Queensland Health

External access Standard

Queensland Health Digital Standard

QH-IMP-484-5: 2021

1. Statement

The external access (including web access) standard sets out the requirements for the use of external access services to access non-public facing Queensland Health Information and ICT resources from outside of the Queensland Health Network boundary.
External access incorporates access from any device, including corporate and personally owned devices, connecting to the Queensland Health network.

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. All external access will be authorised

4.1.1. The use of external access services must be approved by a manager with the required financial delegation.

4.1.2. The use of external access services should be for official use only.

4.1.3. Authorised users must not share credentials; any external access must be under the user's identity.

4.1.4. Non-Queensland Health staff and organisations requiring access to the Queensland Health network must sign the appropriate systems access agreement.

4.2. Approved external access services

4.2.1. All external access to the Queensland Health internal network should utilise the eHealth Queensland External Access Service.

4.2.2. Staff must not use non-approved external access services, such as TeamViewer, unless an exemption has been granted. Office 365 is supported for external access to corporate applications and services.

4.2.3. All non-standard external access to the Queensland Health network must be assessed by the eHealth Queensland Cyber Security Group, e.g. vendor dial home support.

4.3. Use of personal devices

4.3.1. Access to Queensland Health information from personally owned devices must be provisioned through the approved services.

4.3.2. Personally owned devices must be free of malware, viruses, trojans or any malicious software and be fully updated prior to connecting to the External Access Service.

4.3.3. Queensland Health information must not be stored on personally owned devices.

4.3.4. Personally owned devices used for Queensland Health external access must be protected from unauthorised access through the use of strong passwords, pass codes or biometrics.

4.4. Cloud services

4.4.1. All access to external services should be integrated with Queensland Health federated identity providers where possible, e.g. AzureAD.

4.4.2. Authentication methods should comply with the Queensland Government Authentication Framework.

4.5. Vendor external access

4.5.1. All vendors connections to the Queensland Health network must be via the Vendor VPN services and a named account should be issued to each individual within the vendor organisation.

4.5.2. External access to a Queensland Health system must be approved by the system owner/application custodian.

4.5.3. 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.

4.5.4. The use of vendor jump box technologies should be approved by the eHealth Queensland Cyber Security Group.

4.5.5. 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.

4.6. Monitoring

4.6.1. All external access must be monitored.

4.6.2. Management of users, including changes to access and removal must be removed on the day of notification or the day a user leaves Queensland Health or within seven days for a user that moves to another Queensland Health position.

5. Legislation

- *Anti-Discrimination Act 1991*
- *Crime and Corruption Act 2001*
- *Criminal Code Act 1899*
- *Criminal Justice Act 1988*
- *Cyber Crime Act 2001 (Cth)*
- *Electronic Transaction Act 2001*
- *Financial Accountability Act 2009*
- *Hospital and Health Boards Act 2011*
- *Human Rights Act 2019*
- *Information Privacy Act 2009*
- *Public Records Act 2002*
- *Public Sector Ethics Act 1994*
- *Public Service Act 2008*
- *Right to Information Act 2009*
- *Telecommunications (Interception and Access) Act 1979 (Cth)*
- *Workplace Health and Safety Regulation Act 2008*

6. Supporting documents

- Use of ICT services and devices policy
- Access control standard
- Audit and recordkeeping standard
- Collaboration platforms 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
- Information Security policy

7. Additional resources

External network access service

https://qheps.health.qld.gov.au/ea

External Vendor Access - Client - Overview of the Vendor or Partner Client account (Information)

https://qldhealth.service-now.com/nav_to.do?uri=%2Fkb_view.do%3Fsys_kb_id%3D2bfc1132db79409491e0456a3a961971%26sysparm_rank%3D9%26sysparm_tsqueryId%3Dbe92c57bdb5ed0d81a75a056059619cc

8. Definitions

For ICT definitions please refer to:

Digital policy glossary

Version Control

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