ICT cyber security standard

This is a mandated standard under the operational policy framework. Any edits to this standard must follow the process outlined on the creating, updating and deleting operational policies page.

Overview

Cyber security is fundamental to the successful operations of the department. The management and effective sharing of information resources is essential to maintain legal and regulatory compliance, the reputation of the agency, keeping our children and young people safe online and supporting our strategy in delivering a world class education system.

The purpose of this standard is to define the approach for implementing cyber security controls for the Department for Education's IT systems, infrastructure and general information assets (IT assets)

This standard is aligned with the South Australian Cyber Security Framework (SACSF).

Scope

This standard applies to all department sites, staff and students.

Government of South Australia
Department for Education

Contents

ICT cyber security standard 1
Overview 1
Scope 1
Detail 4
Security Governance 4
Access management 6
Password Management 11
Endpoint security and maintenance 15
Server security and maintenance 17
Mobile device and removable media 19
Security logging and monitoring 22
Network security 24
Physical security 26
Application security 28
Vendor Security 30
ICT Risk Management 31
Personnel security and acceptable use 34
Secure information handling 37
Travelling internationally – Department devices and data handling 42
Exemptions to standards 43
Roles and responsibilities 43
Chief Information Officer 43
Site leaders 43
ICT Cyber Security 43
ICT personnel 44
All employees 44
Glossary 45
Supporting information 50
Related legislation 50
Related policies 50

Record history 50
Approvals 50
Revision record 50
Contact 51

Detail

Security Governance

Security objectives

This standard supports the following cyber security objectives of the department:

- Provide a structured approach to information security management that is consistent across the department.
- Maintain the confidentiality, integrity and availability of information assets in compliance with policy, legal and regulatory requirements.
- Provide a mechanism for continual improvement of the information security practices of the department.
- Implement manageable and effective information security controls to ensure appropriate protection of the department's information assets.
- Establish a consistent approach to the assessment, management and treatment of information security risks relating to the services within scope of the Cyber Security Program.
- Provide the department's personnel with sufficient training to ensure both their understanding of relevant cyber security responsibilities and their confidence in the effectiveness of the department's security controls.
- Report and investigate all breaches of information security and suspected weaknesses.
- Provide assurance to stakeholders and other interested parties of the security of their information entrusted to the department whether in storage, processing or transmission.
- Alignment with the whole of government SACSF.

Governance structure

The implementation of the Cyber Security Program is overseen by the Security Steering Group (SSG), which includes the ICT Cyber Security team who has the responsibility for Cyber Security Program (CSP) operations.

The site leader is ultimately accountable for the implementation and effectiveness of the school's cyber security program and compliance to this standard. Each site should nominate an ICT coordinator responsible for the implementation and operation of security controls, even if the school is supported by a third party IT service provider.

The diagram below shows the Cyber Security Program governance structure together with the interfaces and dependencies within the department's Cyber Security Program.

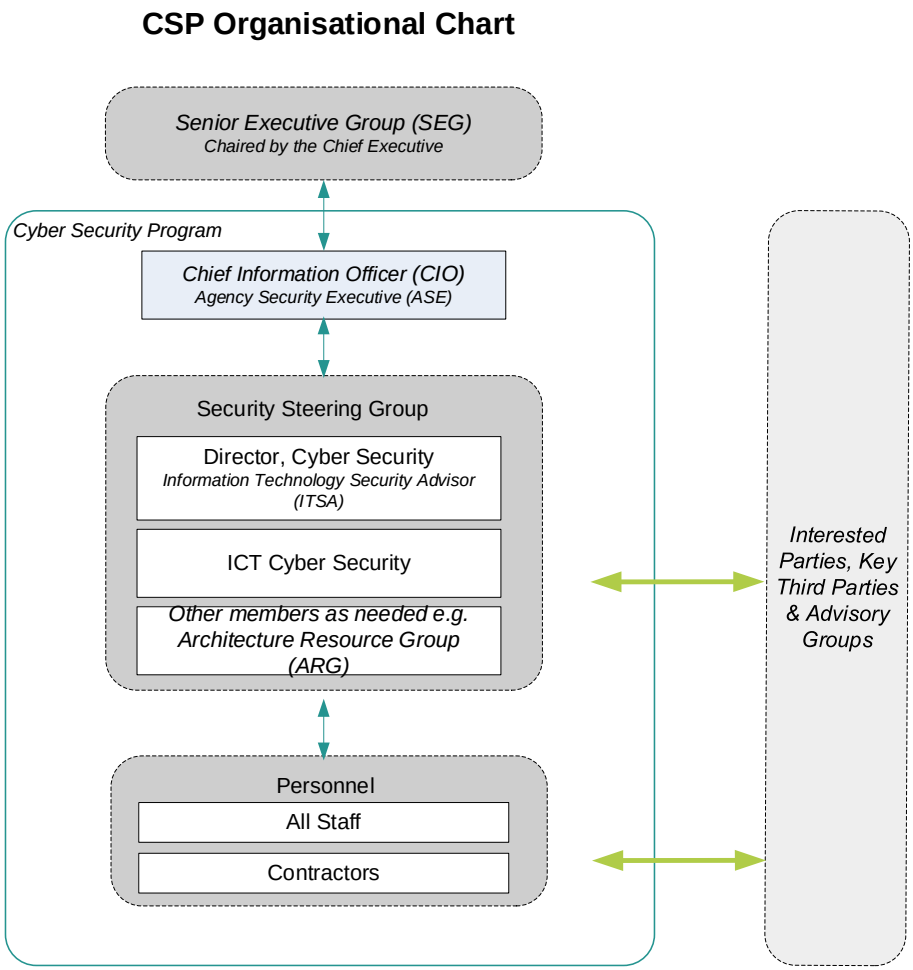

Figure 1 – Cyber Security Program Organisational Chart

Monitoring, evaluation and review

The Security Steering Group will undertake a management review of the operations of the Cyber Security Program and this standard at least annually, or when significant changes to the business occur. This review will assess the effectiveness and practicality of the Cyber Security Program and its ability to meet agency objectives. The management review will also consider the suitability and effectiveness of the existing policies. Actions regarding modifications to these documents will be tasked to the relevant personnel and documented in the Incidents and Actions Register for tracking and management. Input into this review will include industry standards, audit reports, risk management activities, external independent assessments, incidents and the results of education awareness activities.

The results of the review will be documented and must identify any appropriate actions related to the continual improvement and effectiveness of the Cyber Security Program together with improvements to the department's services with respect to stakeholder requirements and their perceived needs. These may include the following:

- adjustments to the scope of the Cyber Security Program
- updating the risk treatment plan
- updating policies and standards
- resourcing and budgeting decisions.

In addition, the results should identify any resources needed to meet the identified actions including persons responsible for carrying out the actions together with time scales for their completion.

Access management

Account access approval

All systems and applications must have a formal process for requesting, reviewing and approving access. Specifically:

- approval to access IT assets and information must first be obtained from the information, IT asset or information owner
- where delegated by the information owner, approval to access IT assets and information may also come from the direct line manager of the user
- the system access requested must be the minimum needed to perform the role, consistent with business requirements
- approval must take into consideration any relevant legislative and contractual obligations regarding limitation of access to data or services.

Mailbox access

Requests for access to another user's department mailbox may arise when a user is no longer employed by the department or is unavailable for a prolonged period. Such requests require written approval (ie, via

email) from the user's director, or site leader, and must specify the level of access required, the circumstances of the request, and who requires access to the mailbox contents. These specifications and approval must then be provided to ICT Services to action the request.

ICT Cyber Security may also provide access to a mailbox when responding to a cyber security incident, via a formal request as part of an internal investigation, or at the behest of SAPOL.

Account access control

Where possible, systems and applications must be configured to apply the following access controls:

- 'Default deny' access to resources should be applied unless explicit access is granted.
- Certificate based authentication must be implemented to identify authorised workstations connected to the department's network.
- Segregation of duties must be implemented to minimise conflict of interest situations based on business requirements.
- Help or error messages must not be displayed unless a user has successfully logged on to the system or application.
- Accounts automatically lock after brute force attempts or a significant number of login attempts fail for a particular user.
- Passwords must not display in clear text while being entered.
- Passwords must only be transmitted over the network using strong encryption in accordance with the secure data handling section.
- Inactive sessions are terminated after a period of inactivity.

User accounts

User accounts are defined as accounts used by staff across the department, including corporate staff, teachers and other department personnel for day-to-day activities. In relation to management of user accounts, staff must adhere to the following:

- All required approvals must be obtained before access is given to the department's systems, applications, source code or associated infrastructure.
- User account and password management and allocation of passwords must only be performed by authorised staff and must follow approved operational procedures.
- Passwords must be managed by users in accordance with the password management section of this document.
- Each user must be issued with a user identifier (user ID) which uniquely identifies them and allows access to systems in conjunction with the use of a password that meets the requirements defined in the password management section of this document. This can include secondary identification provided through privileged access management systems.
- A formal user authorisation process to add, modify and remove access is to be maintained.

- A process to record authorisations and a record of all privileges allocated must be maintained.
- User access (including privileges) must not be granted until the authorisation process is complete.

Shared and generic user accounts

Shared and generic accounts are those that are unable to be attributed to an individual user. They are most common on publicly accessible kiosks, or devices shared by multiple staff. The use of generic or multi-user logins (user IDs) are only permitted under the following circumstances:

- The generic or shared account has been approved by the site leader (if for an education site) or ICT Cyber Security.
- A manager or site leader has been assigned responsible and accountable for the activity performed on the account and is required to change the password whenever there is a change in team members with access to the account.
- Passwords associated with generic accounts are securely communicated to authorised users.
- Access to a shared account is restricted only to the minimal functionality required for its purpose. Where possible, restrictions should be placed on Internet and network resources.
- Access to the account is restricted or limited to specific devices on the network.

