User Management Policy

Version 1

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
1	May 2018	Ali Mitchell	

Review Distribution

Name	Title
Ian Tilsed	Assistant Director Strategy and Architecture
Richard Uren	Assistant Director Service Management
Mike Maling	Operations and Security Manager
Duncan Hepple	Lead Cloud Services Engineer
Matt Harvey	Senior Cloud and Services Engineer
Rhiannon Platt	Information Governance Manager and Data Protection Officer

Approval

Name	Position	Signature	Date
	Members of the IGSSG		May 2018

Contents

1. Introduction

1.1 This policy covers the following aspects of governing IT user accounts:

- Creating accounts
- Applying enhanced privileges
- Changes to users permissions and
- Deletion of accounts.

2. 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.

2.2 This policy applies to all user accounts used to log on to, or interface with such systems.

2.3 This policy applies to 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.

2.4 All University staff members that have line management responsibilities are requested to comply with paragraphs 4.4, 4.5 and 5.6 below.

3. Access Control

3.1 Manual creation, deletion and changes of user accounts and privileges must be carried out by trained and authorised staff.

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

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

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

3.5 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. Managing Privileges

4.1 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.

4.2. 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.

4.3. Users' privilege rights will be periodically reviewed.

4.4. 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.

4.5. 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.

4.6. 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.

5. Managing Elevated Privileges

5.1 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.

5.2 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.

5.3 System administration accounts are created and managed in Active Directory which is shared between multiple systems and platforms.

5.4 System administration accounts may use the same password policy as other accounts, but on some systems may have a separate password policy, as required by that system/service.

5.5 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.

5.6 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.

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

6. Policy Review and Maintenance

6.1 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.

7. Supporting Policies and Documentation

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

- Laptops Encryption Policy
- Encrypted USB and Hard drives recommendations
- Information Security Policy on Portable and Removable Media devices
- Password Security
- Information Security
- Anti-Malware Policy
- Viruses and Malware Guidance
- iPad and iPhone Security
- Privacy and Personal Data Protection Policy
- Records Management Policy

8. Advice

8.1 If you need any further advice, please contact the SID, dataprotection@exeter.ac.uk or refer to the Information governance and IT webpages.