FUW GROUP
PASSWORD POLICY

Policy Introduction

Passwords are used to protect the FUW Group's network and data from intrusion and theft. Therefore, it is essential that all employees understand that account details, passwords, and security credentials should be treated as strictly confidential at all times and should not be divulged to a third party or external entity, to protect the company's data.

1. General Policy Points

1.1. All systems and accounts belong to the FUW Group, therefore the Group reserves the right to access accounts if and when required by using the passwords assigned or by resetting unknown passwords.

1.2. It is strictly forbidden for all the Group's users, to disclose any passwords/credentials used to access the systems in use, to anybody, including colleagues, friends and family members.

1.3. In all those systems which require passwords created by users, long complex passwords must be used. For information about specific systems, please refer to the section on "Password Usage for Specific Systems", in this document.

1.4. Users must not reuse passwords, even if the system permits it.

2. Password Construction

2.1. Passwords must be long and complex in order to be considered a strong password. Strong passwords are between 10 and 18 characters long and have a combination of characters including lowercase and uppercase letters, numbers, spaces between words and symbols whenever allowed. Some systems have different requirements for the construction of complex passwords which needs to be followed.

2.2. Do not use DOB or any words that can be easily guessed when creating new passwords.

3. Passwords Storage

3.1. The password for access to Windows on company owned laptops can be written on a piece of paper as a reminder, stored safely away from the working area (never taped on IT working equipment, such as monitor, computer etc.). The password is assigned by the Group's Head of IT or the IT Technical Support company and cannot be changed by the user.

3.2. Users can store all passwords for access to all systems, in a Microsoft encrypted password protected file such as Word or Excel and save the file in Google Drive.

3.3. It is strictly forbidden to save passwords to browsers or to any password management system unless encrypted.

4. Password Usage for Specific Systems

4.1. **Google Workspace:** All credentials are provided by the Group's Head of IT and the IT Technical Support Provider. Passwords cannot be changed by users.

4.2. In the unlikely event that a password has been compromised, users must do as follows:

a. **If the attempt has been identified out of working hours:** Employees are allowed to change their password immediately but must communicate the new password the to the Head of IT and the IT Technical Support team, the next day.

b. **If the attempt has been identified during working hours:** Employees are allowed to change their password immediately but a further action is strictly required: the user in question must phone the IT Technical Support team to report the issue, ask to check through the available Google Workspace audits if any unauthorised user has accessed the account and allow them to replace the password from the company authorised list. The Head of IT must also be notified of the issue.

4.3. **Remote Desktop:** All credentials are provided by the IT Technical Support Provider.

4.4. **Zoho CRM:** Users can create their own long complex passwords. The system is protected by Multifactor Authentication.

4.5. **Acturis:** Users are allowed to create their own long complex passwords and are forced to be changed every month.

4.6. PIN numbers or any preferred form of biometric authentication like facial recognition and fingerprint scanning, including timed screen locks, must be set up on all work mobile devices and tablets, to stop unauthorised access when left unattended.

4.7. Company owned work Mobiles and Tablets are protected by a PIN assigned by the Head of IT, which must not be changed unless there is concern that the PIN has been seen. Only in that case the PIN can be changed and the change must be reported immediately to the Head of IT.

5. Use of 2-Step Verification/MFA

5.1 2SV has been enforced in Remote Desktop, Google Workspace and Zoho CRM which means that users who have not enrolled cannot access their accounts. The Acturis system is protected by VPN access through Remote Desktop which is also protected by 2 Step Verification.

5.2 All users who have not been provided with a work mobile device, must install the Google Authenticator's app, on their personal mobile phone, needed for the 2 Step Verification as required by the systems/services in use at the FUW Group.

5.3 Failure to be prompted by the 2 Step Verification as expected, must be reported immediately by email, to the Head of IT and the Technical Support helpdesk. A

phone call to the IT Technical Support helpdesk must follow immediately after. Restoring the 2 Step Verification process must be treated with a high priority.