IT Services Policy/Policy Document

DG11 - System Access Controls - Policy

Prepared by: < >
Version: 2.0
**Description & Target Audience:**

<table>
<thead>
<tr>
<th>Effective Date</th>
<th>Next Review</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 2020</td>
<td>July 2023</td>
</tr>
</tbody>
</table>

**Reviewers:**
- Konrad Dziedzic, Cloud Solution Architect
- Terrence Holland, Servers & Storage Manager
- Martin Evans, Head of Data Centre Services
- Skender Osmani, Head of Client Devices
- Olu Solanke, Business Analyst
- Jason Bunning, Head of Application Delivery
- Ed Web, Head Application Solutions

**Policy Owner:**
- Name/Position: Rachel Bence – CIO IT Services

**Revision History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
<th>Author</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Review of Policy and Update of Template</td>
<td>Shelim Miah</td>
<td>18 Feb 2020</td>
</tr>
<tr>
<td>1.2</td>
<td>Review and feedback all sections</td>
<td>Shelim Miah</td>
<td>16/04/2020</td>
</tr>
<tr>
<td>1.3</td>
<td>Further feedback and updates</td>
<td>Shelim Miah</td>
<td>28/04/2020</td>
</tr>
<tr>
<td>2.0</td>
<td>Finalised document</td>
<td>Shelim Miah</td>
<td>08/06/2020</td>
</tr>
</tbody>
</table>

**Authorisation:**
- Name / Position: Rachel Bence CIO IT Services
- Signature: Rachel Bence
- Date: 10 July 2020
1. **Policy Statement**

1.1 This policy ensures that access to Queen Mary systems and system data are controlled and authorised personnel has access at the right level at the right time, and sufficient safeguards are in place to prevent unauthorised access.

1.2 The Policy aims to:

- Outline the expectations of those who have access to systems and system data.
- Ensure the security and protection of Queen Mary data.
- Sufficient controls are in place to ensure that only authorised individuals have access
- Controls are in place to safeguard against misuse
- Outline roles & responsibilities

2. **Scope**

2.1 This policy applies to those who manage and control access to Queen Mary systems and system data, including staff who have access to or wish to have access to these systems and system data.

3. **Policy Detail**

3.1. Where possible, Log-on screens shall display a general notice, warning that the system is to be accessed by authorised users only, the notice shall include a brief description of who authorised users are; (e.g. employees, contract staff, suppliers or students of Queen Mary).

3.2. Log-on screens shall display a general notice, warning that systems may be monitored and that unauthorised access or use may result in disciplinary proceedings and that evidence collected may be passed on to law enforcement agencies. Refer to Guidelines on the Right to Privacy and the Monitoring of Data

3.3. Where possible, log-on screens shall not display any system or application identifiers until the log-on process has been successfully completed. The screen must not provide help messages during the log-on procedure, particularly no warnings on the number of incorrect entries allowed.

3.4. Password characters are to be hidden during log-on and encrypted prior to being sent across the network.

3.5. The username/password credentials are used to authenticate the user. Once the user has completed entering their credential, the system must validate these credentials. If there is an error in the credentials provided, the system will prompt the user to re-enter without indicating which part of the credentials was entered incorrectly.

3.6. The system must automatically record unsuccessful logon attempts and limit the number of consecutive unsuccessful log-on attempts. After the limit has been reached, the system shall reject further attempts and access is disabled automatically for a pre-defined period.

3.7. Where possible, the system is to limit the time allowed for log-on attempts in order to avoid providing attackers with time to guess the correct details.
3.8. After a successful log-on, the system shall display, where possible, details of the date and time of the last successful log-on. This will enable an authorised user to check whether the previous log-on was performed by someone else and report an IT security incident if necessary.

3.9. Users’ access rights to systems shall be limited to those systems that they are authorised to use. Access rights shall initially be granted as part of the provisioning process, but may be extended or revoked as the user changes their role or ceases employment with Queen Mary.

3.10. Application security is to be controlled by an Application Administrator.

3.11. The Application Administrator shall use the application menus and application security to manage and restrict access to functions within applications where necessary.

3.12. Users’ access rights within systems must take account of the functions that they need to perform such as read, write, delete, and execute applying the ‘least privilege principle’ where possible.

3.13. Wherever possible, application systems that include audit trail capabilities must be enabled if the systems contain Confidential or Restricted data, as defined in SOP DG09 – Information Classification.

3.14. PCs, Laptops and workstations must have password-enabled screen savers configured so that the screen contents are no longer visible and the device secured against unauthorised access after a defined period of inactivity.

3.15. Systems that are accessed using thin-client or web-based interfaces must have session timeouts configured so that the session is automatically disconnected after a defined period of inactivity. The actual timeout periods will be agreed between the system owners and IT Services, or the department operating the system, according to the sensitivity of the data being accessed.

