PASSWORD MANAGEMENT PROCEDURE

Introduction
This procedure has been created to ensure that staff and students are aware of the steps required to adequately protect university staff and students’ data and that all users of the University IT systems are aware of their responsibilities with regard to effective password management.

1. Scope of Procedure
This procedure applies to all University of the West of Scotland staff, students, guests, visitors, business partners and vendors who have access to the University’s IT systems and data.

2. Our Procedure
The Password management procedure is designed to ensure all users of the University IT systems have the tools and processes available to them in order to effectively protect their identity and data/systems belonging to UWS. All users of UWS systems must follow to the University Password Management Procedure. This procedure outlines the responsibilities of both system users and Information Services.

End User Responsibilities:
Anyone with access to UWS systems or data is required to:

1. Protect all data files from unauthorised access, disclosure, alteration and destruction;
2. Be responsible for the security, privacy and control of data within their control or view;
3. Change their password when prompted (the change cannot be to simply change a number within an existing password). The main University password for staff (used to access desktop PC, mail and Wi-Fi etc.) must be changed every 180 days although passwords can be changed more frequently than this at user discretion or if a breach is suspected. Students only require to change their password on their initial login, after this they may change it at their discretion, or if a breach is suspected;
4. Multi-Factor Authentication for UWS accounts must be used if available.
5. Create complex passwords that cannot be easily guessed or follow a pattern;
6. Follow best practice by ensuring passwords have a minimum of 8 characters contain both upper and lower case letters, and number or special character (e.g. %, {, £). Longer passwords are more secure.
7. Ensure passwords are never shared with any other person, for any reason;
8. Setup an alternative contact method in the event that you forget your password or get locked out of the system. To setup a security profile go to https://passwordmanager.uws.ac.uk/;
9. Change any temporary password given by IT/HUB the first time you log in;
10. When accessing UWS email accounts using a smartphone or tablet the device must be protected with a PIN, password or biometric;
11. Visitors from institutions using Eduroam can connect to UWS Wi-Fi using their home institution Eduroam login and password. A WiFi network is also provided for visitors who do not have an Eduroam login. The ‘Guest’ network will be available to select from the list of WiFi networks. Full details are available in our Guest WiFi User Guide.

12. Inform Information Services at the earliest opportunity of any known or suspected breaches to this procedure or if you suspect any account or passwords have been compromised.

Information Services Responsibilities

1. Enforce strong passwords and periodic password changes following best practice guidelines;
2. Ensure all password data is securely stored and is not accessible either internally or external to the University;
3. A user account that has system-level privileges granted through group memberships or systems such as Dynamic Local User must have a password that is unique from all other accounts held by that user;
4. Provide a unique initial password for each new user of the IT systems and communicate this password in a secure and confidential manner;
5. Implement processes to handle forgotten or compromised passwords;
6. When a system user requests a password change from the Information Services Helpdesk, IS have a responsibility to verify their identity. As such photo ID may be required or, if over the phone answers to security questions may be required. Ideally, passwords should be changed via self-service: https://passwordmanager.uws.ac.uk/;
7. Automatically suspend a user account after 5 invalid logon attempts;
8. Restrict a suspended account to only allow reactivation by manual action controlled by the system/security administrator.
9. Change admin system passwords on a quarterly basis.

Procedure Author – Information Security Manager

Procedure Owner – Director of Information Services

Parent Policy Statement – IT Policy Statement

Public Access or Staff Only Access – Public

Version – Version 2 – 22 February 2021

Changes and Reason for Changes – Change in department name and MFA advice added