Department of
Education

CYBER SECURITY POLICY

CYBER SECURITY PROCEDURES

This PDF contains the following documents

Document 1:
Cyber Security Policy v3.0
Effective: 9 August 2022

Document 2:
Cyber Security Procedures v3.0
Effective: 9 August 2022

Department of
Education

CYBER SECURITY POLICY

EFFECTIVE: 9 AUGUST 2022

VERSION: 3.0

1 POLICY STATEMENT

The Department of Education (the Department) implements measures to protect the Department's electronic information, infrastructure and services from theft, unauthorised access or use, disclosure, modification or destruction during the information lifecycle.

2 POLICY RULES

Employees must:

- only use the Department's Information and Communication Technologies (ICT) resources to which they have been granted access privileges;
- prevent unauthorised disclosure of data;
- prevent unauthorised access to information on an inactive workstation;
- report any suspicion of, or known security threats or breaches, to their line manager or the ICT Customer Service Centre; and
- only use the Department's ICT resources for:
  - work/business and educational purposes; or
  - personal use when it is not for commercial gain or in any way counterproductive to the business of the Department (refer to Telecommunications Use Policy).

Principals must maintain ICT infrastructure security in schools.

Site managers must:

- confirm that employees are made aware of the requirements of this policy; and
- endorse the use of the Department ICT infrastructure by non- employees and confirm supervision by a Department employee.

Guidance

Employees are accountable for all actions and functions performed on their account.

Employees are encouraged to use private email services for conducting personal business rather than Department provided email facilities. There is no expectation of privacy when using Department email for private use.

3 RESPONSIBILITY FOR IMPLEMENTATION AND COMPLIANCE

Principals and line managers are responsible for implementing the policy.

Line managers are responsible for compliance monitoring.

4 SCOPE

This policy applies to all Department employees.

5 SUPPORTING PROCEDURES

Cyber Security Procedures

6 DEFINITIONS

ADMINISTRATOR ACCOUNT

An administrator account is a user account with high-level privileges to make changes on a computer that will affect other users of the computer. Administrators can change security settings, install software and hardware, access all files on the computer, and make changes to other user accounts.

DAM

Department of Education Account Manager (DAM) administrators use the DAM tool to give schools, business areas, employees and visitors access to online services in accordance with their employment position or agreed contract access requirements.

DEPARTMENT EMPLOYEE

A Department employee is any person paid by the Department to provide a service, be it full time or part time as a staff member or teacher, or as a contractor for a short time or long time.

DEPARTMENT ICT INFRASTRUCTURE

All physical, virtual and cloud-based infrastructure and software owned by the Department, including physical or logical connection to the network, including use of Corporate Information Systems.

GENERIC ACCOUNT

An account created which cannot be directly attributed to an identifiable, auditable user. For example, admin front desk, admin temp, temp technician and temp teacher.

NON-EMPLOYEE

A volunteer or a work-place experience person, or other non-paid individual using the Department ICT infrastructure, is not an employee. For the purposes of this policy, they are classified as non-employees.

SERVICE ACCOUNT

A service account is a user account that is created explicitly to provide a security context for services running on Windows Server operating systems. The security context determines the service's ability to access local and network resources. The Windows operating systems rely on services to run various features.

SITE MANAGER

Officers, including principals, site managers and line managers, who have executive responsibility for overall management and control of any Department workplace.

7 RELATED DOCUMENTS

Relevant legislation or authority

Copyright Act 1968

Criminal Code Act Compilation Act 1913 (WA)(CI)
Privacy Act 1988
Public Sector Commissioner's Circular 2010-05 – Computer Information and Internet Security
School Education Act 1999

Related Department policies

Staff Conduct and Discipline
Records Management
Risk and Business Continuity Management
Telecommunications Use
School Security

Other documents

Encryption of Removable Media (staff only)
Corruption Prevention and Detection
Records Management Manual for School and Campus Records (staff only)

8 CONTACT INFORMATION

Policy manager:	Director, ICT Operations and Customer Service
Policy contact officer:	Cyber Security Consultant
Other contact:	Customer Service Centre (CSC) T: (08) 9264 5555 7.30am – 5.00pm Monday to Friday (excluding public holidays)

9 REVIEW DATE

9 August 2025

10 HISTORY OF CHANGES

Effective date	Last update date	Policy version no	Ref no	Notes
18 August 2015		2.0	D15/0301196	Major review undertaken and split into policy and procedures. Endorsed by Corporate Executive 14 November 2014.
18 August 2015		2.1	D15/0324546	Corrected typing error D15/0324518

				Version 2.1 updated prior to version 2.0 becoming effective.
9 August 2022		3.0	D22/0034547	Major review of policy and supporting procedures

Department of
Education

CYBER SECURITY PROCEDURES

EFFECTIVE: 9 AUGUST 2022

VERSION: 3.0

CONTENTS

1 POLICY SUPPORTED

Cyber Security Policy

2 SCOPE

These procedures apply to all Department employees.

