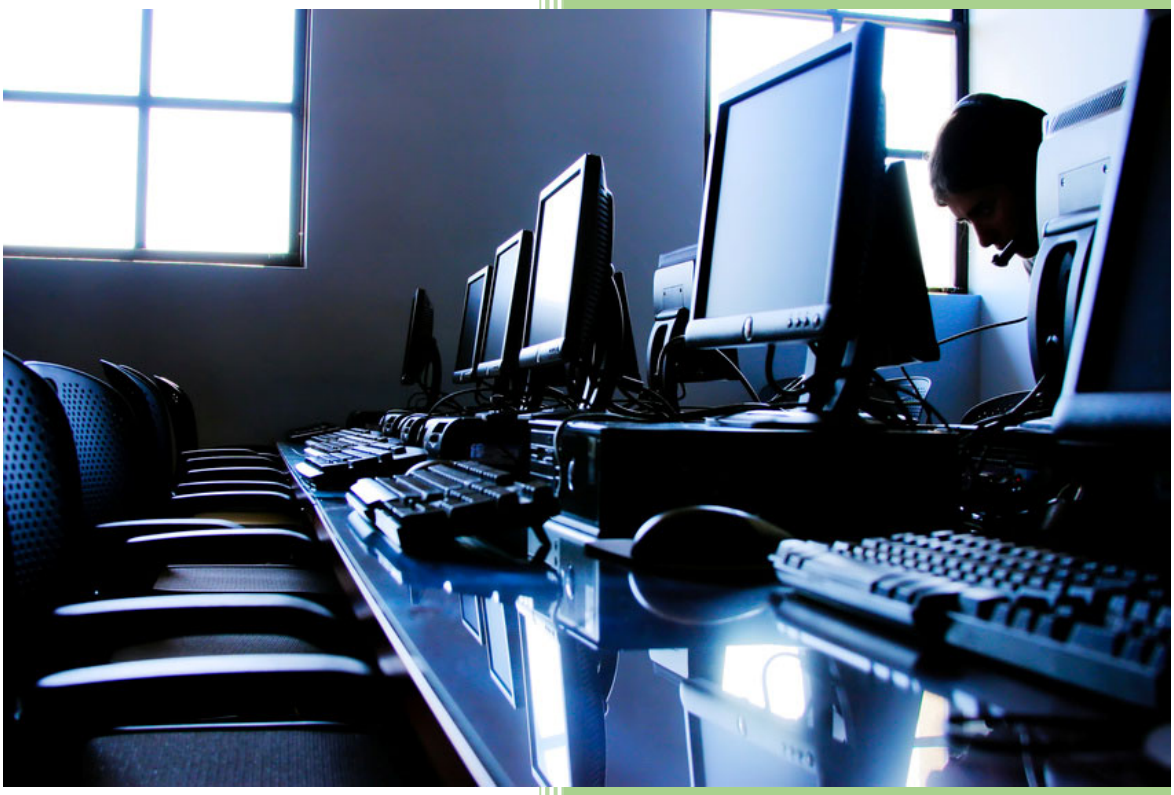
Password Standard

Document Reference and Version No	ICT Password Standard v3
Purpose	This Standard describes the Institute's requirements for acceptable password selection and maintenance.
Commencement Date	November 2020
Date of Next Review	November 2023
Who needs to know about this document	All Staff, Students and external parties using the Institute's ICT Resources
Revision History	Minor revision to version 2
Policy Author	ICT Manager
Policy Owner	ICT Manager
Approval by Sec/Fin Controller	November 2020

iadt
DUN LAOGHAIRE

Password Standard



Information Services Division
Dun Laoghaire Institute of Art Design and Technology

Contents

1.0 Overview

As described by the current ICT Acceptable/Appropriate Usage Policy, each IADT ICT Resource User is responsible for their use of technology on campus and accessing any IADT ICT Resource off campus such as cloud services e.g. Blackboard, Office 365, Agresso etc. The integrity and secrecy of an individual's password is a key element of that responsibility. The Password Standard is therefore inextricably linked with IADT's A/AUP as appropriate usage of ICT in IADT.