Service accounts

Service accounts are created where an application, system or automated service needs access to information or network resources. The use of service accounts is only permitted under the following circumstances:

- The service account has been approved by the site leader (if for an education site) or ICT Cyber Security.
- A manager has been assigned responsible and accountable for the activity performed on the account.
- Passwords of the account are securely stored in accordance with the password management section of this document
- Interactive sessions are disabled by default, if possible, otherwise staff are prohibited from using service accounts interactively, or access to the account is restricted to specific devices on the network.
- All service accounts should follow a standard naming convention that makes them easily identifiable in the environment (eg prefixed with ‘svc-’).
- Service accounts should only be given administrative privileges where strictly required and approved by the Director of the business unit
- Remove or disable service user accounts that have been inactive for 45 days.
- For service accounts that are used infrequently (eg once a year), an exemption to the 45 day inactivity rule can be approved by the Site Leader or ICT Cyber Security with a valid business reason.

These exemptions must be documented and must be reviewed annually at a minimum.

Privileged accounts

Privileged accounts, such as administrator accounts, are those created with elevated capabilities and are generally used by system or application administrators. These accounts may include the ability to create or modify additional accounts, modify system data or files of those belonging to other users, or perform application or database functions outside the control of the application system for which the account was issued.

The following additional access management controls are required for privileged accounts:

- Privileged accounts must be associated with an individual and use a naming convention that can attribute them to an individual. Shared or generic accounts should not be given administrative privileges.
- The naming convention should clearly distinguish that the privileged account from a regular account. The department's preferred way is with a prefix on the username, eg 'a-johnsmith' for administrative accounts.
- Multi-factor authentication must be configured for privileged account access to systems where possible.
- Privileged accounts must have an end period associated of a maximum of one year, after which a new access request and approval is required.
- Privileged accounts must be separate from a user's regular account. The privileged account must not be used for regular business activities.
- Remove or disable privileged user accounts that have been inactive for 45 days.

Access reviews and removal

IT asset and information owners are responsible for ensuring access to assets is appropriate and removed in a timely manner when no longer required. Owners must:

- where possible, implement automatic notifications or triggers to remove access automatically when no longer required (eg terminated employees, employees changing roles or schools)
- where possible, enable automated alerts for new, changed or removed access rights
- where automatic notifications and triggers are not possible, review access rights at periodic intervals, at least quarterly
- remove access immediately after an employee changes role, leaves the department or for other reasons no longer requires access
- remove or disable standard user accounts that have been inactive for 90 days.

Remote access authentication

Remote access is only permitted under the following circumstances:

- Using a secure connection or method (eg VPN) for remotely accessing the network that has been approved by ICT Services.
- Remote access to the department or school networks must use either two-factor authentication, a one-time password authentication, or a public/private key system with a strong passphrase or certificates.
- Remote access sessions must expire after a defined period of inactivity.
- Remote access for user accounts must be removed when the user leaves the department or is no longer under contract to the department.

Remote access connections

The following directives apply with respect to connections via remote access:

- The department's employees, including contractors and suppliers, must ensure that any device they are using that is remotely connected to the department's network is not concurrently connected to any other network at the same time (ie split tunnelling is prohibited)
- All hosts that are connected to the department's internal networks via remote access technologies must use current anti-malware software – this includes personal computers and laptops.
- Supplier connections must comply with requirements as stated in the relevant agreement between the department and the supplier. Refer to the ICT vendor security section of this standard for more information.
- Prior to allowing access to the department's network, remote systems must be checked for current local anti-malware software and a functional firewall on the user's machine.
- Personal equipment that is used to connect to the department's networks must meet the requirements of department-owned equipment for remote access.
- Organisations or individuals who wish to implement non-standard remote access solutions to the department's network must obtain prior approval from the ICT Cyber Security Team.

Remote access sessions

Remote users must ensure that:

- a remote access session is never left unattended, even if not currently signed-on to an application or other information system
- a remote access session is disconnected immediately after having signed off and a password-protected screen saver is always used
- no other person is allowed to operate a remote access session that has been established
- the workstation is locked or logged off when leaving the workstation unattended
- they are aware of an understand the remote access provisions of this standard.

Password Management

Password configurations

Staff and contractor accounts

User accounts are defined as accounts used across the department, including corporate staff, teachers, contractors and other department personnel for day-to-day activities. The following password settings are to be applied to general user and system accounts on department production systems and applications:

- **minimum password length** of 12 characters
- **password expiry** every 365 days (this requirement is optional if multi-factor authentication is available and enabled)
- **password change** required on first login
- **password history** preventing users from using any of the previous 24 passwords
- **minimum password age** of 1 day
- **account lockout** after 10 invalid attempts for 60 minutes.

Privileged accounts

Privileged accounts are defined as accounts with elevated permissions suitable for managing the department's systems, such as those used by system administrators and IT personnel to log into servers, apply patches and manage users. The following password settings are to be applied to privileged accounts, such as Administrator accounts, on production systems and applications:

- **minimum password length** of 16 characters
- **multi-factor authentication** enforced, where possible
- **password expiry** every 365 days (this requirement is optional if multi-factor authentication is available and enabled)
- **password change** required on first login
- **password history** preventing users from using any of the previous 24 passwords
- **minimum password age** of 1 day
- **account lockout** after 5 invalid attempts, indefinitely.

In addition to the criteria defined above, the following standards must also be applied:

- The password of an administrator account must be unique from all other accounts held by that user. It is recommended usernames for privileged accounts be prefixed to distinguish them from regular accounts where possible. For example, prefixing with 'PRV-'.
- Passwords on any shared administrative accounts (where allowed, eg root account) must be changed immediately upon termination of employment or contract of any individual who has knowledge of that password, including accounts managed by third party contractors.

Service accounts

Service accounts are defined as accounts used for purposes such as backups, performing tasks within applications, connecting to other devices and running scheduled jobs. The following password settings are to be applied to service accounts on department production systems and applications:

- **minimum password length** of 24 characters
- **password complexity** requiring at least one of each of the following:
    - uppercase alphanumeric character (A-Z)
    - lowercase alphanumeric character (a-z)
    - numeric character (0-9)
    - special character (eg ?, $, &).

In addition to the criteria above, the following standards must be applied:

- A service account must not be used by any person to log into an interactive session, except where required for the initial configuration of the account or linked service.
- Service account passwords that are not changed automatically as part of a business process or scheduled task are to be recorded in a secure password repository that has access control to restrict access.
- Service account passwords and other passwords must not be stored in clear text or using basic obfuscation methods in source code (eg Base64 cannot be used).

Student accounts

Student password requirements should be commensurate with a student's year level. Exceptions to this standard are to be maintained by the school and based on individual student capabilities and needs. The department recommends schools apply the following password requirements for student accounts:

Year 2 and below

The following password settings are recommended for students at Year 2 or below:

- **minimum password length** of 4 characters
- **password expiry** every 400 days (this requirement is optional if multi-factor authentication is available and enabled)
- **password history** preventing users from using any of the previous 6 passwords
- **minimum password age** of 1 day
- **account lockout** after 30 invalid attempts for 10 minutes.

Year 3 to Year 6

The following password settings are recommended for all students between Year 3 and 6:

- **minimum password length** of 6 characters

- **password expiry** every 400 days (this requirement is optional if multi-factor authentication is available and enabled)
- **password history** preventing users from using any of the previous 12 passwords
- **minimum password age** of 1 day
- **account lockout** after 10 invalid attempts for 10 minutes.

Year 7 and above

The following password settings are recommended for all students in Year 7 and above:

- **minimum password length** of 8 characters
- **password expiry** every 400 days (this requirement is optional if multi-factor authentication is available and enabled)
- **password history** preventing users from using any of the previous 24 passwords
- **minimum password age** of 1 day
- **account lockout** after 10 invalid attempts for 10 minutes.

Allocation of passwords

Staff and contractors

When allocating passwords to staff and contractors, the following must be observed:

- Where possible, passwords should be provided to staff automatically without the need for other staff to see or know the password.
- Where this is not possible, passwords must be delivered to the user via a secure means, such as with a sealed envelope or a text message directly to the user's registered mobile phone number. Secret text applications that automatically delete their contents after one view may also be used provided the links are unique and that the username and password are not contained within the same text.
- Passwords must be set to expire upon first login, where possible.
- Default passwords allocated to new staff accounts must be unique for each user. Default passwords such as 'CHANGEME', 'PASSWORD1' or 'TODAY1234', for example, are not to be used.

Students

When allocating passwords to students, schools must take into consideration the capacity and needs of the students when determining the best method for distributing passwords. For younger students (Year 2 or below), passwords may need to be set on the student's behalf, distributed to students on their first day of school and possibly recorded and tracked by a teacher. For older students, schools are encouraged to allow students to manage their own passwords.

If a school determines it appropriate to store and manage student passwords on behalf of the student, the following must be observed:

- Passwords must be stored in a secure document or register.

- Access controls must be used to restrict access only to the teacher.
- Management of passwords on behalf of students should only occur when approved by the site leader.
- Passwords must not follow a regular system or pattern and must be unique and hard to guess. Passwords such as 'Lastname2023', the student's date of birth or ID number, for example, are not to be used.

Password resets

The department provides a self-service password reset facility for users to manage their passwords in a secure manner. When resetting passwords, all staff must adhere to the following:

- Where possible, users must use self-service or automated facilities provided by ICT Services to change their password.
- Where a password is unable to be changed using self-service facilities, passwords must only be changed by either ICT services, ICT personnel, or the site leader.
- A person's identity must be verified either in-person, through verification of identify documents, or based on known secrets or questions.
- After resetting a password, user accounts must be required to change the password on next login.
- Unique, non-standard password must be assigned when the password is reset. Passwords such as 'CHANGEME' or 'TEMPPASSWORD' or 'MONDAY01' are not to be used.
- Password reset requests must be formally tracked in an appropriate ticketing system or logs.