3 PROCEDURES

3.1 IDENTITY AND ACCESS MANAGEMENT

Site managers must:

- grant the minimum access required to information assets and systems for Department employees to perform a role or task;
- review and update access to information assets and systems when a network user's role or position within the Department changes;
- when projected cessation dates are known, set user access or permissions to cancel automatically;
- confirm that any users of Department ICT infrastructure are uniquely identifiable based on their user ID or other approved identifier;
- not create or use generic accounts within the Department's cyber network, except under strictly controlled conditions where there is no other solution to enable the business process to be actioned;
- approve remote access only for authorised work purposes; and
- endorse the use of the Department ICT infrastructure by non-employees and confirm supervision by a Department employee.

Employees must:

- take responsibility for actions undertaken under their assigned identity;
- only use remote access for authorised work purposes and advise the ICT Customer Service Centre when:
  - they no longer require their remote access e.g. change of position or circumstances;
  - they are planning on travelling overseas and intending to remote access from another country, otherwise unidentified remote access from overseas may be blocked; and
  - they have reason to believe that their account or account password has, or may, have been compromised.

Guidance

Generic accounts are approved at director level and are assessed and endorsed through the Department's Change Advisory Board (CAB). They are fully recorded, with the details readily accessible in the event of a real or suspected cyber security event.

Unidentified use of the Department ICT infrastructure is prohibited.

The ICT Customer Service Centre will assist in establishing multi-factor authentication (MFA) for employees traveling overseas, if required.

For further information, see Appendix A: Identity and Access Management

3.1.1 SERVICE ACCOUNTS

Site managers must:

- confirm the appropriate permissions are applied when service accounts are added into HRMIS or the Department's Access Management (DAM) tool (this is automatically applied with a previously established template);
- have variations to service accounts endorsed by the line manager of the service account and ICT Security Management team via the ICT Change Management process;
- assign responsibility for managing and maintaining a service account to a permanent staff member;
- confirm the password security management procedures in s3.2 are applied to service accounts; and
- advise ICT Customer Service Centre when:
  - they no longer require the service account; and
  - they suspect account information or account password has been compromised.

Employees must:

- only use service accounts for authorised work purposes; and
- not use service accounts for:
  - accessing or using email services (unless the account is linked to a mailbox);
  - accessing or using internet services (e.g. web browsing or downloading content from the internet); and
  - unauthorised access to information or information systems.

3.1.2 ADMINISTRATOR ACCOUNTS

Site managers must:

- have variations to administrator accounts endorsed by the line manager of the service account and ICT Security Management team via the ICT Change Management process; and
- confirm the password security management procedures in s3.2 are applied to administrator accounts.

Employees must:

- only use administrator accounts for authorised work purposes;
- not share their administrator account, and
- not use service accounts for:
  - accessing or using email services (unless the account is linked to a mailbox);
  - accessing or using internet services (e.g. web browsing or downloading content from the internet); and
  - unauthorised access to information or information systems.

Guidance

Administrator accounts are created and assigned specific high-level permissions that are entered into DAM. Usually highly technical contract staff, engaged by the Department, are assigned to these positions to carry out the functions of that particular account.

The owner of an administrator account is accountable for all actions performed by the account. The owner of the administrator account is identified and recorded in the Active Directory (AD) account properties.

Administrator accounts automatically expire and are disabled after one year. Administrator account holders are required to re-apply for administrator account access annually.

3.2 PASSWORD SECURITY MANAGEMENT

Employees must:

- not reveal or share their passwords and other personal authentication mechanisms with anyone;
- apply the password system standards in Appendix B;
- immediately inform the ICT Customer Service Centre when they suspect their:
  - password may have been compromised; and
  - account has been accessed by someone else.

Guidance
Employees are accountable for any activity occuring under their login ID and password.

4 DEFINITIONS

ADMINISTRATOR ACCOUNT

An administrator account is a user account with high-level privileges to make changes on a computer that will affect other users of the computer. Administrators can change security settings, install software and hardware, access all files on the computer, and make changes to other user accounts.

DAM

Department of Education Account manager (DAM) administrators use the DAM tool to give schools, business areas, employees and visitors access to online services in accordance with their employment position or agreed contract access requirements.

