# A black background with red text  Description automatically generated

# Third-Party User & Access Management Policy

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Changes** | **Author** |
| 0.1 Draft | 21st October 2024 | New Policy | James Vincent (Cyber Security Manager) |
| 1.0 Approved | 18th December 2024 | Approved following review. | Greg McCloskey (Director of D&IS) |

### Purpose

This policy establishes requirements for managing user access to University IT systems, applications, and data. The aim is to ensure that access is granted, managed, and revoked efficiently, securely, and in alignment with security standards, including special considerations for privileged accounts.

### Scope

This policy applies to anyone requiring privileged access to university systems, including on-premises and cloud-based resources.

### Definitions

**Active Directory (AD):** Microsoft directory system for managing access to systems and resources.

**Entra ID**: A cloud-based directory and identity management service from Microsoft.

**Single Sign-On (SSO):** A session and user authentication service that allows users to log in with one set of credentials to multiple applications.

**Microsoft Identity Manager (MIM):** A Microsoft product that facilitates identity and access management across systems.

**iTrent/QSIS:** Internal systems used to manage staff and student data respectively.

**Privileged Account:** Accounts with elevated permissions that require additional security controls as detailed in the [Privileged Accounts Process.](https://qubstudentcloud.sharepoint.com/%3Ax%3A/r/sites/issmt/_layouts/15/Doc.aspx?sourcedoc=%7B19347771-6C6E-4198-93E4-F11D7EE30AB6%7D&file=IAM%20Privileged%20Accounts%20Process.xlsx&action=default&mobileredirect=true).

**JML Process:** The "Joiners, Movers, Leavers" process that manages access throughout the lifecycle of an individual's relationship with the university.

### Rationale

Proper user access management is crucial to protect sensitive data, maintain operational integrity, and comply with security standards. Through appropriate use of Active Directory, Entra, and automation tools like Microsoft Identity Manager (MIM), human error can be reduced to help ensure timely provisioning and deprovisioning of accounts, and secure access to critical resources.

## Policy Statements

### Access Control

Access should be managed via Active Directory or Entra ID groups.

Where possible, Single Sign-On (SSO) through Microsoft Entra ID should be used for authentication and authorisation.

### Privileged Account Management

All privileged accounts must adhere to the Privileged Accounts Process, which outlines access controls, monitoring, and auditing requirements. These accounts must undergo regular security reviews, and access should be limited to those with a justified business need. Accounts are regularly checked to ensure they are still required. The process also enforces strict onboarding and offboarding procedures to ensure that only authorised personnel can access sensitive systems and data.

### Provisioning and Deprovisioning

Microsoft Identity Manager (MIM) will automatically create staff and student accounts based on data from iTrent, QWork, Additional Person Database and Qsis. This includes assigning users to the appropriate groups for resource access.

Dynamic groups may be created using data synchronised from iTrent/QSIS. These groups may be used for access management primarily in Office 365/Entra ID but can also be used in on-premises applications. Some example uses include:

* SharePoint Online
* University line-of-business applications
* Departmental resources

User accounts will be automatically provisioned or deprovisioned based on changes in iTrent/QSIS data. Any issues with incorrect provisioning must be corrected by updating the source data. If the data is correct but access is wrong, a helpdesk ticket should be raised for the IAM team to analyse and resolve the issue.

Synchronisation occurs every two hours from 08:30 until 20:30 each day. For urgent access changes (e.g., immediate revocation), the IAM team must be contacted directly.

### Non-Automated Access Requests

For access not managed through iTrent/QSIS or MIM, users must follow specific request procedures:

|  |  |  |
| --- | --- | --- |
| **Access Type** | **Creation/onboarding** | **Removal/offboarding** |
| Privileged Account | Follow privileged account process (https://www.qub.ac.uk/directorates/InformationServices/Services/#6347493) | Account expiry date |
| Shared mailbox | Use shared mailbox access request form (<https://go.qub.ac.uk/sharedmbx>) | JML process, shared mailbox reminders |
| AD Guest account | Guest Account request process (https://go.qub.ac.uk/guestaccount) | Account expiry date |
| Entra Guest account | Invitation | Access reviews |
| Vendor account | Follow privileged account process | Account expiry date |
| New access group | Request via IT Service Desk | Access reviews |
| Other | Request via IT Service Desk | N/A |
| Service Accounts | Follow privileged account process | Account expiry date |

All types of accounts have defined onboarding and offboarding processes, with regular access reviews and account expiry where applicable.

### Monitoring and Review

The JML process integrates with key data sources to ensure accurate tracking and timely updates to access controls. These include:

* Telephone extensions
* Shared mailbox memberships
* Systems access
* Server ownership
* Privileged access
* QF22 IP records (implemented for some schools)
* Service accounts

Regular reviews are required to ensure ongoing compliance with the policy and security requirements.

### Enforcement

Violations of this policy may result in disciplinary action, under relevant P&C policies and procedures. Access violations may also lead to revoked privileges, including temporary suspension of accounts.

### Responsibilities

IAM Team: Responsible for handling urgent access issues, resolving provisioning errors, and overseeing access management processes.

Digital & Information Services: Ensures that provisioning, deprovisioning, and access request processes are automated and efficient where possible.

Managers and Supervisors: Responsible for initiating access requests and ensuring their teams follow appropriate access procedures.

### Review and Revision

This policy will be reviewed every two years or whenever significant changes occur in the access management systems or organisational structure.