This Standard describes the Institute's requirements for acceptable password selection and maintenance. Its purpose is to reduce overall risk to the institution by helping ICT Resource Users reasonably avoid security and privacy risks that result from weak password choices and to encourage attention to password secrecy. The Password Standard reflects current best International Practice and recommendations from IADT's security auditors.

2.0 Scope

This Standard applies to all passwords used by systems that participate in IADT's enterprise authentication systems and is employed in conjunction with a Network ID to connect to IADT network-based services. It also applies to other IADT systems that aren't directly linked to IADT's enterprise authentication systems and these system must follow the password standard as closely as possible as each system will allow.

3.0 Password Composition

ICT Resource Users at IADT shall select passwords according to the following:

Password minimum length: A password must be no fewer than eight characters. The longer the password is, the harder it is to be cracked or guessed.

There may be technology constraints on some systems that may restrict/impose a maximum password length or other restrictions.

The use of "Pass Phrases" (memorable short sentences instead of single words) shall be supported where possible and practical.

A user must not use their previous fifteen passwords.

Information Services will provide an electronic password management service that will supply timely and detailed information on applicable password limitations.

A strong password is always a difficult one to pick as one has to also remember it.

Passwords should not be repeated on multiple systems that aren't linked to the IADT's enterprise authentication system.

Composition: Passwords should be composed so that they:

- Be at least 8 characters in length;
- Must not be the same as the last 15 passwords;
- Must contain different characters (no repeats);
- Look like a sequence of random letters and numbers;
- Be easy to remember but hard to guess;

- A varied set of characters, including lowercase and uppercase letters, numerals, and symbols (like spaces, dots, colons, quote marks, dollar signs) helps with making a password more secure;
- Be changed immediately if compromised.

Attempts to create or change a password to one that does not meet the above parameters may result in rejection of the change to the password.

Systems that aren't directly linked to IADT's enterprise authentication systems must follow the password standard as closely as possible as the system will allow.

Password must not:

- Include ICT Resource User's name, e-mail address or the word "password" or "12345678";
- Resemble the Network ID or the name of the account holder;
- Use any actual word or name in any language;
- Use numbers in place of similar letters e.g. Pa$$word;
- Use consecutive letters or numbers like "abcdefg","234567";
- Use adjacent keys on the keyboard like "qwerty";
- Include repeating sequences like "xyzxyz"
- Reuse the same password on multiple systems inside and outside the Institute.

Some examples of bad passwords are:

- mypasswo - Obviously plain-text based ("my password")
- nicole3 - Name-based
- lkjlkj - Repeating sequence
- S411y - Based on the word Sally with common letter/number substitution

4.0 Multifactor Authentication

Key and high security ICT Resource Users can expect a greater level of protection through the deployment of multi-factor authentication (MFA) where the system allows. IADT will implement multi-factor authentication (MFA) where the system allows. MFA must not be circumvented by ICT Resource User in anyway.

5.0 Password Expiration

An IADT ICT Resource User must change their password at least every 90 days. Attempts to log in using an expired password will not succeed. After changing a password, an ICT Resource User must wait at least one hour before changing their password again.

Expired passwords will be accepted as valid only when changing one's password, and only by the system(s) designated and supported by Information Services for this purpose.

Advance warnings of upcoming password expiration will be displayed at log-in (Windows users only) and via the Institute's webmail beginning 14 days prior to expiration, with repeated reminders thereafter until the expiration date.

An account holder may change their password at any time -- it is not necessary to wait for expiration.

In the event where the Institute is physically closed or unavailable to staff and students for significant periods of time the password expiry lasts maybe extended with agreement of the ICT Manager.

5.0 Reuse of Previous Passwords

Reuse of any of the account's fifteen previous passwords will not be permitted. Passwords must not be reused on multiple systems that aren't linked to the IADT's enterprise authentication system.

6.0 Further Information

If you have queries in relation to this password standard, please contact:

ICT Manager

Dun Laoghaire Institute of Art Design and Technology

Tel: 012394777

Email: ict_manager@iadt.ie