NUI Galway
OÉ Gaillimh

Policies and Procedures

Code: QA404

Title: Password Policy

Review Date: September 2020

Approval: University Management Team (UMT)

1. Purpose

The purpose of this policy is to establish standards for the creation and maintenance of strong passwords, the protection of those passwords, and the frequency of change of passwords for all users of the University network. Passwords are an important aspect of security. The policy ensures a more consistent measure of security for the University's network and applications.

2. Description

The policy applies to:

- All staff and students who have access to University IT systems.
- All contractors, vendors or others (3rd parties), who have access to University IT systems.
- All systems and production stages of development including production, test and development.

3. Definitions

"Must", or the terms **"required"** or **"shall",** refer to an absolute requirement of the policy.

"Must not" or **"shall not",** refer to statements which are an absolute prohibition of the policy.

"Should" or **"recommended"** refer to a statement that should be applied. In certain circumstances, there may be a valid reason to ignore a particular item. In this case the full implications must be understood and carefully weighed before choosing a different course.

"Should not" or **"not recommended"** mean the specified behaviour should not be performed. There may exist valid reasons in particular circumstances when the particular behaviour is acceptable, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.

4. Requirements

The following requirements apply:

1. All passwords must have the following minimum complexity requirements:

    a. Must be a minimum of 8 characters long

    b. Should contain characters from at least 3 of the following character sets

    - Lower case characters 'a' - 'z'
    - Upper case characters 'A' - 'Z'

- numbers '0' - '9'
- Special characters, e.g.!"£$%^&*()@

On systems which can support the above, the setting must be technically enforced.

c. Should not be the same as the username, based on the word “password”, or based on variants of your name or username, date of birth, children's names, department name, key/character sequence, or dictionary word.

2. This policy applies to all systems and stages of projects including development, test and production. Weak passwords must not be assigned to systems at any stage (including development, testing stages, or as a temporary measure).

3. User passwords should be changed at least every 120 days. On systems which can support this the setting should be technically enforced.

4. Users should not re-use their previous passwords when changing passwords, or cycle through similar passwords (i.e. change 1 character).

5. A lockout should occur after five consecutive incorrect password entry attempts; the account lockout period should be 30 minutes.

6. A screen lock of unattended devices connected to the University’s directory service should occur after no longer than 20 minutes of user inactivity; the relevant user credentials will be required to unlock the PC (Windows OS Lockout).

7. Users are responsible for the maintenance and protection of their own passwords, in line with University Regulations. Users must not share their NUI Galway accounts or access codes with anyone. This includes sharing account password.

8. Passwords must never be written down or stored in unencrypted electronic file format on any device.

9. When a password is created on behalf of any user (initial password or password reset), the requestor must be authenticated and identified as the owner of the account prior to the setup or reset taking place. A unique randomly generated password must be assigned in line with this Policy. Common or initial passwords must not be used (e.g. today01, Happy123, Password123, etc.).

10. All default, vendor supplied, or passwords shipped with a system must be changed (e.g. manufacturers supplied passwords/PINs, application generated passwords), as soon as the system/application/device is used within the environment.

11. Common passwords must not be used for multiple accounts with different levels of security or which may be used by different groups of users. Instead, unique passwords should be used for every account type.

12. Where administrative passwords or secrets are used to secure communications between devices, a complex password should be used in line with this password policy.

13. Passwords should not be distributed in clear text on public or external communication networks.

14. Passwords must not be saved in clear text, or in an easily recoverable format. All passwords stored electronically must be encrypted. For the recommended types of encryption please refer to the ISS department.

15. Administrators shall not be able to view user passwords using any means, but they should be able to reallocate new one-time passwords to users under certain conditions (e.g. a user forgets his/her password) using defined procedures.

16. Systems must ensure passwords never appear on the screen in clear text by default

17. Systems must ensure passwords are not transmitted in clear text during the user's authentication process.

18. Users with privileged access must use a separate account and password (where available) for carrying out tasks that require elevated permissions.

19. University Passwords must never be sent via email or inserted into questionnaires etc. ISS will never ask a user to send them their password in an email or to insert it in a questionnaire / form.

20. Any suspicion of a password breach/ compromised account must be reported to ISS immediately

5. Exceptions

1. Agresso and Core Back Office passwords are locally controlled within the applications directly. These system mandate password changes every 120 days.

6. Responsibilities

Name	**Responsibility**
ÌCT Security Committee Chair	Policy Owner
Director ISS	Revisions and updates to the policy
University Management Team	Approval of the Policy
All who use or have access to NUI Galway IT System	Responsible for implementation of the policy.
Internal and external audit policy	Monitoring and reporting compliance with the policy
ISS Service Desk	Tracking of calls related to Security Incidents

7. Related Documents /Attachments

Password Guidelines

QA406 Remote Access Policy

QA408 Logical Access Policy

QA411 End User Policy