Management of passwords

All users are required to keep their passwords secure. Specifically:

- passwords must not be reused across the user's other accounts, eg personal email, Facebook, online shopping, etc.
- passwords must not be shared with anyone, including other corporate staff, teaching staff, students, or family members.
- the 'remember password' feature of applications or in web browsers must not be used on shared devices.
- passwords must not be written down, eg on a sticky note posted on a computer, or any other visible location.
- the usage of secure password management tools approved by ICT personnel is permitted and encouraged.
- if an account or password is suspected to have been compromised, the incident must be reported to the ICT Service Desk and site ICT personnel and all compromised passwords must be

changed.

- provision of access to an individual's personal files or system privileges may only be permitted upon documented authorisation from the ICT Cyber Security Team or site leader.
- password cracking or guessing software may be performed on a periodic or random basis as authorised by the Chief Information Officer. Users will be required to change any password guessed or cracked during one of these scans.

Additional requirements for service accounts

In addition to the requirements to securely manage passwords, the following requirements also apply to the management of passwords for service accounts:

- service account passwords must not be stored as clear text – storing of clear text passwords in source code, service tickets or knowledge base articles is strictly prohibited.
- service account passwords must not be inserted into email messages or other forms of electronic communication.

Endpoint security and maintenance

Configuration baselines

The following defines the standard configuration requirements for each of the department's desktops and laptops. These requirements should be applied via a standard operating environment (SOE) template. The department's ICT personnel must ensure that:

- all security updates for the operating system are installed prior to deployment
- an anti-malware solution approved by the site leader (for schools) or ICT Services (for corporate) is installed and configured to automatically update
- unnecessary operating system services or features are disabled
- remote management access is configured so that only designated management workstations and networks can connect to the device
- insecure protocols such as Telnet, FTP or RDP are disabled, or protected by other secure protocols such as IPsec or SSL/TLS as required
- user sessions are configured to time out and lock after no more than 10 minutes of inactivity
- local administrator rights are disabled for standard user accounts
- security monitoring agents are installed and configured where available
- local accounts are configured to meet password requirements as defined in the password management section
- vendor default credentials are changed
- logging is configured in line with the security logging and monitoring section

- software restrictions are configured (either using an application whitelisting product or operating system software restrictions, eg Windows Defender Application Control for Windows or Gatekeeper for Mac).

Application Whitelisting

Application whitelisting must be implemented across all workstations and servers to restrict the use of unapproved executables, software libraries, scripts, and installers. Operating system software restriction configurations are sufficient as a whitelisting product in most circumstances (eg Windows Defender Application Control for Windows devices, or Gatekeeper for Mac devices).

In instances where application whitelisting cannot be applied to a workstation or server, an exceptions register must be maintained that is visible to site leadership as well as site ICT personnel. The exceptions register at a minimum must include the following information: asset/serial number of the device, justification for why application whitelisting cannot be enforced on the device, and what are the required actions that would need to be performed to make the device compliant with this standard. The exceptions register must be reviewed on at least an annual basis to ensure that where possible, devices that were previously exempt are made compliant.

eg ICT Cyber Security or site ICT personnel are responsible for reviewing requests for new application whitelisting rules and conducting a review of existing rules at least annually.

Vulnerability management

ICT personnel are responsible for monitoring relevant information services (eg State Government vulnerability alerts, assert, vendor advisories) to identify the latest security vulnerabilities and how to remediate them.

ICT Services or site ICT personnel are responsible for ensuring that scheduled patching takes place.

The department's risk management procedures must be followed to prioritise the implementation of identified mitigations or treatments. Identified security vulnerabilities in applications and operating systems must be patched or mitigated in accordance with the level of risk, as follows:

- **Extreme** – 48 hours
- **High** – 2 weeks.

Medium or Low vulnerabilities should be prioritised by system and risk owners on a case-by-case basis based on other mitigating factors, resources, etc.

When categorising a vulnerability, ICT personnel should consider the likelihood of the vulnerability being exploited, the impact of the vulnerability being exploited, and any existing mitigating controls or factors that reduce the likelihood or impact.

Standard and non-standard software

ICT Services or site ICT staff are responsible for maintaining a list of standard software, add-ins and extensions that can be installed on workstations (either automatically or as required for individual users) for corporate staff. Site ICT personnel are responsible for maintaining a list of standard software for school-

managed networks.

Unauthorised or unlicensed software, add-ins or extensions must not be installed on, attached to, or operated on any department ICT facilities.

Where non-standard software is required, it must be approved by an individual's line manager and either the site leader (for school staff) or ICT Cyber Security (for corporate staff). Use of non-standard software must only be approved under the following circumstances:

- reasonable research has been conducted to ensure the vendor is reputable
- the software has been reasonably tested to ensure it is not known to be malicious
- software integrity checks have been performed to ensure authenticity (eg checksum).

Unsupported and end-of-life systems

Endpoints with operating systems which are unsupported, end-of-life or are no longer receiving security updates from vendors are strictly prohibited unless an exemption has been obtained (see Exemptions).

Server security and maintenance

Configuration baselines

Standard configuration requirements for servers hosted in environments operated by sites or the department are defined below. ICT personnel must ensure that:

- sensitive and non-sensitive systems and environments (eg production, testing) are segregated where feasible
- approved anti-malware applications are installed. The ICT Cyber Security managed Palo Alto Cortex XDR product is recommended for all sites
- all security updates for the server operating system are installed prior to deployment
- unnecessary operating system services or features are disabled
- remote management access is configured so that only designated management workstations and networks can connect to the device, where possible
- the following access is limited to users with a defined business need:
    - console or interactive access
    - local administrator access.
- the display of previous usernames at operating system login prompts are disabled
- local accounts are configured to meet password requirements as defined in the password management section
- functionality that automatically executes code on removable media is disabled, eg Windows auto run

- synchronisation with an authorised central time source is enabled
- logging is configured in alignment with the security logging and monitoring section.

Application whitelisting

Application whitelisting must be implemented across all servers to restrict the execution of unapproved executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets.

In instances where application whitelisting cannot be applied to a workstation or server, an exceptions register must be maintained that is visible to site leadership as well as site ICT personnel. The exceptions register at a minimum must include the following information: asset/serial number of the device, justification for why application whitelisting cannot be enforced on the device, and what are the required actions that would need to be performed to make the device compliant with this standard. The exceptions register must be reviewed on at least an annual basis to ensure that where possible, devices that were previously exempt are made compliant.

ICT Cyber Security or site ICT personnel are responsible for reviewing requests for new application whitelisting rules and conducting a review of existing rules at least annually. Server application whitelisting may be handled on a server-by-server basis or sets of rules applied across different groups of servers.

Software restrictions using in-built operating system features such as AppLocker or Windows Defender Application Control (for Windows), or Gatekeeper (for Mac) may be used by schools to facilitate application whitelisting.

System backup

Data custodians are responsible for determining the backup strategy and methods, including recovery points, implementation, and test procedures.

Offsite backup arrangements (ie backups stored at another physical location or stored in another secure data centre) must be implemented to limit potential for total loss. Periodic testing of backup procedures must take place on a scheduled annual basis, or when significant IT infrastructure changes occur.

In the event of server compromise (eg through malware, virus, or other malicious activity), staff should rebuild the server from a backup rather than relying on removal tools, where possible. This approach limits the risk of future system compromise as a result of introduced vulnerabilities that may not be identified after a server's malware has been removed. Backup arrangements must be maintained in line with the secure information handling section of this document.

Physical security

Server security must be maintained in line with the physical and environmental security section of this standard.

Only authorised staff shall be permitted to access areas where servers reside.

Integrity controls

The successful compromise of a server or an associated system may result in changes to its data.

The department and sites should use suitable monitoring tools to alert responsible staff to changes to key files on the server, allowing an assessment to be made as to whether the change was the result of a hostile attack.

Vulnerability management

Personnel managing servers are responsible for monitoring relevant information services (eg State Government vulnerability alerts, AusCERT, vendor advisories) to identify the latest security vulnerabilities and how to remediate them.

The department's infrastructure personnel or site ICT personnel are responsible for ensuring that scheduled patching takes place.

The department's risk management procedures must be followed to prioritise the implementation of identified mitigations or treatments. Identified security vulnerabilities in applications and operating systems should be categorised by ICT personnel, and patched or mitigated in accordance with the level of risk, as follows:

- **Extreme** – 48 hours
- **High** – 2 weeks.

Medium or low vulnerabilities should be prioritised by system and risk owners on a case-by-case basis based on other mitigating factors, resources etc.

When categorising a vulnerability, ICT personnel should consider the likelihood of the vulnerability being exploited, the impact of the vulnerability being exploited, and any existing mitigating controls or factors that reduce the likelihood or impact.

Unsupported and end-of-life systems

Servers with operating systems which are unsupported, end-of-life or are no longer receiving security updates from vendors are strictly prohibited unless an exemption has been obtained (see exemptions).

Mobile device and removable media

Acceptable use of department mobile devices

Mobile devices include mobile phones, tablets, USB drives, external hard drives, and laptops. The following must be observed with respect to the use of mobile devices on the school or department network:

- Only mobile devices owned and/or operated by schools or the department may be used to connect to department infrastructure or services, unless connecting to a network segment specifically designed for personal or unmanaged devices.
- Department-owned mobile devices must not be used by an employee's family or friends.

