IT Password Management Procedure

Version 4 – May 2025

Procedure Author – IT Security and Customer Support Manager

Procedure Owner – Vice Principal (Finance and Infrastructure)

Parent Policy Statement – Information Services Policy Statement

Public Access or Staff Only Access – Public

Version – Version 4 – May 2025

Changes and Reason for Changes - minor changes to text for clarity, minor changes to requirements.

IT 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 and personal 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 procedure is designed to ensure all users of the University IT systems have the tools and knowledge available to them, to effectively protect their identity and data/systems belonging to UWS. All users of UWS systems must follow 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 main University password for account holders (used to access desktop PC, mail and Wi-Fi etc.) must be changed in the event of a potential or actual compromise, although passwords can also be changed at user discretion. It is recommended that passwords are changed at least annually. If IT have concerns that an account has been compromised, they have the discretion to change the password without contacting the account user. Account users will subsequently be informed and all changes are documented.
4. Use Multi-Factor Authentication for UWS accounts which are active and mandatory;
5. Create complex passwords that cannot be easily guessed or follow a pattern;
6. Never use your UWS account password for any other personal or work related account you use.
7. Follow best practice by ensuring passwords have a minimum of 10 characters contain both upper and lower case letters, and number or special character (e.g. %, {, £). Longer passwords are more secure;
8. Ensure passwords are **never** shared with any other person, for any reason;
9. Passwords can be changed at any time via the Microsoft Authenticator App;
10. Change any temporary password given by IT/HUB the first time you log in;

11. Ensure any mobile device used to access UWS systems is protected with a PIN or biometric.
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 System Administrator 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 IT Helpdesk, IT have a responsibility to verify their identity. As such photo ID may be required or, if the request is over the phone answers to security questions may be required. Ideally, passwords should be changed via ctrl-alt-del or via the Microsoft Authenticator App.
7. Monitor user accounts for unusual login activity or ‘impossible travel’ login. Restrict a suspended account to only allow reactivation by manual action controlled by the system/security administrator.
8. Change admin system passwords on a quarterly basis.