gov.au domain names on behalf of ACT Government agencies.

Instructions

1. Domain name registration requests must be approved by the agency Director-General or Executive Delegate.
2. Domain names must be registered with a Registrant Contact Position (an employee of the agency).
3. Shared Services ICT 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. Shared Services ICT has the right to reject an application for a domain name.
5. Domain name registrations are reviewed every 2 years.

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 Shared Services must be protected according to the highest level of sensitivity and criticality required by directorates. Business systems must be integrated with ACT Government email in a way that does not reduce this security posture.

Shared Services has developed an ACT Government Email Authentication Standard to assist directorates with best practice security controls, which include:

- SPF – a DNS name record that advertises the authorised mail senders for a specific mail domain;
- 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; and
- 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 Shared Services will provide; and
   c. When unable to comply, seek a waiver when using a subdomain dedicated to the system or business function.
2. Directorates must comply with the ACT Government Email Authentication Standard and use the forms provided by Shared Services when engaging third parties that provide mail services.
3. ICT Security and nominated directorate contacts will assist third parties to correctly use email authentication protocols, including making any necessary changes to Shared Services managed systems like DNS.
4. System Owners should ensure their business systems are modified to comply with the Standard. Directorate CIOs should assist them to migrate to a dedicated mail subdomain if they cannot support email authentication.

5. Shared Services will provide DMARC reporting and forensics capability to assist in SPF, DKIM and alignment.

6. 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.

References
ACT Government Email Authentication Standard

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. Shared Services should adopt and promulgate OWASP standards for secure coding, code review and testing practices for all bespoke business systems.

2. ICT Security will reduce the likelihood of relevant security risks when assessing websites, cloud services and mobile applications that can demonstrate compliance with OWASP standards.

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 Center for Internet Security (CIS) Security Benchmarks.

Instructions
1. Shared Services should adopt and promulgate CIS Security Benchmarks for all server builds.

2. ICT Security will take into account CIS compliance when assessing relevant security risks of ICT platforms.

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 it supports.

Instructions
1. Approved secure data transfer methods include:
   a. Secure File Transfer Protocol (SFTP) system approved by ICT Security
   b. Application Programming Interfaces (APIs) that use a security protocol approved by ICT Security, and
   c. Physical transfer via encrypted media or physical safehand if encryption to ACT Government Standard is not possible.
Secure desktops

While no single mitigation strategy is guaranteed to prevent cyber security incidents, ACT Government implements eight essential mitigation strategies recommended by the Australian Signals Directorate 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 having to respond to a large-scale cyber security incident.

Shared Services configures ACT Government desktops (including laptops and 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 Shared Services.

Instructions

1. ACT Government should adopt and promulgate Microsoft standards for all desktop builds.

2. ACT Government must implement standard desktops on behalf of directorates that support the Australian Signals Directorate’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

3. End users must not be able to install non-standard applications without prior written approval from ICT Security.

4. Technical staff should not be able to install non-standard applications without central deployment.

Vulnerability Management

The ACT Government will, according to and ICT system’s assurance level, perform vulnerability testing to identify security weaknesses caused by misconfiguration, bugs, obsolescence or design flaws.

The ACT Government will also implement and manage malware protection tools for all endpoints including servers, desktop computers and mobile devices, and gain assurance that service providers do the same throughout the life of a cloud service through the governance, risk management and compliance auditing process.

Instructions

1. Externally hosted or externally exposed business systems, including cloud services and websites, must be vulnerability tested by ICT Security if they meet the triage criteria for Medium or High Assurance (see the ACT Government Security Assurance Model).

2. Initial vulnerability testing 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.

3. ICT Security will monitor new information from a variety of government and industry sources on emerging security vulnerabilities and threats to ICT resources.
4. Ongoing vulnerability management in the form of automated vulnerability scanning and/or patching may be performed throughout the life of Shared Services hosted ICT systems to maintain security in the face of emerging vulnerabilities and threats.

5. Externally facing websites will be audited more frequently as they are historically more vulnerable to compromise.

6. ICT Security will analyse identified vulnerabilities to determine their potential impact and advise System Owners of appropriate treatments.

7. System Owners must ensure the advised treatments are implemented on a risk-assessed basis agreed with the CISO or their delegate.

8. System Owners must ensure vulnerabilities are treated as soon as possible (within 30 days, or immediately if it is an extreme-risk vulnerability that would otherwise require the system to be taken offline).