- Any installed management software, such as anti-malware software, must not be removed and must be kept up to date on devices.
- USB thumb drives or portable drives from an unknown or untrusted source are not to be connected to department equipment.
- The user of the device must notify the ICT Service Desk or site ICT personnel immediately upon loss, theft, or suspected loss/theft of the device. Where possible, the contents of the device will be remotely erased, and the services associated with the device must be disabled.
- Mobile device usage must comply with the department's ICT acceptable use agreement (staff login required).

Schools must ensure that acceptable use policies are applicable to students, and students are aware of their responsibility to report lost/stolen devices.

Personal devices

Personal and BYOD devices must only be allowed to access the network provided the following is implemented:

- a dedicated network segment has been established for personal or un-trusted devices
- the network segment is limited only to Internet access – personal or un-trusted devices must not have access to corporate or school network drives or services
- users are still required to authenticate on the network to ensure that any internet or network logs are able to be traced to a specific user.

By connecting a personal device to the network, the user's device becomes subject to the controls and requirements defined in this standard, including the department's authority to remotely wipe the device should a security compromise be suspected.

Conditions of use

Extending this standard's requirements, department-owned and personally owned mobile phones and tablets used to connect with the department's ICT assets require acceptance and implementation of the following conditions:

- The user of the device must accept the installation of a department-controlled profile, where it is deemed necessary by ICT Services or the site leader, on the device. This profile must enforce certain configuration parameters, which may include, where possible:
    - an inactivity timer lock with a passcode
    - a maximum of 60 days of mail and calendar items stored on the device
    - multi-factor authentication for access email accounts on initial set up and each time the user account password is changed.
    - encryption.
- The user of the device is responsible for ensuring that device software is updated appropriately to

ensure security risks are not introduced to the department's infrastructure when connected.

- The department will reserve the right to erase the contents of the device and/or disable the device at any time, at the discretion of ICT Cyber Security or site ICT personnel. This includes personal devices that hold departmental data if staff choose to user personal devices for this purpose.

Site leaders (for schools) or ICT Services for corporate staff must obtain and refresh acceptance of these requirements from staff prior to issuing a mobile device or allowing a personal device to connect to the network. A template user agreement is available from ICT Services.

Protection of information on mobile devices

The following must be observed by staff to securely protect information on mobile devices to store or process sensitive information:

- Encryption must be configured for all mobile devices and removable storage, where possible.
- Every reasonable effort must be made to ensure that the department's information is not compromised using mobile devices in a public place. Screens displaying information classified as OFFICIAL: Sensitive or higher must not be seen by unauthorised persons.
- Mobile devices are not to be used as the sole repository for department information. All department information stored on mobile devices must be regularly backed up to an appropriate network location, cloud service, or application intended and approved for storing official information.
- Officers from ICT Services will provide guidance, upon request, on user responsibilities and options in relation to data back-up for important information that is stored locally. These back-ups must be given adequate protection against theft or loss.
- Never leave mobile communication devices unattended in a public place, car (even if locked), or in an unlocked house or office. Where possible, devices must be physically locked away, or special locks used to secure the equipment. Devices must be password protected with auto-lock where possible.
- When travelling, mobile communication devices such as laptop computers should be transported as hand luggage rather than in the hold of the plane and should be stowed under the seat not in overhead lockers.
- Information transported on mobile devices outside of department environments must satisfy the requirements defined in the secure information handling section.

Security logging and monitoring

Scope of logging

At a minimum, all systems that handle security-classified information that accept network connections or make access control (authentication and authorisation) decisions should record and retain logs and/or audit trail information in accordance with these standards. This may apply to activities and systems including:

- web browsing
- network hardware (eg switches, routers, wireless access points, etc)
- network-related infrastructure (eg servers, load balancers, cloud solutions, etc)
- applications responsible for any form of user authentication and authorisation
- Allowed and blocked execution events
- user devices
- databases.

Logging requirements

Logs are collected for purposes such as auditing access, investigating incidents, reviewing disaster recovery, and complying with state and federal retention requirements.

Where feasible, logs shall identify or contain at least the following elements, either explicitly or can be unambiguously inferred by a reviewer or automated system:

- type of action (eg authorise, create, read, update, delete and accept network connection)
- subsystem performing the action (eg process or transaction name)
- identifiers for the subject requesting the action (eg username, computer name, IP address or MAC address)
- identifiers for the object that the action was performed on (eg file names accessed, unique identifiers of records access in a database, query parameters used to determine records accessed in a database, computer name, IP address and MAC address). Note that such identifiers should be standardised in order to facilitate log correlation
- before and after values when action involves updating a data element, if feasible
- date and time the action was performed, including relevant time-zone information if not in Coordinated Universal Time (UTC)
- whether the action was allowed or denied by access control mechanisms
- description and/or reason codes of why the action was denied by the access control mechanism, if applicable.

Activities to be logged

Where possible, logs and/or audit trails must be collected for:

- all activities performed by privileged users, ie system administrators
- create, read, update, or delete information classified as OFFICIAL: Sensitive or above, including authentication information such as passwords
- user authentication and authorisation for activities such as user login and logout
- grant, modify or revoke access rights, including adding a new user or group, changing user privilege levels (eg AD group membership), changing file permissions, changing database object permissions, changing firewall rules, and user password changes
- system, network, or services configuration changes, including installation of software patches and updates, or other installed software changes
- application process start-up, shutdown, or restart
- application process abort, failure, or abnormal end, especially due to resource exhaustion or reaching a resource limit or threshold, eg CPU, memory, network connections, network bandwidth, disk space or other resources
- the failure of network services such as DHCP or DNS, or hardware failure
- detection of suspicious/malicious activity such as from an Intrusion Detection/Prevention System, or other monitoring or security systems
- Connections to and from internet resources, applications, and websites.

Log management and retention requirements

Application and system owners are responsible for ensuring logs are retained and disposed in accordance with the information and records management policy.

If the information and records management policy is not clear on a specific type of record or logs, system and application owners should aim for a retention period of 2 years. However, in determining the retention period, application and system owners need to consider the following:

- the sensitivity of the information or functionality provided by a system
- the primary purpose of logs (eg investigating misconduct, system performance, or troubleshooting)
- the level of risk associated with a particular system
- system limitations or performance impacts of logging functionality.

At a minimum, application and system owners must ensure the following:

- logs are of an appropriate size such that they do not fill up and overwrite existing records in a way that causes non-compliance with retention policies, ie overwriting existing records before they can be backed up
- logs are forwarded to a centralised log server for archival purposes, where possible

- copies of logs are properly archived and rotated offsite, where possible
- logs and/or audit trails are secured so that they are protected from unauthorised modification (including unauthorised modifications attempted by administrators)
- logs are monitored using automated alerts and/or periodically reviewed manually
- the log retention strategy is sufficient to reasonably troubleshoot issues or investigate misconduct given the nature of information or functionality provided by the system.

Network security

Network management

ICT personnel must ensure that the following is complied with in relation to network management:

- Security controls must be established and implemented to safeguard information passing over public networks and for the protection of connected systems and networks.
- Network modifications are subject to change control and approval processes. Changes made in the corporate environment require approvals from the Change Advisory Board (CAB). Changes made to schools require approval from the site leader or delegate.
- Appropriate security control mechanisms must be implemented to ensure that diagnostic ports or management interfaces are only accessible to authorised personnel.
- An accurate time source must be established and used consistently across systems and network devices.

Network access

Adequate security controls must be in place to restrict unauthorised access. ICT personnel must ensure the following:

- Access to network services must be limited to that required to meet business needs.
- All network connections with external environments must have controls to prevent unauthorised access.
- All remote access to department or school systems is to be authorised by ICT Cyber Security and must be compliant with the department's ICT Acceptable Use Agreement (staff login required).
- Remote access to corporate or school networks must be conducted via a secure connection authorised by ICT Cyber Security.
- Network segregation is to be implemented to segregate sensitive environments from general environments to limit damage in a situation where one environment is compromised.

Third party products and tools that allow staff or vendors to connect into department devices and networks remotely using non-approved connections are strictly prohibited.

Network operations

- Data passing across department and public networks must be protected (eg encrypted) from compromise commensurate with risk, as determined by ICT Cyber Security or site ICT personnel and accepted by the site leader.
- All new network services shall be assessed in terms of potential security features and reporting capability.
- Controls are to be implemented to protect information assets from illegal software, eg malware or any software designed to circumvent controls.
- Encrypted network connections originating from external sources (eg VPN traffic) must be decrypted and scrutinised by the implemented security solutions (eg perimeter firewall, anti-malware) before connections are permitted to the department's network.
- Network monitoring tools must be used to identify signs of malicious activity, such as unauthorised connections or unrecognised devices connecting to the network. Connections found responsible for suspected malicious activity must be disconnected from the network.

Wireless networks

The following requirements apply with respect to wireless networks:

- All wireless access points (WAPs) connected to a department network must be approved by ICT Services, or the site leader for school-managed networks, before installation.
- Controls over WAPs are to follow the same requirements as for wired networks, including but not restricted to:
    - network registration
    - up-to-date patches
    - insecure or unneeded services should be disabled
    - strong passwords in line with the password management section
- Wireless networks are to be segregated from the department's network using access control mechanisms (eg access restricted VLAN, firewall).
- Access to department infrastructure via WAPs must utilise industry accepted authentication and encryption mechanisms (ie WPA2, WEP and WPA are not sufficient)
- All wireless communication between department devices and networks must be encrypted, with the exception of wireless networks providing internet-only access for guest users (see below)
- Effective physical security is to be applied to hardware associated with WAPs, in line with the physical and environmental security section of this standard
- All wireless network equipment is to be periodically scanned for vulnerabilities to assess the needed base level of security relevant to the network.

