Access Management Policy

Version 1.0

Document History and Reviews

Version	Date	Revision Author	Summary of Changes
0.1	May 2018	Ali Mitchell	New policy
0.2	May 2018	Ali Mitchell	Minor changes due to peer feedback
0.3	Feb 2020	Ali Mitchell	Merged User Management Policy details in this policy as similar
0.4	June	Ali Mitchell	Added in introduction section, moved some paragraphs around and update contents table. Changed word in 5.1 from should to must

Review Distribution

Name	Title
Ira Goel	IT Risk and Compliance Manager
Martyn Goldsborough	Information Security Manager
Mike Maling	Operations and Security Manager
Brenda Waterman	Information Governance Manager and Data Protection Officer
Simon Hallett	Security Architect

Approval

Versions	Position	Approved Date
1	Members of the ISG	1/7/2020

Contents

1. Introduction

1.1 Access management is an integral part of good information security practices and having a robust policy and processes in place help protect the University's IT network and data sets from potential cyber-attacks and reputational damage.

2. Purpose

1.1 The purpose of this policy is to ensure IT accounts are controlled and managed to minimise any security risks and covers the following aspects of governing IT accounts:

- Creating accounts
- Applying enhanced privileges
- Changes to permissions
- Service accounts
- Deletion of accounts

3. Scope

2.1 This policy applies to:

- All information systems managed by, or on behalf of, the University of Exeter, including (but not limited to) those hosted in the cloud; such as SharePoint and OneDrive for Business.
- All accounts used to log onto, or interface with such systems.
- All University IT members responsible for the management of user accounts and the privileges associated to them, specifically those designated as owners of information systems.

4. Access Control

4.1 Account creation, deletion and modification must be:

- Requested and recorded via change control process.
- Authorised and approved via change control process.
- Performed by appropriately trained individuals.

4.2 Account creation processes must ensure that individuals are only given access to specific systems where required; justification must be recorded as part of the change process.

4.3 Creation of user accounts will be driven by authorised feeder systems including but not restricted to HR and student registration.

4.4 The person enacting any change in a user account must be different from the one authorising/requesting the change.

4.5 Logs will be kept of all account creation/deletion/changes.

4.6 Account details will only be shared with the line manager / or person requesting the new account. Users receive a document from their line manager that the Student Information Desk (SID) has produced which contains their log in details which also clearly articulates that users much change their password.

4.7 All accounts must have a unique ID, and a password allowing accountability of actions conducted using the account.

4.8 A process must be present that adequately manages account changes for joiners, movers, and leavers.

4.9 Logging and monitoring activities are undertaken as routine risk prevention measures.

4.10 When access is no longer required, the account must be immediately disabled.

4.11 Inactive accounts must be removed where there is no requirement for the account to be retained.

5. Privileged account use

5.1 Accounts that are required for systems to interact, such as system accounts or service accounts, must be configured as specific service account types where possible, rather than user accounts that have interactive access or shell access.

5.2 Privileged and administration accounts must be requested and recorded via change control process.

5.3 Privileged and administration accounts must be authorised and approved via change control process.

5.4 Logging and monitoring activities must be enabled for all systems and accounts.

5.5 Privileged and administration accounts must only be used for the activities that require elevated privileges, and must not be used for day-to-day usage, such as internet browsing and general work.

5.6 Privileged and administration accounts should not be used for interactive login where possible, and instead be used via techniques such as run-as, sudo etc.

5.7 Privileged and administration accounts must be controlled using a formally documented procedure, which details appropriate usage for that particular account.

6. Managing Privileges

6.1 A user account should have the least privilege that is sufficient for the user to perform their role within the university. Access to information and information systems and services must be driven by business requirements.

6.2 Changes in the privilege of an account must be authorised by the user's line manager and the Information Asset Owner of the information system to which the account affects.

6.3 Escalations of privilege to administrator level (including local or domain) must be subject to change control, approval and time limits/recertification annually.

6.4 Users' privilege rights will be periodically reviewed and is the responsibility of the relevant Information Asset Owner.

6.5 Line managers and Information Asset Owners are responsible for ensuring that users' access rights are adjusted appropriately, and in a timely manner, whenever there is a change in business need, a user changes their role, or a user leaves the University. This can be achieved by logging a call with the SID.

6.6 Generally user accounts should be disabled immediately once the user leaves the university or after a period agreed with HR. However, there are some staff that are permitted to have access to their emails and folders once they have retired. As such, the user's line manager and Information Asset Owner will inform IT via the SID and confirm the level of access required before the user retires. Once the user has retired it is the Information Asset Owner's responsibility together with HR to manage the user's access and perform periodic reviews of ongoing accessibility to emails and folders. Note that the user's data will not be deleted until after a period agreed with Human Resources, Registry, IT Services management and service owners.

6.7 Users should be informed of their responsibility to inform information system owners of any change in their role which might affect their privileges. IT Services should be informed as part of the starters/leavers process.

7. Managing Elevated Privileges

7.1 With the exception to Linux-based systems; users whose work requires system administration access will be given a separate specialist account for this purpose, in addition to their standard user account. Users cannot request their own system admin accounts; the request for such accounts should come from the line manager (who raises a SID call) and be subject to approval by an Exeter IT authorised person.

7.2 Users of Linux-based systems do not have the ability to have a separate system admin account but it is managed by additional permissions that can only be applied by Exeter IT staff.

7.3 System administration accounts are created and managed in Active Directory which is shared between multiple systems and platforms. Such accounts will have multi factor authentication applied as standard.

7.4 System administration accounts must conform to the University's current Password Policy but can use the same password policy as other accounts. However, there may be some systems that have a separate password policy, as required by that system/service.

7.5 In all other ways, these system administration accounts should be managed and the user is responsible for them similarly to standard accounts. When a user logs into a system admin account for the first time they are mandated to change their password before being able to continue.

7.6 Line managers are responsible for taking action to remove user's admin account when they move roles. This should be achieved by logging a call with the SID.

7.7 System administration accounts will automatically be disabled when the users' standard account becomes expired.

8. Supporting Policies and Documentation

8.1 Staff are also asked to read this policy in conjunction with other related policies and guidance documents defined below:

- Password Policy
- Remote Access Policy
- Overarching Information Security Policy
- Regulations Relating to the Use of IT Facilities

9. Policy Review and Maintenance

9.1 This policy will be reviewed and updated, annually, or as needed, to ensure that the policy remains aligned with changes to relevant laws, contractually obligations and best practice.

10. Advice

10.1 If you need any more information please contact the IT Security and Compliance team at itsecurityandcompliance@exeter.ac.uk