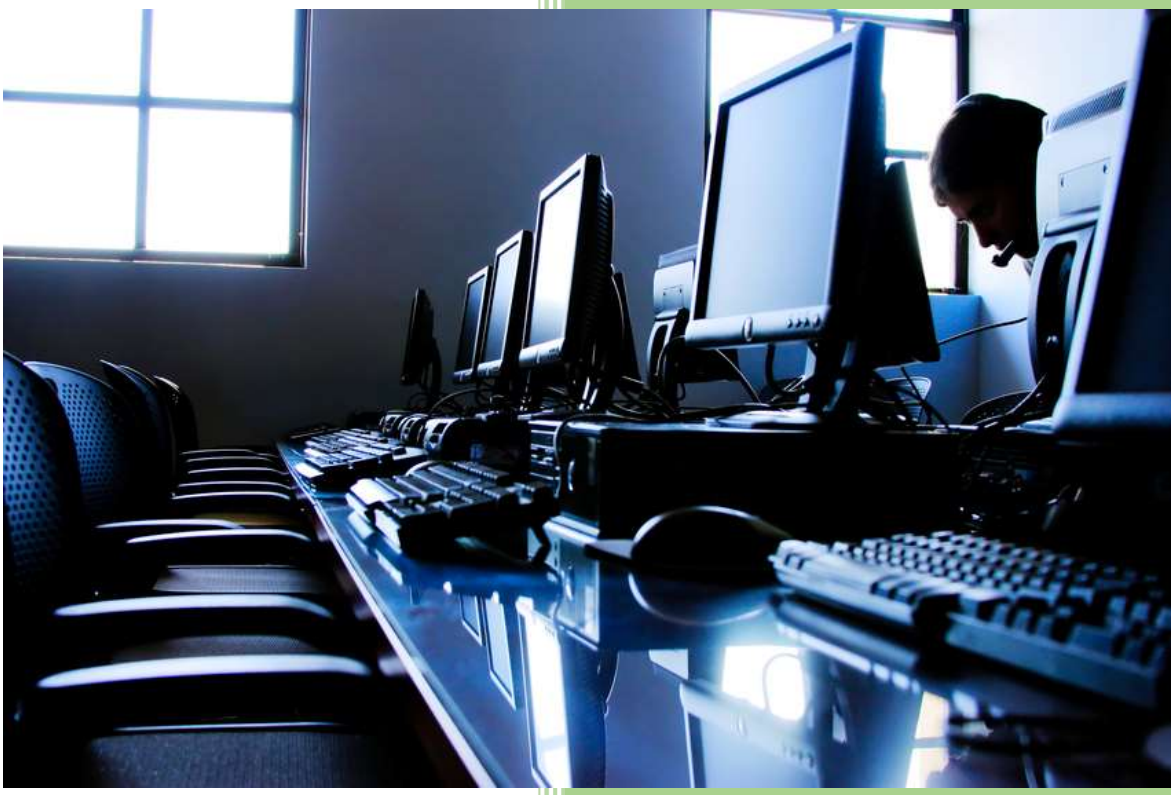
Password Standard

Document Reference and Version No	ICT Password Standard v2
Purpose	This Standard describes the Institute's requirements for acceptable password selection and maintenance.
Commencement Date	September 2017
Date of Next Review	August 2020
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 1
Policy Author	ICT Manager
Policy Owner	ICT Manager
Approval by Sec/Fin Controller	August 2017

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 his or her use of technology on campus. 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 computer 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 passwords used by systems that participate in IADT's enterprise authentication employed in conjunction with a Network ID to connect to IADT network-based services. One's Network ID password must never be used with systems or services that do not participate in IADT's enterprise authentication.

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. Though technology constraints may impose maximum length or other restrictions, use of "Pass Phrases" (memorable short sentences instead of single words) shall be supported where possible and practical.

A user cannot 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.

Composition: Passwords should be composed so that they:

Be at least 8 characters in length. The longer your password is, the harder it is to crack.
You cannot use your last 15 passwords.
Contain different characters (no repeats).
Look like a sequence of random letters and numbers.
Be easy to remember but hard to guess.
Use a varied set of characters, including lowercase and uppercase letters, numerals, and symbols (like spaces, dots, colons, quote marks, dollar signs).
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.

Password must not:

Include your name, e-mail address or the word "password".
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 like S411y ("Sally").
Use consecutive letters or numbers like "abcdefg","234567".
Use adjacent keys on the keyboard like "qwerty".
Include repeating sequences like "xyzxyz".

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 Password Expiration

An IADT ICT Resource user must change his or her password at least every 90 days. Attempts to log in using an expired password will not succeed. After changing a password, a computer user must wait at least one hour before changing his or her 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 his or her password at any time -- it is not necessary to wait for expiration.

5.0 Reuse of Previous Passwords

Reuse of any of the account's fifteen previous passwords will not be permitted.

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