4. **Administrative Access**

4.1. System administrators with elevated privileges must be known and documented so that it is clear who is authorised to have access and system admin understand the responsibility placed on them.

4.2. All users with administrative access to IT systems must receive a secondary admin account with elevated privileges, separate from their general email enabled productivity account. Administrative access (elevated privileges) will only be granted to the user’s admin account and must only be accessed for performing functions that are required to fulfil their role.

4.3. Wherever possible Multi Factor Authentication (MFA) (token or key based) must be enforced for administrative access.

4.4. Admin account credentials should not be used directly on unmanaged/self-managed machines without MFA.

4.5. Wherever possible, administrative changes on windows managed machines should be done using Local Administrative Password Solutions passwords (LAPS) and not directly with an Admin account.

4.6. System Administrators must not make unauthorised changes to systems and must follow established procedures for installing, modifying, or removing system hardware or software and for deploying patches, updates, or upgrades.
4.7. System Administrators must not access a user’s files or email or files unless specifically requested by the user or otherwise requested by and authorised in writing or email by appropriate senior management and or the appropriate personnel.

4.8. System administrators with or without elevated privileges must not use hardware or software tools to circumvent or bypass security controls except under exceptional circumstances and the approval from senior management.

4.9. System administrators with or without elevated privileges will not access information that is outside of their role or share access or information with unauthorised users.

4.10. They are responsible for protecting the password and token and the confidentiality of the information accessible by that account.

4.11. Non-AD accounts e.g. local admin accounts, should only be used in circumstances where the admin account cannot be used (e.g. during setup or if active directory is unavailable)

4.12. Administrators must surrender their elevated privilege accounts, if they no longer have a business need or, change their roles.

4.13. The surrendered accounts must be disabled and any shared access revoked and passwords changed if necessary.

4.14. No admin with or without elevated privileges is allowed to remote into systems or system data containing Confidential, restricted or sensitive information.

5. Roles & Responsibility

5.1. The Risk and Governance Manager will be responsible for initiating the review cycle for the document owner to carry out the review. The document owner will assess and incorporate appropriate comments/feedback received.

5.2. Once the document has been updated, the Risk and Governance Manager will request approval from the appropriate approval body. All approved documents are to be stored in a central repository and uploaded to the web where applicable.

6. Monitoring

6.1. IT Services may request checks to be carried out as part of internal audits, any findings will reported to the IT Lead Team (ITLT) for any corrective actions to be issued.

6.2. Where non-compliance is identified and the corrective actions have not been implemented, ITS will take appropriate action, which may result in escalation to senior management.

7. Exceptions

7.1. Where an exception to this policy is required, the matter should firstly be referred to the ITLT to assess the exception.

7.2. The ITLT will then make a decision or refer this to the IT Strategy Board (ITSB) for a decision.

8. References

SOP DG09 – Information Classification
9. Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managed Device</td>
<td>A device that is centrally managed by IT Services, who has control over the policies that govern the device</td>
</tr>
<tr>
<td>Unmanaged/Self-managed</td>
<td>A device that is managed by the local school or dept. IT Services is unable to centrally control policies that govern the device.</td>
</tr>
<tr>
<td>MFA</td>
<td>Multi Factor Authentication is a security system that requires more than one method of authenticating credentials from the user to verify the user's identity for a login</td>
</tr>
<tr>
<td>Policy</td>
<td>A set of rules or framework that outlines the boundaries in which to operate.</td>
</tr>
<tr>
<td>Process</td>
<td>A structured set of Activities designed to accomplish a specific Objective. A Process takes one or more defined inputs and turns them into defined outputs</td>
</tr>
<tr>
<td>ITLT</td>
<td>IT Lead Team – Team of Senior Managers consisting of the Assistant Directors of IT, Faculty Relationship Managers and Chaired by the IT Director.</td>
</tr>
<tr>
<td>ITSB</td>
<td>IT Strategy Board – Team of Executive Managers consisting of Vice Principals and the IT Director, who oversee the delivery of the IT Strategy.</td>
</tr>
<tr>
<td>User</td>
<td>A member of staff, enrolled student, contractor, visitor, or another (any other) person authorised to access and use Queen Mary services.</td>
</tr>
<tr>
<td>Access Control</td>
<td>Users are assigned privileges to access, view, edit modify or delete files and folders. Users may be prevented from accessing files and folders by removing the privileges.</td>
</tr>
<tr>
<td>Thin-Client</td>
<td>Remote Access tool, to allow users to connect to the network and applications off campus</td>
</tr>
<tr>
<td>LAPS</td>
<td>Local Administrator Password Solution (LAPS) is a Microsoft product that manages the local administrator password and stores it in Active Directory (AD)</td>
</tr>
</tbody>
</table>