References
Vulnerability Management Standard
Vulnerability Testing Fact Sheet

Reporting and disclosure of vulnerabilities

ACT Public Service staff and contractors must report security vulnerabilities directly to ICT Security. Security researchers not employed or contracted to ACT Government are encouraged to report vulnerabilities in government systems to ICT Security or through the business system owner or delegate who is then required to report this to ICT Security.

Instructions

1. Security researchers are encouraged to report identified vulnerabilities and exploits to the ACT Government.

2. Security researchers should report security vulnerabilities to itsa@act.gov.au

3. Reports should include:
   a. details of the identified vulnerability (type, products and platforms affected)
   b. where identified (URL or link)
   c. likely impact of exploit on users, critical infrastructure or physical safety
   d. proof of concept
   e. date identified
   f. can it be replicated
   g. evidence that the vulnerability is not already public, and
   h. contact details (optional).

4. Security researchers may make public (disclose) vulnerabilities 90 days after reporting to ACT Government, unless otherwise agreed by both parties.

5. ACT Government may acknowledge discovery of vulnerabilities but does not pay bug bounties.

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.

Directorates must have in place Critical Response and Incident Reporting procedures to manage incidents occurring within critical ICT systems. Directorates should consider applying this policy to non-critical ICT systems on a case-by-case basis.
ICT Security provides investigation and digital forensic services to ensure only qualified investigators are involved and ensures that any chain of evidence is maintained.

**Instructions**

1. System Owners must establish an incident reporting procedure for their ICT systems.
2. Critical response and incident reporting must comply with established directorate procedures, e.g. directorate fraud control.
3. Where the incident involves a government system, the ICT Security team must be notified, kept informed of developments, and involved with resolution of the incident.
4. Investigations and forensic analysis will only be conducted by ICT Security.
5. Incident response and reporting must comply with the *Critical Response and Incident Reporting Policy* and the *ICT Security Incident Response Policy*.
6. The collection of audit trails for all ICT systems must comply with the *Monitoring and Logging Standard*.

**Reference**

Critical Response and Incident Reporting Policy
ICT Security Incident Response Policy
Monitoring and Logging Standard

HB 171 – Guidelines for the Management of IT Evidence

**Notification of data breaches**

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

The ACT Government is committed to transparency and protection of the public interest and should provide notification of data breaches.

**Instructions**

1. System Owners are responsible for assessing a suspected data breach to determine its likely impacts. ICT Security can provide technical assistance on request.
2. System Owners must make the Director General completely aware of all information in relation to the breach.
3. With the approval of the relevant Director General, the directorate should notify any individuals whose personal information is involved in a data breach of their ICT systems, where the breach is likely to result in serious harm including (but not limited to):
   a. Physical
   b. Reputational
   c. Financial.
4. With the approval of the relevant Director General, 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.

5. With the approval of the relevant Director General, System Owners should notify the Australian Information Commissioner using the Notifiable Data Breach statement — Form. 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.

6. The Australian Information Commissioner is empowered to request information from System Owners if there is a reasonable belief that a government system (including cloud services) is involved in a data breach.
Associated documents

The following ACT Government documents are part of the ICT and ICT Security policy suites that support this ICT Security Policy:

- Acceptable Use of ICT Resources Policy
- Access and Use of ICT Resources Policy
- Access Control Policy
- Business Continuity Management Policy
- Critical Response and Incident Reporting Policy
- Data Backup and Restore Standard
- Encryption Policy
- Gateway Security Standard
- ICT Security Incident Response Policy
- Monitoring and Logging Standard
- Password Policy and Standard
- Policy Waiver Standard and Procedure
- Sensitive Information in Non-Production Environments Policy
- Server Hardening Standard
- Software Acquisition and Control of Local Hard Drives Policy
- Vulnerability Management Policy
- Vulnerability Testing Fact Sheet
# Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>The process of confirming the correctness of the claimed identity.</td>
</tr>
<tr>
<td>Availability</td>
<td>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.</td>
</tr>
<tr>
<td>BCP</td>
<td>Business Continuity Plan</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Ensuring that information is accessible only to those authorized to have access.</td>
</tr>
<tr>
<td>Data integrity</td>
<td>Information in a condition in which it has not been altered or destroyed in an unauthorised manner.</td>
</tr>
<tr>
<td>DRP</td>
<td>Disaster Recovery Plan</td>
</tr>
<tr>
<td>Encryption</td>
<td>The process of transforming information using an algorithm or cipher to make it unreadable to anyone except those possessing the key.</td>
</tr>
<tr>
<td>ICT Asset</td>
<td>Any physical or logical computing device either owned, leased, or used by the ACT Government to hold or process ACT Government electronic information. Includes, but is not limited to, ICT hardware, software and operating systems, cloud services and outsourced ICT solutions.</td>
</tr>
<tr>
<td>ICT System</td>
<td></td>
</tr>
<tr>
<td>Remote access</td>
<td>The ability to get access to a computer or a network from a remote location. An external location being a premise not controlled or maintained by the ACT Government.</td>
</tr>
</tbody>
</table>
Metadata

