GOVERNMENT OF
WESTERN AUSTRALIA

Department of
Education

Cyber Security Procedures

Effective date: 9 August 2022

Version: 3.1

These procedures must be read in conjunction with the Cyber Security Policy.

Table of contents

These procedures must be read in conjunction with the Cyber Security Policy.

1. Policy supported

Cyber Security Policy

2. Scope

These procedures apply to all 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

Government of Western Australia's Cyber Security Policy

School Education Act 1999

Related Department policies

Staff Conduct and Discipline

Records Management

Risk and Business Continuity Management

Telecommunications Use

School Security for Public Schools

Other documents

Corruption Prevention and Detection

Encryption of Removable Media Guidelines (staff only)

Manage records at your school (staff only)

6. Contact information

Policy manager:

Director, ICT Operations and Customer Service

Policy contact officer:

Cyber Security Consultant

Other:

Customer Service Centre (CSC)

T: (08) 9264 5555

7.30am – 5.00pm Monday to Friday (excluding public holidays)

7. History of changes

Effective date	18 August 2015
Last update date **Procedure version no.**	2.0
Notes	Major review undertaken and split into policy and procedures. Endorsed by Corporate Executive 14 November 2014.

Effective date	18 August 2015
Last update date **Procedure version no.**	2.1
Notes	Updated inconsistencies in Appendix A D15/0324895. Version 2.1 updated prior to version 2.0 becoming effective.

Effective date	9 August 2022
Last update date **Procedure version no.**	3.0
Notes	The new Cyber Security Policy and Procedures, replaces the Information and Communication Technologies Security policy and procedures. Approved by the Director General on 14 July 2022 D22/0539066 Summary of changes to the Cyber Security Procedures on Ikon (staff only).

Effective date	9 August 2022
Last update date	17 November 2022
Procedure version no.	3.1
Notes	Minor change to update links D22/0841360

8. Appendices

Appendix A: Identity and Access Management (PDF file - 84.8kB)

Appendix B: Password System Standards (PDF file - 132.1kB)

9. More information

Supporting content

Policy
Cyber Security Policy

Procedure review date

9 August 2022

Procedure last updated

17 November 2022