DEPARTMENT EMPLOYEE

A Department employee is any person paid by the Department to provide a service, be it full time or part time as a staff member or teacher, or as a contractor for a short time or long time.

DEPARTMENT ICT INFRASTRUCTURE

All physical, virtual and cloud-based infrastructure and software owned by the Department, including physical or logical connection to the network, including use of Corporate Information Systems.

GENERIC ACCOUNT

An account created which cannot be directly attributed to an identifiable, auditable user. For example, admin front desk, admin temp, temp technician and temp teacher.

NON-EMPLOYEE

A volunteer or a work-place experience person, or other non-paid individual using the Department ICT infrastructure, is not an employee. For the purposes of this policy, they are classified as non-employees.

SERVICE ACCOUNT

A service account is a user account that is created explicitly to provide a security context for services running on Windows Server operating systems. The security context determines the service's ability to access local and network resources. The Windows operating systems rely on services to run various features.

SITE MANAGER

Officers, including principals, site managers and line managers, who have executive responsibility for overall management and control of any Department workplace.

5 RELATED DOCUMENTS

Relevant legislation or authority

Copyright Act 1968
Criminal Code Act Compilation Act 1913 (WA)(CI)
Privacy Act 1988
Public Sector Commissioner's Circular 2010-05 – Computer Information and Internet Security
School Education Act 1999

Related Department policies

Staff Conduct and Discipline
Records Management
Risk and Business Continuity Management
Telecommunications Use
School Security

Other documents

Encryption of Removable Media (staff only)
Corruption Prevention and Detection
Records Management Manual for School and Campus Records (staff only)

6 CONTACT INFORMATION

Policy manager: Director, ICT Operations and Customer Service

Policy contact officer: Cyber Security Consultant

Other contact: Customer Service Centre (CSC)
T: (08) 9264 5555
7.30am – 5.00pm Monday to Friday (excluding public holidays)

7 REVIEW DATE

9 August 2025

8 HISTORY OF CHANGES

Effective date	Last update date	Policy version no	Ref no	Notes
18 August 2015		2.0	D15/0301204	Major review undertaken and split into policy and procedures. Endorsed by Corporate Executive 14 November 2014.
18 August 2015		2.1	D15/0325006	Updated inconsistencies in Appendix A D15/0324895. Version 2.1 updated prior to version 2.0 becoming effective.
9 August 2022		3.0	D22/0034543	Full review of policy and supporting procedures

APPENDIX A. IDENTITY AND ACCESS MANAGEMENT

Category	Minimum mandatory requirements	Additional target requirements
User identification	Users accessing shared mailboxes or other resources are uniquely identified and their actions logged electronically. These are maintained for reference in the event an investigation into an anomaly or breach of policy or security is required. There are exceptions to this rule. For example, some training rooms have shared identities/passwords. In these instances, the responsible officer, such as the trainer, is to manually record which user is logged into what device to ensure that shared accounts are closely monitored to prevent and detect misuse. Other exceptions are to be treated in a similar manner. Unidentified use of resources is strictly prohibited.	
Authentication	All Department systems have automated authentication systems. However, not all are capable of complicated authentication methodology. Where technically and economically possible, the preferred methods of system authentication, in priority order, are: • multi-factor authentication (MFA); • single-factor authentication (SFA); and • password authentication.	
Multi-factor authentication (MFA)	MFA is the preferred method of authentication. MFA is required to access Department information systems and resources from a location external to the Department. Where MFA is used, a six digit PIN may be used as the secondary factor. Examples of other secondary factors include: • telephone call-back; • SMS; • security tokens; and • authenticator mobile apps. Multifactor authentication is required for access to: • critical or privileged capabilities; and • identified sensitive information.	
Single-factor authentication (SFA)	Biometric authentication is the preferred method of single-factor authentication, followed by token based authentication. Password authentication may be used as a last resort, subject to compliance with the Password System Standards (see appendix B).	
Password authentication	Where systems rely upon password authentication as their single factor, they must be	