Personal devices and guests

Personal and other untrusted devices must only be connected to a dedicated segment specifically for these types of devices and implementation must comply with the mobile device and removable media security section and the security logging and monitoring section.

Visitors are only to be allowed to connect to a designated guest network.

Internet of Things (IoT)

Internet of Things (IoT) refers to devices on the network that do not typically require users to authenticate, often embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the Internet. Common examples include smart refrigerators, smart TVs, security cameras, and personal or home assistant devices (eg Google Home, Amazon Echo).

IoT devices must only be connected to a dedicated network segment specifically for these types of devices and implementation must comply with the endpoint security and maintenance section, where possible. At a minimum:

- administration consoles (if they exist) must be password protected
- default vendor-supplied passwords must be changed
- devices should be configured to automatically update firmware and/or software
- devices should be configured use secure protocols to encrypt data in transit.

Network documentation

The department's network architecture must be documented, showing the department's internal network structure, and incoming/outgoing egress points.

Information flows associated with critical processes must also be documented, listing:

- the type of information passing
- the classification of information
- the parties with whom the information is being exchanged
- controls in place to protect the information.

ICT Services and site ICT personnel are responsible for documenting, maintaining, and securing network-related documentation pertaining to the department's corporate and schools' networks respectively.

Physical security

Computer rooms

All sites must implement appropriate controls to restrict access to computer rooms to authorised personnel.

Specifically, sites must:

- implement physical controls (eg locks, key card scanners, etc.) to restrict access
- review access lists, where applicable, on a periodic basis to ensure access to restricted areas is appropriate
- maintain a secure audit trail or log of access to restricted areas and visitors
- ensure contractors and suppliers wear a visible form of identification and are escorted in restricted areas at all times.

Workstations and work areas

All sites must ensure staff implement the following to protect classified information in work areas:

- Personnel must lock or log out of their devices when leaving their work area.
- Personnel must maintain clear and tidy work areas. Information classified as OFFICIAL: Sensitive or higher must be securely stored when not in use.
- Portable media must be securely stored when not in use.
- Whiteboards and other display sources in shared areas must be cleaned of any information classified as OFFICIAL: Sensitive or higher after use.

Equipment security

Network equipment must be appropriately secured so that it cannot be directly accessed or harmed as follows:

- Network equipment or hardware connected to the network must be located within the physical security perimeter, and access to areas housing the equipment must be restricted to authorised employees.
- Physical security for these areas must be sufficient to ensure that the assets in these areas are adequately protected against loss, damage, or any other risk.
- Delivery of equipment or other goods into any controlled area must be actively supervised and managed.
- Building management systems must provide automatic alerts when relevant thresholds are exceeded.
- All equipment must be correctly maintained to ensure its availability and integrity where required.

Environmental security

Controls must be in place to secure ICT assets from damage from the elements as follows:

- Alternative power sources must be sufficient to cope with business requirements for continued system operation in the event of a loss of power.

- Cabling must be appropriately protected from accidental or deliberate damage or unauthorised access.
- Information assets vulnerable to environmental threats, namely fire, flood, and earthquakes, must have appropriate protection from these threats, where feasible.
- ICT assets must be suitably protected from extreme temperature and moisture variations through the deployment of adequately maintained equipment.

Application security

System development

The following requirements must be followed to ensure that source code is developed and contained securely:

- Security reviews must be embedded in various stages at the software development lifecycle (SDLC). This includes the design stage, of the SDLC process. Considerations to be made include, but are not limited to:
    - injection flaws (eg SQL injection)
    - buffer overflow
    - broken access control
    - cross-site scripting
    - insecure cryptographic storage
    - insecure communications
    - improper error handling.
- Software development environments (eg development, testing, and production) must be segregated.
- Suitable tests based on established testing criteria must be performed on new and modified systems during development and prior to acceptance.
- Test data must be protected and controlled such that it does not breach the confidentiality which has been afforded to it in the production environment.
- Code audits or security assessments must be conducted periodically to detect any malicious or vulnerable code that is present before introduction to the production environment.
- Web applications under development must be tested for existence of web application vulnerabilities following significant changes, with vulnerabilities addressed before deployment to the production environment.
- Source code repositories must be adequately secured to protect against misuse.
- All software versions must be secured using version control and access restrictions.

- Vulnerability assessments and penetration tests must be conducted before systems are deployed to production, after significant changes have been made, and on a periodic basis at the discretion of the system owner.
- It is recommended that in addition to the above, all software development should be in line with the OWASP Application Security Verification Standard.

Outsourcing

The following requirements must be met when outsourcing the development of code to a third-party contractor or vendor:

- The software development outsourced to a supplier must be supervised and monitored to ensure that all department security requirements are met.
- When entering into outsourcing arrangements for software development, legal advice must be sought to ensure that the department's rights and interests are protected.
- Contracts with suppliers must meet the requirements outlined in the ICT vendor security section of this standard
- Security and privacy requirements must be formalised in contracts with external developers.
- The right to audit must be included in all outsourcing contracts and must extend to outsourced contracts and vendors.
- For the purpose of this document, contractors hired for in-house development must:
    - be provisioned with a department device and/or virtual machine instance to conduct their duties
    - be provisioned with an account configured in accordance with the access management section of this standard.

System acquisition

The following requirements must be met when the department acquires or inherits ownership of a new system:

- Acquisition of new systems (ie software, services and infrastructure, or physical locations that host such items) must be authorised by ICT Services or site leaders as appropriate.
- Documented business requirements for new systems, or enhancements to existing systems, must specify the requirements for security controls.
- Specifications must consider the automated controls to be incorporated into systems together with supporting manual controls.

Vendor Security

Access approval

Approval for access to information assets by vendors must be obtained from the information owner. For the purposes of this standard, school site leaders are the information owners. For corporate systems, ICT Services are responsible for approving and administering access.

Access provided to information assets for vendors or their representatives must be the minimum needed, consistent with business requirements and the access management section of this standard

Contracts with vendors

Security impacts and risk must be considered prior to engaging any ICT service providers, including support services, cloud vendors and software as a service. ICT Services must be consulted on all corporate contracts, or contracts that impact multiple schools or are department wide. Schools are encouraged to engage with local site ICT personnel or ICT Services prior to engaging with vendors. All contracts must comply with department procurement policies and procedures.

The contract and, where applicable, service level agreements, must clearly specify:

- the contract owner
- confidentiality requirements
- that engagements with the department must comply with the secure information handling section of this standard and requirements, including the ICT Acceptable Use Agreement (staff login required)
- the types of access to information assets provided to vendors, the means by which it will be provided, the duration of access and the means of changing access, should it be required
- expectations regarding the vendor's security controls to ensure that they are consistent with the department's standards and information asset classifications
- requirements mandated by the governing law, legal and contractual obligations, including the *Privacy Act 1988*, the *State Records Act 1997*, Premier and Cabinet circulars, and any other applicable governing requirements – all sites should consult Legal Services to ensure these requirements are addressed in each case
- that individuals who have access to the department's information assets are bound by the relevant vendor contract
- background verification requirements for the personnel resources provisioned by the vendor, based on the classification of information being accessed. These background verifications must be able to be verified upon request
- any requirements associated with the ownership of intellectual property (including passwords).

Other contractual specifications that may be applicable include:

- where the vendor has access to the department's ICT assets, an appropriate clause to allow the

department to conduct audits, as deemed necessary, of the vendor's conformance to the department's information security standards

- vendors developing software for the department must include the requirement to follow secure development practices and that the software developed is secure, and in line with the application security section of this standard
- resilience and recovery requirements based on the criticality of the services provisioned by the vendor to the department's operations, ie business continuity and disaster recovery plans
- requirements for the return or disposal of the department's ICT assets on termination of the contract.
- requirements to ensure sensitive information is handled in accordance with the requirements defined in the secure information handling section of this standard, in particular, those requirements relating to storage of sensitive information in third party cloud environments.
- should ICT support services be outsourced to a vendor then any vendor set service or system account usernames and passwords on systems or networking equipment is shared (including when updated) with the site leader who is responsible to securely record and retain this information.

The SACSF Guideline - Engaging Suppliers and Cloud Security must be referred to for further detail regarding contractual considerations and supplier engagements.

Vendor physical and network access

In conjunction with other security requirements described:

- vendor devices are not to be connected to the department's network without approval from ICT Cyber Security or site ICT personnel for schools and preschools.
- vendor connections terminating within the department's network boundary must be approved by ICT Cyber Security and suitable controls must be put in place to prevent a vendor from having unrestricted remote access to the department's information resources.

ICT Risk Management

When is an ICT risk assessment required?

Information on the process to conduct an ICT Security Risk Assessment can be found by visiting this link.

An ICT risk assessment is **recommended** for schools (approved by the Site Leader) and **required** for Corporate and approved by the business unit Director where the product or service being procured or implemented:

- Stores, transmits, processes or has access to corporate, personal or sensitive information (including but not limited to, first names, surnames, date of birth, home/mailing addresses, personal email addresses, financial information)
- Configuration changes to web or network filtering tools to allow or unblock third party websites or

applications where there is intent to share personal or sensitive information with a third party.

- Configuration changes to web or network filtering tools to allow or unblock third party websites or applications that host user-generated content (eg social media, search engines, content delivery networks).
- Implementation of applications or websites that collect, transmit or store sensitive information, even if stored on-premises.
- Widescale deployment of software (eg to an entire site, or the entire department).
- Significant network architectural changes.
- Implementation of large volumes of data from one system to another.
- Implementation of social media or other third-party platform to communicate with the public or external individuals on behalf of a school or department (eg setting up a school Facebook page or using third party mass-mailing service providers).

