IT Password Management Procedure

Version 3 – March 2023

Procedure Author – IT Security and Customer Support Manager

Procedure Owner – Director of Information Services

Parent Policy Statement – Information Services Policy Statement

Public Access or Staff Only Access – Public

Version – Version 3 – March 2023

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 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 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 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 initial login, after this they may change it at their discretion, or if a breach is suspected;
4. Use Multi-Factor Authentication for UWS accounts which is active and mandatory;
5. Create complex passwords that cannot be easily guessed or follow a pattern;
6. 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;
7. Ensure passwords are **never** shared with any other person, for any reason;
8. If you need to reset your password, do this using the Authenticator App on your phone.
9. Change any temporary password given by IT/HUB the first time you log in;
10. Ensure any mobile device used to access UWS systems is protected with a PIN or biometric (fingerprint\facial recognition).

11. Inform IT 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 IT Helpdesk, IT have a responsibility to verify their identity. As such photo ID may be requested or, if the request is over the phone answers to security questions may be required. In the first instance passwords should be reset using the authenticator app on your phone;
7. Automatically suspend a user account after 10 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.