Queensland Health

Access control Standard

Queensland Health Digital Standard

QH-IMP-484-4: 2021

1. Statement

This standard establishes the controls required to ensure the identification and remediation of risks to Queensland Health digital information assets.

2. Scope

This standard supports the Use of ICT services and devices policy and applies to all staff within Queensland Health. Staff. Staff is defined as employees, students, interns, volunteers, contractors, consultants, Board Members and managed service providers working for Queensland Health. Queensland Health consists of:

- the Department of Health, and
- Hospital and Health Services.

3. How to apply this standard

This standard uses a referencing terminology to specify the level of rigidity of each article. These have been broken down into two major groups:

- **Must** means that the statement is an absolute requirement of the policy.
- **Should** means that there may exist valid reasons in particular circumstances to not comply to a particular statement. The full implications must be understood and carefully weighed before choosing a different course.

4. Requirements

4.1. Access control

4.1.1. Access to Queensland Health networks should only be granted where there is legitimate and authorised requirement.

4.1.2. Access rights and privileges should be assigned based on job classification, role and/or function. Users must only be given access to systems necessary to perform their required role.

4.1.3. All access granted must be recorded to capture the privileges and rights for each access role and the business functions or teams that may be assigned to each role. Access control should be automated and centralised wherever possible to reduce administrative burden.

4.1.4. Access control procedures should be documented and maintained for each access control process.

4.2. Identification (ID) and authentication

4.2.1. Users must be assigned a unique, individual user ID to allow accountability.

4.2.2. Shared or non-standard accounts should be disabled or removed. Any exceptions must be requested and managed in accordance with the Non-Standard Account and Exemption Process.

4.2.3. Where supported, all systems must be configured to enrol identities and authenticate users against an approved federated identity management solution. Federated identity must be included as a requirement when developing applications or procuring applications, whether they be delivered on-premise or via cloud services.

4.2.4. Identity enrolment processes and procedures must be maintained that provide an adequate level of assurance.

4.2.5. When developing identity registration processes, Cyber Security Group (CSG) must be engaged in the risk assessment to verify that the proposed identification mechanism provides an adequate identity registration assurance level based on the security classification of the system, following the guidelines in the Queensland Government Authentication Framework (QGAF).

4.2.6. All systems must be configured to require authentication with an approved authentication method in addition to the username. Authentication mechanisms are:

- something the user knows – a memorised secret such as a password or passphrase
- something the user has – such as a hardware token, smartcard, network location or registered mobile device to which a software token can be sent
- something the user is – a biometric identifier such as a fingerprint, face or retina scan.

4.2.7. New systems must have CSG or other CSG authorised third party perform a risk assessment to verify that the proposed authentication mechanism provides an adequate identity authentication assurance level.

4.2.8. Users should be assigned a unique, temporary password that they must be forced to change on first use of a system. Users must be then allowed to select their own password that conforms to the requirements of this standard.

4.2.9. Temporary assigned passwords must not be easily guessable and must meet password requirement regardless of if randomly generated or manually provisioned.

4.2.10. Systems must be configured to render passwords unreadable when recorded, stored or transmitted, using strong cryptography, where technically possible.

4.2.11. The login process should not display the last username or any other information that could aid an unauthorised user.

4.2.12. Systems must be configured to hide or mask password when entered into password fields.

4.2.13. The login process must validate the user credentials only on completion of all input data. If an error condition arises the system should not indicate which part of the data is correct or incorrect.

4.2.14. A user acceptance notice should be displayed prior to manual logon. The notice should ensure the user is informed of their responsibilities and requirements when accessing the system and acknowledges their understanding and acceptance of the stated conditions of use.

4.2.15. User sessions should be configurable to time-out after a period of no more than 15 minutes of inactivity, and the re-activation of the session must require the user to re-authenticate.

4.3. Multi Factor authentication

4.3.1. Multi-factor authentication is required for all non-console administrative access to servers or network devices. Where devices have been segmented into a security zone, multi-factor authentication must be used to access a management server within the security zone, and single authentication is to be used from the management server to other devices within that zone.

4.3.2. Multi-factor authentication is required for all remote access accessed by employees or third parties.

4.3.3. Multi-factor authentication is required for any access to information classified as Protected. Multi-factor authentication should also be considered for access to applications of a lower classification, based on an authentication assurance assessment. The authentication assurance assessment must be facilitated by Cyber Security and be performed in accordance with the Queensland Government Authentication Framework (QGAF).

4.3.4. As with the primary authentication mechanism, the secondary authentication mechanisms should be assigned to an individual account, and access control systems must be configured to ensure that the authentication mechanism can only be used with the intended account.

4.3.5. Authentication mechanisms used for multi-factor authentication must be independent of one another such that access to one factor does not grant access to any other factor.

4.4. Supplier identities

4.4.1. Vendor accounts used for remote support or maintenance of systems should only be enabled during the time period needed and disabled when not in use.