Risk assessments must also be considered if any of the following are present:

- Where the product or service is critical to business operations
- A perceived threat or security risk to the wellbeing of staff or students
- Potential for damage to ICT infrastructure or interruption of ICT services
- Potential for damage to the department's reputation or possibility of media coverage

Minimum risk considerations

At a minimum, ICT risk assessments need to consider the applicability of the following risks:

- **Data sovereignty** – Differing privacy laws in other jurisdictions (ie overseas) allow third parties to share or disclose personal information with other third parties.
- **Data breach –** Department or third-party server infrastructure is compromised by cyber criminals and used to access or exfiltrate sensitive information.
- **Unauthorised disclosure** – Department or third-party service provider disclose personal or sensitive information without consent (intentionally or unintentionally).
- **Inappropriate content** – Children access or share inappropriate content online.
- **Inappropriate contact with children** – Children are contacted inappropriately by staff or third parties or use online communication tools to contact other staff or students inappropriately.
- **Fraudulent transactions** – Financial systems are used to process transactions without authorisation.
- **Account compromise** – An account is compromised resulting in unauthorised access to sensitive information and other systems (if users share passwords across multiple systems).
- **Service outage impacts business operations** – system experiences a service outage which impacts the site's ability to continue business operations.
- **Network bandwidth impact** – Network bandwidth is throttled due to unforeseen increase in

network traffic leading to service outages.

- **Loss of critical data** – Critical data is lost due to unforeseen circumstances and is unable to be recovered.
- **Loss or damage of physical assets** – Physical servers and other infrastructure are lost, stolen, or damaged by environmental factors (eg fire, flood, earthquake).
- **Malicious software** – Malicious software is introduced to the network or downloaded by users resulting in compromised endpoints.

Risk analysis and evaluation

ICT services may provide additional tools to assist staff in completing a risk assessment that complies with the risk management policy (PDF 169KB) (staff login required) and risk management procedure (staff login required).

At a minimum, the risk assessment must detail:

- identified ICT security risks
- likelihood, impact, and risk rating of each risk
- existing and planned controls to manage and mitigate risk
- residual risk after planned controls have been implemented.

Risk likelihood

When measuring the likelihood of a risk, staff should consult the department's risk assessment criteria matrix (PDF 218KB) (staff login required). In addition, staff should also consider how often security events typically occur on a day-to-day basis as detailed below:

Impact	Description
Almost certain	• Security event typically happens on a daily basis.
Likely	• Security event typically happens on a monthly basis.
Possible	• Security event typically happens at least once a year.
Unlikely	• Security event typically happens once every 5 years.
Rare	• Security event typically happens every 10 years.

Risk impact

When measuring the impact of a risk, staff should consult the department's risk assessment criteria matrix (PDF 218KB) (staff login required). In addition, staff should also apply the following criteria when measuring the impact of ICT cyber security risks.

Impact	Description
Catastrophic/Critical	• Personal information of the entire department exposed.
Major	• Personal information of an entire site or multiple sites exposed. • Service outage impacting multiple sites or department wide.
Moderate	• Personal information of large group of users (100+) • Service outage impacting an entire site.
Minor	• Personal information of single individual or small group exposed. • Service outage impacting a small group of users.
Insignificant	• No exposed records or personal information, and no service outage.

Risk treatment, acceptance and monitoring

When determining whether a risk is acceptable or needs additional controls to manage or monitor the risk, staff should consult the department's risk assessment criteria matrix (PDF 218KB) (staff login required).

ICT cyber security risks must be treated and monitored in accordance with the risk management policy (PDF 169KB) (staff login required) and risk management procedure (staff login required).

Personnel security and acceptable use

Employee acknowledgement

A standard template (staff login required) is provided for managers and site leaders to obtain written acknowledgement from staff of what is considered acceptable use of ICT resources, and consequences of inappropriately using department assets. Users of the department's ICT resources must:

- understand and adhere to the requirements of this standard
- use school or department ICT facilities in an appropriate and professional manner in accordance with the Code of Ethics for the South Australian public sector
- follow the directions of ICT personnel in relation to their use of school or department ICT facilities
- acknowledge that violations of this standard, depending on severity and nature, may result in reprimand, loss of ICT access privileges, termination of employment or any other appropriate disciplinary action.

Student acknowledgement

A standard template (staff login required) is provided for schools to obtain written acknowledgement from students and families of what is considered acceptable use of school resources, and consequences of

inappropriately using school assets. This template is provided as an example only - schools may choose to modify this template to meet the varying needs of students or groups of students.

Recommended periods for re-signing acceptable use agreements

User agreements must be signed before a user is given access to systems. The following is recommended for periodically re-signing agreements:

- For staff
    - if any major changes are made to the agreement
    - if the staff member has been involved with any disciplinary action involving their unacceptable use of ICT assets
- For contractors
    - each time their contract is renewed
    - if any major changes are made to the agreement
    - if the contractor has been involved with any disciplinary action involving their unacceptable use of ICT assets
- For students
    - once per year, generally at the start of the school year
    - if any major changes are made to the agreement
    - if the student has been involved with any disciplinary action involving their unacceptable use of ICT assets.

Staff obligations

All staff using school or department assets are obligated to:

- store and secure official records as required by the *State Records Act 1997*
- manage information in line with its classification, as defined in the secure information handling section of this standard
- protect their username and passwords
- log out and/or lock systems when leaving them unattended
- store equipment in a safe and secure environment when not in use and do not leave assets unattended in public places
- inform site ICT personnel, ICT Services, and their line manager immediately if an asset is lost or stolen
- inform site ICT personnel or ICT Services of any malfunction or damage that occurs
- report any suspicious activity or inappropriate use to site ICT personnel and ICT Services

- report any suspicious emails to education.spam@sa.gov.au
- comply with the South Australian Public Sector Code of Ethics
- Upon termination of an employee or change in roles or permission, department equipment must be returned, and all department information securely backed up. Where personal devices were used for remote work, all department information must be removed.

Unacceptable use of ICT assets

The following is considered unacceptable use of school or department assets and may result in disciplinary action:

- Use of ICT assets to access or share inappropriate content on the Internet (eg offensive or sexually explicit content).
- Sharing of sensitive, personal, or official information to unauthorised third parties.
- Downloading non-standard software that has not been approved by the site leader or ICT Services.
- Making comments that reflect poorly on the department or its employees, students, and other stakeholders.
- Illegally downloading, storing, transferring, or sharing copyright materials.
- Recording and sharing videos or photos of students without parental consent and approval of the site leader.
- Use of assets to compromise other systems via security holes or exploits or using equipment to search for security holes or exploits that may exist on other systems without appropriate approval from a site leader or ICT Services.
- Any activity that maliciously destroys, alters, dismantles, disfigures, prevents rightful access to or otherwise interferes with the integrity of any electronically stored information.
- Attempts to gain unauthorised access to a system, resource, or entity.
- Spamming (bulk broadcasting of promotional material or emails), including chain letters.
- Use of systems to bully staff or students.
- Promotion of political lobbying.
- Any activities that intentionally degrades or disrupts performance of ICT assets.
- Development or distribution of malicious software or malware.
- Sending messages with intent to conceal or misrepresent the identity of the sender.
- Sending any messages or emails that suggests they have a level of approval that they do not have.
- Using unauthorised personal devices (ie mobile phones, tablets, laptops) to store work information, or to connect to school or department networks unless using a remote working solution approved by ICT Services.

- Revealing an account password to others or allowing others the use of an account (this includes family and other household members when work is being done at home).
- Any other activities which violate any State or Commonwealth laws.

Additional requirements for working remotely

When working remotely, staff must adhere to the following:

- Personal devices should not be used to access department systems or information unless authorised by ICT Services or the site leader.
- Staff must take reasonable measures to securely stow devices containing department information when not in use to prevent misuse, loss, or theft.
- Remote access equipment must not be shared with unauthorised users such as family or friends.
- Devices connecting remotely to the school or department network must use a connection method approved by ICT Services.

Copyright infringement

Employees must not carry out activities that violate the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, similar laws, and regulations. This includes, but is not limited to, the unauthorised use and distribution of copyrighted material, copyrighted images from books, copyrighted music and unlicensed ('pirated') software. Employees found to be engaging in activities contrary to this standard will be subject to disciplinary action which may result in their access being revoked.

Monitoring and compliance

The department reserves the right to record and monitor ICT services, systems, and equipment for the purposes of managing system performance, monitoring compliance with policies and standards, or as part of disciplinary or other investigations. This includes, but is not limited to, access to department mailboxes, email data, network drives, cloud storage, and files.

Secure information handling

Information classification

Information owners are required to classify information assets to ensure that they are handled and secured appropriately commensurate to the sensitivity of the information.

Department information is to be classified as per the South Australian Information Classification System (ICS). Only the following classifications may be used:

- **UNOFFICIAL -** can be used for non-work-related information (including non-work-related emails) and other non-sensitive work that is stored or processed on department or school assets.
- **OFFICIAL -** describes routine information created or processed by the South Australian public sector with a low business impact. Day to day work-related information that is not personal in nature

typically falls into this category.

- **OFFICIAL: Sensitive** - identifies sensitive but not security classified information. Compromise of the information may result in limited damage to an individual, organisation or government generally. Examples may include financial details of individuals, commercial data pertaining to the department or an Australian company, personal information about staff/students, payroll information, and medical information/records.
- **PROTECTED -** a security classification which indicates that compromise of the information may result in damage to the state or national interests, organisations, or individuals. Use of the protective marking is mandatory. Ongoing access to PROTECTED information requires a Baseline security clearance or above.
- **SECRET -** a security classification which indicates compromise of the information may result in serious damage to the state or national interests, organisations, or individuals. Use of the protective marking is mandatory. Ongoing access to SECRET information requires a Negative Vetting 1 security clearance or above.
- **TOP SECRET -** a security classification that indicates compromise of the information may result in exceptionally grave damage to the state or national interests, organisations, or individuals. Use of the protective marking is mandatory. Ongoing access to this information requires a Negative Vetting 2 security clearance or above.

