PASSWORD POLICY

Name of regulation: Password Policy

Purpose of regulation: To provide a definition of backups to be taken to maintain the integrity of the Institute systems and data

Approval for this regulation given by: Board of Directors

Responsibility for its update: ICT Consultant

Regulation applies to: All Institute staff, students and other authorised users

Date of Approval: October 2016

Proposed Date of Review: October 2017

1. **Introduction / Rationale**
   This policy supports the ICT Regulations to ensure that passwords used to access computer resources are selected and updated in line with best proactive security standards.

   The Institute ICT Regulations state that ***Users must take all necessary steps to protect and maintain security of any equipment, software, data, storage area and/or passwords allocated for their use.*** This policy dictates the minimum that a user must do to conform to this requirement when selecting and updating a password.

   Password policies are used to mitigate possible attacks against the Institute ICT Infrastructure and data held upon it. Use of long, complex passwords helps to mitigate attacks that attempt to guess passwords, and regular password changes to mitigate long term exploitation of any disclosed or discovered passwords.

2. **Password selection**
   To protect Institute systems and data, users must select a password that is secure and difficult to guess.

   In accordance with security best practice the following rules are mandatory:
   - All passwords should have a minimum of **eight** characters,
   - Each password must contain a combination of at least three out of four character sets:
     - uppercase characters (A through Z)
     - lowercase characters (a through z)
     - numerial digits (0 through 9)
     - non-alphabetical characters (e.g. ! $ # % @ +)
   - Previous passwords used for an Institute system must not be re-used.

   In addition, while not actively enforced by the password creation process:
   - Accounts created for use on external online resources **must not** use the same password for Institute authentication.
   - Passwords must not be something that can be easily guessed (avoid using your name, children or a pet's name, car registration number, sports team, etc.)

See Appendix A for a complete list of enforced password settings.

3. Changing a password

Passwords must be changed at the earliest available opportunity by the user if there is suspicion that the password may be compromised or someone else may know it. Administrators may also change passwords immediately, or disable accounts if there is suspicion that the passwords have been compromised.

Passwords must be changed regularly to mitigate the long term exploitation of any disclosed or discovered passwords. It is recommended that those passwords are changed every 60 days. It is mandatory that Institute passwords are changed based on the category of user as follows:

- Student account passwords must be changed every 455 days
- Standard staff accounts must be changed every 365 days
- Staff with access to key systems must change their passwords every 90 days

See Appendix A for a complete list of enforced password settings.

4. Password use

Passwords are the mechanism used to protect the security of Institute systems and must be protected.

- Passwords must be kept secret
- Passwords must not be written in a form that others could identify
- Passwords must not be stored electronically in a non-encrypted format
- Passwords must never be shared with others
- Care should be taken to prevent anyone from watching you type your password

Appendix A – Enforced password settings and rationale
This policy relates to Institute accounts and is enforced by security settings within the authentication system. The settings and the rationale for determining them for each category of user is detailed in the table below.

STUDENTS

	Setting	Rationale
Minimum password length	8 characters	In line with recommended minimum password sizes, to reduce the risk of dictionary attacks
Minimum password age	0 days	To allow immediate changing of password following help desk reset
Maximum password age	455 days	To ensure passwords are changed each academic year, while avoiding potential impact on students at the start of each academic year
Password history	24 passwords	To prevent the same password from being re-used (Note this is the maximum possible value)
Password complexity	Enabled	To enforce stronger passwords (three of uppercase, lowercase, numbers, symbols)
Change password at first use	No	Disable to simplify logon process for distance learners and e-enrolment
Account lockout	30 minutes automatic Account Lockout after 30 bad passwords	To prevent dictionary attacks without impacting on students

STANDARD STAFF

	Setting	Rationale
Minimum password length	8 characters	In line with recommended minimum password sizes, to reduce the risk of dictionary attacks
Minimum password age	0 days	To allow immediate changing of password following help desk reset
Maximum password age	365 days	To ensure passwords are changed annually
Password history	24 passwords	To prevent the same password from being re-used (Note this is the maximum possible value)
Password complexity	Enabled	To enforce stronger passwords (three of uppercase, lowercase, numbers, symbols)
Change password at first use	No	To support wholly offsite users, including partner colleges and external examiners
Account lockout	30 minutes automatic Account Lockout after 10 bad passwords	To prevent dictionary attacks

STAFF WITH ACCESS TO KEY SYSTEMS

	Setting	Rationale
Minimum password length	8 characters	In line with recommended minimum password sizes, to reduce the risk of dictionary attacks
Minimum password age	1 days	As per audit recommendation
Maximum password age	90 days	As per audit recommendation
Password history	24 passwords	To prevent the same password from being re-used (Note this is the maximum possible value)
Password complexity	Enabled	To enforce stronger passwords (three of uppercase, lowercase, numbers, symbols)
Change password at first use	No	To support wholly offsite users, including partner colleges and external examiners
Account lockout	30 minutes automatic Account Lockout after 10 bad passwords	To prevent dictionary attacks