4.4.2. The use of Vendor accounts is to be monitored as follows:

- Vendor remote access sessions must be monitored to ensure the vendor is performing actions as required and not abusing the use of their privileges.
- The activation of vendor accounts should to be audited and regularly reviewed to ensure that vendor accounts are not being used for unauthorised purposes.

4.5. Administrative/Privileged account control requirements

4.5.1. The use of administrative privileges must be strictly limited. Administrative privileges must only be granted where there is an identified, authorised need for these privileges to perform the role.

4.5.2. Administrator privileges are required:

- For users responsible for providing system administrator services on an ICT device or system such as system maintenance and user support within the scope of their employment.
- To perform software application operations by an ICT device or system.

4.5.3. Administrative privileges must be assigned to a separate user account. If assigned a privilege account, the non-privileged user account must be used for standard activities and the privileged account only used when required to perform tasks requiring administrative privileges. Privileged accounts should be given an identifiable prefix to indicate that they have administrative privileges.

4.5.4. Administrators must be issued with multiple accounts with differing sets of privileges depending on job function and responsibilities. Each account will require separate passwords.

4.5.5. Processes, such as automated tools, must be used to identify and inventory all administrative accounts. Access review procedures should be developed to ensure that any unapproved or unnecessary administrative access is immediately revoked.

4.5.6. Application and service accounts must be configured with the least level of privileges required to perform the task. Rather than granting administrative rights to an account, vendor guidelines should be reviewed to identify individual rights and privileges that can be granted instead of full administrative rights.

4.5.7. The issuing of administrative/privileged accounts must:

- be kept to a minimum be assigned to an identifiable individual
- be limited to and consistent with the user's job function and responsibilities
- use strong passphrases
- not have the ability to send and receive email or access the Internet
- be allocated as a separate account for the performance of administration tasks with the least amount of privileges to undertake those duties
- have an unique username and password for each account
- use two-factor authentication for both internal and remote access sessions
- be scheduled for review (at least quarterly) to ensure they are still required and align with current roles
- not be included in code or script
- be logged, monitored and recorded as per the requirements of the General Retention and Disposal Schedule for Administrative Records.

4.6. System and application access

4.6.1. Access controls must be configured on all system components, including applications, operating systems, virtualisation technology, databases, network devices, appliances, biomedical devices and other operational technology. When implementing a system component, it must never be assumed that the default access controls are adequate. All system components must be configured to limit and control access in accordance with the requirements of this standard.

4.6.2. The classification and risks to data must be taken into account when designing or managing systems.

4.6.3. The use of utility programs that might be capable of overriding system and application controls must be restricted to authorised users, and their use controlled. System administrators must ensure that appropriate permissions are maintained on all system utilities to restrict their use to privileged accounts.

4.6.4. All use of system utilities should be logged.

4.6.5. Unnecessary system utilities must be disabled or removed.

4.6.6. When designing, procuring or implementing applications, access controls, data integrity checks, version control mechanisms and other features should be used to adequately mitigate the risk of accidental or deliberate deletion or modification of data.

4.7. Access reviews

4.7.1. Application custodians are responsible for ensuring a standardised process is in place to authorise and monitor user access, and for ensuring guidelines are set around allowable system access (direct and interfaces).

4.7.2. Access reviews should be performed at least quarterly. The goal of the access review is to verify that provisioning and de-provisioning processes are working correctly.

4.7.3. Access review procedures are to be rigorous enough to:

- Ensure users who have left the organisation or changed role are identified and access is immediately revoked or amended.
- Ensure that granted access rights and privileges match those documented in an approved access request form.
- Ensure that the use of administrative privileges is strictly limited.

4.7.4. In addition to formal access reviews, automated tools should be used to identify and disable inactive accounts.

5. Legislation

- *Criminal Code Act 1899*
- *Cybercrime Act 2001 (Cth)*
- *Financial Accountability Act 2009*
- *Financial and performance management standard 2019*
- *Hospital and Health Boards Act 2011*
- *Information Privacy Act 2009*
- *Public Records Act 2002*
- *Right to Information Act 2009.*

6. Supporting documents

- Use of ICT services and devices policy
- Audit and recordkeeping standard
- Collaboration platforms standard
- External access standard
- Information access, use and disclosure standard
- Monitoring and reporting standard
- Training, awareness and disciplinary procedure standard
- Use of email standard

- Use of ICT services and devices standard
- Data and application custodianship policy
- Data and application custodianship standard
- Information security policy
- QGEA Information Security Classification Framework
- Queensland Government Authentication Framework

7. Definitions

Term	Definition
Digital information assets	A digital information asset is anything that exists in a binary format and comes with the right to use. Digital information assets include: digital documents, electronic mails, websites and other relevant digital data that are currently in circulation or are, or will be stored on digital appliances.

For more ICT definitions please refer to:

Digital policy glossary

Version Control

Version	Date	Comments
1.0	01/03/2021	New standard. Endorsed by Architecture and Standards Committee. Approved by Director-General.