The use of PROTECTED, SECRET and TOP SECRET information within the department is highly unlikely. If you believe to be producing or are in possession of this type of information, the information must be handled in accordance with Annex A, B, and C in the PSPF INFOSEC-8 Sensitive and Classified Information Policy (PDF 1.5MB). Staff should consult the Agency Security Advisor immediately for additional guidance.

Information Management Markers

An information management marker (IMM) may be used alongside a classification and/or any caveats and may be used to help identify information which may have legislative or professional restrictions. IMMs include:

- legal privilege
- legislative secrecy
- personal privacy
- medical in confidence.

Further details regarding caveats and IMMs can be found in the SAPSF INFOSEC 1: Protecting official information policy.

Applying classifications

Information produced within the SA Government must be appropriately protected to prevent from intentional and accidental threats. Assessing the business impact or damage that may occur from the compromise of such information enables the application of the appropriate classification.

The SAPSF how to classify your information (PDF 111KB) tool should be used to guide correctly applying a

classification.

Implications of classifications

Correctly classifying information is important to balance the need to protect information of a sensitive nature with the operational need to distribute and correctly store that information. Applying a classification lower than the business impact level (BIL) exposes information of sensitive nature to unacceptable risk of misuse. Conversely applying a classification higher than the BIL will result in unnecessary restrictions to how the information is shared to parties that otherwise have a legitimate need to know, and a higher resource BIL in the storage of that information.

Principles of classification

Over time, information may require a lower classification level and processes need to support this requirement. For example, an annual report in its compilation stage may be classified as OFFICIAL: Sensitive, however once published it is likely to become OFFICIAL.

There can also be an aggregated effect to data classification, eg information records such as archives will contain various records and are therefore likely to contain information with varying classifications. Furthermore, ICT assets are likely to contain information of varying classifications.

Data repositories and communications are to be managed according to the requirements of the highest classification of data held or transmitted.

External information classification

Information obtained from outside of the department that is received without a defined classification must be handled according to the department's classification scheme as defined above.

The recipient of information obtained from outside of the department labelled with an external classification must ensure that the information classification is understood and applied as expected.

Supplier classification

Where necessary, data sharing agreements are to specify the handling and labelling requirements of the shared information.

Information classified as OFFICIAL: Sensitive or higher must not be shared with any non-department employees unless a non-disclosure agreement is in place that specifically details the obligations of the involved party/parties to protect the security of the information being disclosed.

If there is an ongoing requirement to disclose information classified as OFFICIAL: Sensitive to a partner or external organisation over an extended period, advice must be sought from ICT Cyber Security on whether the controls being applied are appropriate to protect the information, or whether additional controls are required, eg stronger encryption processes.

Classification requirements

The default classification level for all information assets within the department is OFFICIAL. Any information without a classification label is classified as OFFICIAL.

Department personnel must:

- determine appropriate classification levels for information assets
- set classifications at the lowest reasonable level to protect against compromise to secure the confidentiality of information
- ensure all information and emails classified as OFFICIAL: Sensitive or higher are marked with the correct protective markings in accordance with this standard
- ensure that all information is handled according to this standard
- seek permission from the information asset owner to make changes to its classification.

The process of classification may be assisted with the SAPSF classification assessment tool (PDF 111KB).

Labelling

Documents (eg Microsoft Word, Publisher documents) containing information classified as OFFICIAL: Sensitive or higher must be labelled, where possible. Sites should ensure commonly used forms and templates are adequately labelled as required by the SA Government Information Classification System (PDF 227KB).

Emails containing information classified as OFFICIAL: Sensitive or higher must also be labelled. In relation to sending emails, labels must be placed at the top of the email.

Text-based protective markings should be:

- in capitals (other than for information management markets), in a large, plain text font in a distinctive colour (red preferred)
- centred and places at the top and bottom of each page
- separated by a double forward slash (//) to help to clearly differentiate each marking (eg **OFFICIAL: Sensitive // Legal Privilege**).

Information stored as data in electronic systems (eg finance system, payroll system) are not required to be labelled. However, information stored in these systems must be protected in alignment with other sections of this standard.

Information distribution

The distribution of OFFICIAL: Sensitive or higher classified information within the department is limited to those with a valid business reason, and this information must not be published on department or site intranets. This information is only distributable to a third party if confidentiality agreements are in place and approved by the information owner.

Information classified as OFFICIAL may be freely shared within the department and published on the department or site intranet, but judgment should be exercised regarding distribution of this information.

Applying a classification to a document does not exempt it from being released under the *Freedom of Information Act 1991*.

Physical transmission

Physical transfer of information classified as OFFICIAL: Sensitive or higher must be transferred via couriers or registered mail services. Information classified as OFFICIAL may be transferred via other means, but judgment should be exercised regarding the delivery method.

Electronic transmission

Strong encryption must be used when transmitting any information classified as OFFICIAL: Sensitive or higher. Insecure protocols such as Telnet, FTP or RDP should be disabled and not used, or protected by other secure protocols such as IPsec or SSL/TLS as required.

Electronic storage (and cloud storage)

All staff are obligated to ensure all department information is suitably protected from unauthorised access, theft, and loss. Information classified as OFFICIAL: Sensitive and above, including backups, must:

- be stored in an access-controlled repository, with access to the repository limited to only those individuals that need access in line with the access management section
- be stored in a repository which is auditable
- be encrypted at rest, either at the disk, file, or database level. Where encryption has significantly detrimental impact on performance, compensating controls may instead be used as authorised by ICT Cyber Security
- be stored on systems which are periodically patched against known security vulnerabilities.

Cloud solutions include any systems, applications or websites whereby the underlying data is not hosted on physical machines managed and maintained by the department, including the department's Office 365 environment and third-party apps. Use of cloud service providers must only occur under the following circumstances:

- A formal risk assessment has been conducted and approved by a Director or above (for corporate changes) or the site leader (for schools and education sites) in accordance with the risk management policy (PDF 169KB) (staff login required).
- Compensating or mitigating controls have been implemented to appropriately reduce identified risk to an acceptable level in alignment with the departments risk appetite statement.
- ICT Cyber Security has been consulted during the risk assessment and solution design process.
- Where possible, private cloud environments should be used for storing sensitive information. Where public cloud is being utilised, appropriate access management controls must be implemented to segregate tenancies.
- Information that is classified as PROTECTED or above must not be processed or stored outside of Australia.
- The storage of any information that is classified as OFFICIAL or above must comply with SACSF Ruling 2 (PDF 184KB)

- The engagement and contract is compliant with the ICT vendor security section of this standard

If cloud service providers utilise offshore staff to provide support or other technical services, the following mitigating controls must also be implemented:

- Access to sensitive information must be via a secure remote connection approved by ICT Cyber Security to virtual or physical machines hosted on shore.
- Vendor contracts must prohibit offshore staff from saving information classified as OFFICIAL: Sensitive or higher on to persistent storage (ie to disk, screenshots, print etc).

Electronic disposal

Hardware assets and media must be disposed of externally through the computer recycling scheme (CRS).

All hardware assets must be checked prior to disposal to ensure that any information classified as OFFICIAL or higher has been removed or securely overwritten. The presence of internal disks must be checked when disposing of multifunction devices. An internal disk must be removed or overwritten before disposal.

Hardware and non-reusable electronic media must be sanitised before disposal. This may be conducted via digital file shredding, degaussing, physical destruction, or irreversible formatting.

Printing

Information classified as OFFICIAL: Sensitive or higher must be collected immediately from printers.

Paper storage

Information classified as OFFICIAL: Sensitive or higher must be stored in a locked cabinet or container when not in use.

Paper disposal

Information classified as OFFICIAL or higher must be disposed of in a secure disposal facility, such as a secure disposal bin or shredder.

Information must be disposed of in accordance with the standards set out in the SAPSF (PDF 162KB).

Information must be disposed of in accordance with the department's information and records management policy. Copies of documents marked as OFFICIAL: Sensitive or higher, should be shredded or placed in a locked confidential bin for disposal.

Travelling internationally – Department devices and data handling

Additional care must be taken when travelling internationally with department devices including laptops, mobile phones, tablets, and any other device capable of storing department data or connecting to department systems. Laws and privacy expectations differ between countries which may put department information at risk. A risk assessment should be performed when the department becomes aware of the

intent for personnel to travel overseas to understand if the travel is considered high risk.

When travelling internationally, the following precautions must be taken

- All devices should be securely wiped prior to travel and set to a secure baseline standard for the type of device (eg a fully updated basic Microsoft Windows installation. Do not use an 'SOE' image).
- No department data should be stored on the device while travelling or when staying internationally.
- Any department data stored on personal devices should be securely wiped prior to travel.
- Any connections to department systems or data should only be done in accordance with the Access management section of this standard, in particular the requirements on remote access.
- When travelling, devices should be transported as hand luggage rather than in the hold of the plane, and should be stowed under the seat not in overhead lockers.
- If you are compelled to provide access to devices or reveal credentials, this should be reported to ICT Cyber Security immediately.
- If any device has been taken out of sight for inspection by foreign government officials, or have been lost or stolen and later found or returned, this should be reported to ICT Cyber Security immediately.
- Never use chargers supplied by third parties or charge devices in public charging outlets.
- If the device was accessed by unauthorised persons, advice should be sought from ICT Cyber Security prior to connecting the device to any department systems or data.
- Upon return, all user credentials that were used with electronic devices or for remote access should be reset.