	configured to confirm user passwords adhere to the requirements defined in the Password System Standards (see appendix B) where technically possible. Exceptions to Password System Standards are addressed at Appendix B.	
Account locking	User accounts are locked after five unsuccessful login attempts. After that, the login screen should direct the user to contact the ICT Customer Service Centre.	Users may unlock their accounts using approved multi-factor authentication.
Suspending accounts	User accounts should be suspended: • immediately after the individual ceases work for the Department; • as directed by a responsible officer during extended periods of leave, or in case of suspension of duties; or • automatically after 90 days of inactivity.	
Protecting authentication verification information	General user: Authentication verification information cannot include passwords, passphrases, or other user credentials. Technical oversight: Authentication verification data should be stored as secure, salted cryptographically sound hashes of assigned user secret credentials and protected from unauthorised access.	
Logon banner	All systems should display a logon banner that requires the user to acknowledge and accept their security responsibilities before access to the system is granted. Logon banners should explicitly state the following conditions: • Access is restricted to authorised users only. • Acceptable usage and information security policies apply. • The user must agree to abide by the aforementioned conditions. • User activity must be monitored and audited. • Legal ramifications of violating the relevant policies. • There is no expectation of privacy when using the system (refer to Telecommunications Use Policy). • Authorised point of contact for questions on these conditions.	
Screen lock	All systems should be configured to lock the user screen and display a generic screen when locked, initiated by either: • manually locking by the user; or • after 10 minutes of inactivity. Users are required to re-authenticate to disengage the screen lock.	
Temporary access	Temporary access to information assets follow the Department's user identification requirements outlined above.	

APPENDIX B. PASSWORD SYSTEM STANDARDS

The following standards apply to all passwords used to access Department systems.

Exceptions include:

- All Department legacy systems which cannot technically comply with these standards (i.e. legacy applications are outdated or obsolete but are still being used until a suitable replacement is found). These are to be noted with the non-compliance details and mitigated as technology allows.
- All Department essential applications (non-legacy) which cannot technically comply with these standards. These are to be noted with the non-compliance details and mitigated as technology allows.
- New applications which do not or cannot comply with these standards must be approved through the Change Management process.

All exceptions must include mitigation controls to reduce the risk of exploitation by cyber criminals.

B.1. DEFAULT ACCOUNTS

Category	Standard (Where technically feasible)
Default accounts	Default accounts are to be disabled, renamed or have their passphrase changed.
Length	The minimum length for all passwords is 10 characters.
Composition	Systems should allow users to choose passwords that contain any characters, numbers, punctuation, or other keyboard symbols (e.g. spaces). Passwords: • must not start or end with a number; • cannot contain three or more consecutive identical characters; • must not contain the username, first or last name or any part of the business unit name; and • on the password blocklist cannot be used. Users should use a number of random words for their password. This is also known as a passphrase (see Table 1 for example passphrases), which tends to be easier to remember and harder to crack than passwords. Choosing a common phrase is likely to result in the password being revealed during password security audits, resulting in a forced password change.
Complexity	Systems should not enforce password complexity, however, if 10 characters is the default, then complexity must be applied.
Blocklists	A password blocklist must be maintained. This blocklist will contain common weak passwords and weak passwords obtained as part of the password security audit. The Department password blocklisting system must confirm that users cannot choose a password that is on the password blocklist. Where a system does not use the Department central authentication system and does not enforce password blocklisting, the password length requirement will be set to at least 12 characters.

Repetition	Passwords will not be identical to any of the user's previous 10 passwords.
Multi-factor authentication	MFA shall be required for remote access or administrative access.
Expiry	Passwords of 15 characters or more shall not expire periodically. However, users will change their passwords if compromised as revealed by password security audit, through threat intelligence, or some other security threat. Passwords with 10 or more, but less than 15 character shall expire after 90 days, or sooner if compromised as described above.

Table 1: Example Passphrases

A passphrase meeting the requirements of this standard may look like this: “This passphrase contains special characters, numbers and is 78 characters long”.
Passphrases do not need to be grammatically correct or be a proper sentence; for example: “Brunnea Lazuli Unhappy Estuary” Less complex than the first passphrase, but still stronger than the 12 character password below. Additionally, the user can associate it to memory as the acronym “BLUE”, as all items of the passphrase are somehow related to that word.
A 12 character complex password may look like this: “Hgc?Rfkzh94*”

B.2. SERVICE ACCOUNTS

Category	Standard (Where technically feasible)
Composition and length	Service account holders must choose a secure password that meets the following criteria: • The length of the password is a minimum of 20 characters. • The password contains a minimum of three random words. • The password must be changed when a user of the account has left the Department or no longer requires access to that account. Service account passwords must not be written down (unless they are secured in a safe or an approved encrypted USB storage device).

B.3. ADMINISTRATOR ACCOUNTS

Category	Standard (Where technically feasible)
Composition and length	Administrator account holders must choose a secure password that meets the following criteria: • The length of the password is a minimum of 20 characters. • The password contains a minimum of three random words. • The password is not the same as the administrator’s normal user account password. • The password is not the same as any password that the administrator has used on any external or internet system. Administrator account passwords must not be written down (unless they are secured in a safe or an approved encrypted USB storage device).