Document Reference Number	**UoG/ILS/IS 007**
Title	Policy for Password Management and Multifactor Authentication
Owning Department	Information and Library Services
Version	9.2
Approved Date	12/12/2023
Approving Body	IT Management Board (IM)
Review Date	24/10/2024
Classification	Public – Non-sensitive

Policy for Password Management and Multifactor Authentication

1.0 Introduction

1.1 Passwords are broadly used to authenticate users to access IT resources, and to provide the frontline of defence against unauthorised access. Good password management will minimise the likelihood of user accounts being easily compromised and mitigate risks to university information and IT systems.

1.2 All activities carried out on university IT systems using a username and password can be traced to the respective owner, activities are logged and audit trails can be generated for analysis. Generic usernames and passwords make it arduous to trace an activity to an individual due to the use of the login details by multiple users. It is therefore important that passwords are not shared. Sharing of passwords may result in an individual being held responsible for someone else's actions.

2.0 Purpose

2.1 The purpose of this policy is to set out the requirements and guidelines for using and managing university passwords and the use of multi-factor authentication.

3.0 Scope

3.1 This policy applies to all individuals with university user accounts.

4.0 ISO 27001 Reference

4.1 This policy complies with the university's Information Security Strategy and draws upon the ISO 27002 Code of Practice.

5.0 Principles

5.1 All passwords must be treated as confidential information and should not be shared with anyone or made public in any form, verbal or written.

5.2 The same password must not be used for multiple university IT systems where users have the option to set local passwords for these systems.

5.3 Where a specific group of users requires access to a particular system, they must be provided with their unique login details to that system or use the university's same sign-on technology if practical.

5.4 Privileged account users such as IT systems administrators and support staff must have privileged user accounts and passwords different from their standard user accounts.

5.5 University IT systems must not store passwords in clear text or any reversible form, and passwords must not be transmitted in clear text over the network.

5.6 University login details must not be used for non-work systems or applications e.g. on social media websites, retail websites, personal email and non-work cloud services.

5.7 All accounts must have their default passwords changed at first login.

5.8 If a password is not changed within 3 weeks for staff and affiliates / 10 weeks for students, of creation or password expiry, the account will be blocked and the password will be invalidated.

5.9 For approved third-party systems that require the use of university email address or user ID as part of its authentication:

5.9.1 a password that is the same or similar to the standard university user account should not be used for third-party systems.

5.9.2 whilst this policy may not be enforced through technology, the policy still applies and should be enacted manually (eg the password change frequency and password complexity requirements)

5.10 Default passwords must be changed before deploying any IT system.

5.11 A password must be changed every 18 months (approximately 550 days) or immediately if an account has been compromised or is suspected to be compromised.

5.12 MFA must be configured (see 7.2) within 3 weeks for staff and affiliates / 10 weeks for students, of account creation, or the account will be restricted to prevent remote access to services (access will only be available on-premise).

5.13 Account inactivity for a period greater than 6 months, will result in the account being blocked.

5.14 To unblock or unrestrict an account, a request would need to be made to the IT Service Desk.

6.0 Acceptable Methods to Create and Manage University Passwords

6.1 A Password must be at least 14 characters long.

6.2 A password should be comprised of 3 random words and should not include common words such as password, qwerty, computer.

6.3 Use a different password for each application/system that you use.

6.4 Change the initial or default password given to you when you connect to the network or a system for the first time.

6.5 Do not share your password with any staff. If required, a user account should be requested for a substitute if necessary.

6.6 Avoid reusing passwords.

6.7 Passwords must never be made public e.g. written down, stuck to your workstation screen or stored digitally in cleartext.

6.8 Do not use the "Remember Password" feature in applications.

6.9 Do not use known information about yourself as a password hint (e.g., "my dog").

6.10 Any suspected or actual incident relating to a password compromise must be reported immediately to the IT Service Desk, and the password must be changed promptly.

6.11 Visit this link for more information on Managing University Passwords

7.0 Multi-factor Authentication

7.1 Most university IT systems use a standard method of authentication, Single Sign-On (SSO) to login. When accessing services remotely, SSO authentication requires the use of Multi-Factor Authentication (MFA) in addition to a username and password to provide extra security from non-university networks. Users **will not** be able to access these resources on a non-university network without setting up MFA first.

7.2 User Requirement:

7.2.1 Configure your MFA settings to either send a text message, make a telephone call or use the Microsoft Authenticator mobile app on your mobile device as an additional authentication factor.

7.2.2 It is the user's responsibility to keep their personal device secure and available to be able to access university resources remotely. Avoid registering multiple devices for MFA authentication and unregister any unused devices from receiving MFA authentication notifications.
Further information on the university's MFA is available here: UoG Multi-Factor Authentication

8.0 Policy Compliance

8.1 The university has an obligation to comply with relevant statutory, legal and contractual requirements. This policy is designed to ensure user passwords are managed properly to mitigate any risks to the confidentiality, integrity and availability of university information and information systems.

8.2 The necessary steps to verify compliance with this policy shall be undertaken. This includes, but is not limited to, business tool reports, internal and external audits and feedback to the policy owner.

8.3 Failure to adhere to this policy will be addressed under the university's disciplinary processes and relevant contractor and third-party contractual clauses relating to non-conformance with the information security policies.

9.0 Exception to Policy

9.1 Any exception to this policy must be approved by the Executive Director and Chief Information Officer or a nominee in advance.

10.0 Policy Review and Maintenance

10.1 This policy shall be reviewed annually and where necessary will be updated as part of the continual improvement process.

11.0 Related Policies

- Link to the Information Security Policies
- Link to the Information Compliance Policies