Exemptions to standards

Requests for exemptions from any requirements in this standard must have prior approval from the ICT Cyber Security Team.

Roles and responsibilities

Chief Information Officer

Responsible for ensuring that in-scope operations within the department have the appropriate support and resources to meet the requirements of this standard.

Site leaders

Responsible for ensuring that in-scope operations within their site meet the requirements of this standard.

ICT Cyber Security

Responsible for the maintenance and implementation of ICT security standards and procedures, the monitoring of their effectiveness, socializing them, and providing advice and guidance as needed.

Reviewing and approving requests for exceptions to this standard.

ICT personnel

Responsible for supporting the maintenance and implementation of this standard in the environment and managing exceptions to this standard as required under the direction of site leaders.

Responsible for reporting security gaps or non-compliant systems to ICT Cyber Security or the Chief Information Officer.

All employees

Responsible for complying with the standard, and consulting ICT Cyber Security/school ICT staff when further advice and guidance is required.

Glossary

This glossary provides definitions of ICT security terms that are used in various Department for Education ICT security related policies, procedures and standards.

Term	Explanation
Acceptable Use Agreement	An agreement which defines what is, and isn't, allowed when using an organisation's ICT facilities and services. The consequences of not adhering to the agreement should also form part of the agreement.
Access route	The particular path within a network that traffic follows. For example, in terms of ICT security, you may require all traffic which enters your internal network to enter through a filter to remove offensive material – this is the access route.
Access privileges	The particular level of access that has been authorised. For example, a person's access privileges may allow them to use a particular application.
Applications software	A program or group of programs designed for end users. Examples include word processing, spreadsheets and web browsers. Compare with 'System software'.
Authentication	The process of proving the identity of a user. This is usually achieved by supplying a password.
Availability	Ensuring that information and ICT services are available to authorised users, when and where they are required.
Confidentiality	Ensuring that information is only available to those authorised to have access.
Contract owner	The person or entity who has legal ownership or control over a contractual agreement.
Data custodians	This is the individual or group responsible for backup strategy and methods, including recovery points, implementation, and test procedures. This will generally be the site's ICT group.
DMZ (De-Militarised Zone)	An area of an IT network which sits between a trusted internal network, such as a Department for Education network, and an untrusted external network, such as the public Internet. Typically, the DMZ contains devices accessible to Internet traffic, such as web and email servers – for example, you may want anyone to be able to access your web server, but you do not want to allow them into your internal network.

Encryption	The process of hiding the true meaning of data. Data which has been encrypted will be presented as a meaningless collection of random characters, unless you have the appropriate key to decrypt that data (ie. convert back into meaningful data).
External networks	Any non-Department for Education managed network is considered an external network. Examples include the Internet, connections from other Internet Service Providers, or the networks of third-party companies.
Firewall	A firewall is usually located between an internal trusted network, and an external less trusted part of a computer network. Its aim is to protect the internal network from threats originating from outside, by applying rules to the types of network traffic which are allowed through the firewall.
ICT security incident	Any event, actual or threatened, which may impact on the confidentiality, integrity or availability of Department for Education information assets, or which is in breach of Department for Education ICT cyber security standard.
ICT security vulnerability	Any area of vulnerability in Department for Education ICT systems which may be exploited by a threat.
Identification	The process of establishing a claim to be a particular user, identification normally involves supplying a user ID.
Information asset	Any data or information, or related equipment, that contains or processes data or information that is relevant to Department for Education business functions.
Information owner	This is the individual or position responsible for the management and protection of a specific information asset within the department. This includes determining the appropriate classification, handling and access controls and protection for the information in line with department policies and standards.
Integrity	Ensuring the accuracy and completeness of information, and that it has only been modified by authorised people in authorised ways.
Intranet	A website which is only visible within Department for Education. An intranet facilitates communication and sharing of information within the department.
Logical security	Measures to ensure that only authorised users are able to perform actions or access information in a network or computer. It includes elements such as usernames, passwords, and associated access rights.

Malicious software	Sometimes shortened to ‘malware’, this refers to software which is intended to cause harm to a computer by impacting on the confidentiality, integrity or availability of an information asset. Examples of malware include computer viruses, worms, trojans and spyware.
Mobile computing	Covers mobile computing devices including laptop/notebook computers, tablets and smartphones.
Multi-Factor Authentication	Also shortened as ‘MFA’, this refers to providing an additional piece of evidence in authenticating a user in addition to the usual username and password. For example, this could be in the form of a one-time code from an authentication application or by using a physical token key.
Network segment	A portion of a network which has been separated. Networks are usually segmented if they have different security requirements, or different levels of trust. In a school, for example, the administrative network segment, which contains sensitive information, is kept separate from the curriculum network segment, which students access.
Password	A secret string of characters that authenticates a user’s claim to be able to access to a computer system.
Personal information	Includes but is not limited to, full names, date of birth, home/mailing addresses, personal email addresses, and financial information
Phishing email	A type of malicious email that is designed to trick a user into divulging their login credentials, sensitive information, or to provide system access to an unauthorised party.
Physical security	Measures that prevent or deter threats to actual Department for Education facilities, resources or information stored on physical media. Examples include control over who has access to a particular location, environmental controls such as air-conditioning, and guarding against theft of Department for Education ICT equipment.
Privileges	See 'Access privileges'
Remote Access	The ability to access internal resources, from outside. For example, accessing a school’s curriculum server from your home using your private Internet service provider.
Risk	A risk takes into account the likelihood of a threat happening, and the potential impact of that threat.
Risk assessment	The formal process for assessing the level of risk to Department for Education information assets.

Security incident	See 'ICT security incident'
Security weakness	See 'ICT security vulnerability'
Segment	See 'Network segment'
Separation	Describes maintaining various network segments. Separation may be achieved by various means including keeping the networks physically apart or using technology such as routers to make it appear that networks operate independently.
Spam	Spam is electronic junk mail – unsolicited messages sent by email, text message or instant message without the recipient's consent. Spam is usually considered as high volume, but the definition includes even a single email that fits the stated criteria.
System software	Computer software's primary purpose is to help run a computer system. System software includes operating systems, printer drivers, or special programming tools. Compare with 'Applications software'.
Threat	A threat is something, which if it were to occur, would cause harm to an information asset.
Traffic prioritisation	The process of controlling network traffic in order to optimise or guarantee performance for specific applications. For example, videoconferencing requires a certain amount of guaranteed network bandwidth to provide an acceptable end-user experience, therefore this type of traffic may be given a priority over other, less time-critical, applications such as web browsing.
Trust	The level of confidence that a service or facility will preserve the necessary security. For example, a trusted network is one that you are confident will provide the necessary information confidentiality. Internal Department for Education networks are usually considered trusted. See also 'Untrusted'.
Untrusted	In terms of ICT security, if something is untrusted you do not have an adequate level of confidence in its level of security. For example, the Internet is considered untrusted as there is no control over who uses it, or the type of network traffic which may be encountered. See also 'Trust'.
User	In terms of the ICT security documents, includes any person granted access to Department for Education ICT facilities or services located at any Department for Education site. This includes employees, members of the community, contractors and external parties granted access for ICT support.

User ID	Also known as username or login name, a user id identifies you to a computer system. Usually a user id identifies a person, and the associated password, which only the legitimate user knows, proves their identity. See 'Identification' and 'Authentication'.
User identification	The process of managing the identification and authentication of the users of computer facilities and services.
VPN (Virtual Private Network)	Provides a method to securely access an internal network over an untrusted network, such as the public Internet. See 'Remote access'.

Supporting information

ICT Acceptable Use Agreement for corporate users (staff login required)

ICT Acceptable Use Acknowledgement Form Template for Staff (staff login required)

ICT Acceptable Use Acknowledgement Form Template for Students (staff login required)

South Australian Cyber Security Framework (SACSF) (PDF 520KB)

Related legislation

Freedom of Information Act 1991 (SA)

Privacy Act 1988 (Cth)

State Records Act 1997 (SA)

Related policies

Cyber Security Framework Policy (not published)

Cyber security incident response procedure (PDF 199KB) (staff login required)

Record history

Published date: April 2024

Approvals

OP number: 302
File number: DE21/22555
Status: approved
Version: 1.4
Policy Officer: Risk and Compliance Lead, ICT Cyber Security Governance
Policy sponsor: Director, Cyber Security
Responsible Executive Director: Chief Information Officer
Approved by: Director, Cyber Security
Approved date: 5 April 2024
Next review date: 5 April 2027

Revision record

Version: 1.4
Approved by: Director, Cyber Security
Approved date: 5 April 2024
Review date: 5 April 2027

Amendment(s): Added inactive account review for Service Accounts. Removed reference to AppLocker and replaced with Windows Defender Application Control. Added definition regarding separation of privileged and unprivileged accounts.

Version: 1.3
Approved by: Director, Cyber Security
Approved date: 29 February 2024
Review date: 28 February 2027
Amendment(s): Minor amendment to align with 'SACSF Guideline 13 – Cyber security when travelling overseas'.

Version: 1.2
Approved by: Director, ICT cyber security
Approved date: 19 September 2023
Review date: 19 September 2026
Amendment(s): Minor clarification of detail around when an ICT risk assessment is required.

Version: 1.1
Approved by: Assistant Director, ICT cyber security
Approved date: 10 May 2023
Review date: 10 May 2026
Amendment(s): Minor updates to standard

Version: 1.0
Approved by: Manager, ICT Cyber Security
Approved date: 21 October 2021
Review date: 21 October 2024
Amendment(s): New standard.

Contact

ICT Cyber Security

Email: education.ICTCyberSecurity@sa.gov.au

Phone: 8204 1866 (metro) or 1300 363 227 (regional)