<table>
<thead>
<tr>
<th>Owner</th>
<th>Senior Manager, ICT Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authority</td>
<td>CTO, Shared Services ICT (Executive responsible for ICT Security)</td>
</tr>
<tr>
<td>Location</td>
<td><a href="http://sharedservices/actgovt/ICTdocs/ICT">http://sharedservices/actgovt/ICTdocs/ICT</a> Security Policy.docx</td>
</tr>
<tr>
<td>Review cycle</td>
<td>This document should be reviewed annually or when relevant change occurs to technology, business or the threat environment.</td>
</tr>
<tr>
<td>Associated documents</td>
<td>ACT Protective Security Policy Framework 2017</td>
</tr>
</tbody>
</table>

Revisions

<table>
<thead>
<tr>
<th>Version</th>
<th>Published</th>
<th>Details</th>
<th>Author</th>
<th>Approval</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>11/2001</td>
<td>Initial release.</td>
<td>ACTIM</td>
<td>ACTIS Management Board</td>
</tr>
<tr>
<td>2.0</td>
<td>11/2009</td>
<td>Major revision and expansion to bring into line with current ACT Government infrastructure.</td>
<td>ICT Security</td>
<td>Approved by Shared Services Governing Committee 12/10/2009</td>
</tr>
<tr>
<td>2.1</td>
<td>02 2012</td>
<td>Changes to reflect new Shared Services ICT structure, Include reference to the Workplace Privacy Act, and changes references to Agencies to Directorates</td>
<td>K Webb</td>
<td>Executive Director, Shared Services ICT</td>
</tr>
<tr>
<td>2.2</td>
<td>11/2012</td>
<td>Update classification system to reflect new classification standards and include references to ISO 27000 series standards.</td>
<td>P Major</td>
<td>Executive Director, Shared Services ICT</td>
</tr>
<tr>
<td>2.3</td>
<td>01/2014</td>
<td>Para 1.3 adjusted to include Instant messaging and the use of unapproved hardware and software on the ACT Govt network. Approval process for SRMPs and Glossary updated</td>
<td>P Major</td>
<td>Executive Director, Shared Services ICT</td>
</tr>
<tr>
<td>2.5</td>
<td>11/2016</td>
<td>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.</td>
<td>S Callahan</td>
<td>Executive Director, Shared Services ICT</td>
</tr>
<tr>
<td>Version</td>
<td>Published</td>
<td>Details</td>
<td>Author</td>
<td>Approval</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>2.6</td>
<td>14/07/2017</td>
<td>Requirement for security clauses with cloud service providers; revised Secure Data Transfers, Secure Desktops, and Sensitive Information in Non-production Environments</td>
<td>S Callahan</td>
<td>Executive Director, Shared Services ICT</td>
</tr>
<tr>
<td>2.8</td>
<td>12/11/2018</td>
<td>Notification of data breaches, email security, identity federation, domain name policy and change exemption policies added. Changes accepted by CISO.</td>
<td>C Callahan, J Owen</td>
<td>CTO, Shared Services ICT (Executive responsible for ICT Security)</td>
</tr>
<tr>
<td>2.9</td>
<td>08/01/2019</td>
<td>Minor update to MFA rules and reference to data release standard.</td>
<td>C Callahan</td>
<td>CISO, SS ICT</td>
</tr>
<tr>
<td>2.10</td>
<td>06/06/2019</td>
<td>Update to user account inactivity period, GRC triage criteria and shadow ICT management</td>
<td>C Callahan</td>
<td></td>
</tr>
</tbody>
</table>
This is a CONTROLLED document. Copies in paper form are not controlled and should be checked against the version on the Shared Services Portal before use.