# Ulster University Standard Cover Sheet

| | |
|---|---|
| Document Title | PASSWORD STANDARD 3.8 |
| Custodian | Deputy Director of Finance and Information Services (Information Services) |
| Approving Committee | ISD Committee |
| Policy approved date | 2018 – 02 – 06 |
| Policy effective from date | 2018 – 02 – 06 |
| Policy review date | 2018 – 02 – 07 |

| **Changes to previous version** |
|---|
| |

## INTRODUCTION AND BACKGROUND

A computer password is a secret string of characters (preferably not actual words) that is used along with a user name for authentication, to prove identity and provide access to networks, systems and services. Passwords should be protected and have characteristics that assure their effectiveness.

Further information on ISD policies, standards and guidelines is available at:

http://www.ulster.ac.uk/isd/policies

## RELEVANT LEGISLATION

The University will comply with all legislation and statutory requirements relevant to information and information systems, including:

- Computer Misuse Act 1990;
- Data Protection Act 1998;
- Communications Act 2003;
- Copyright, Designs and Patents Act 1988;
- Freedom of Information Act 2000;
- Human Rights Act 2000;
- Regulation of Investigatory Powers Act 2000;
- Police and Justice Act 2006;
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 ('the Lawful Business Regulations')

## STANDARD

### *Password protection standards*

1. Passwords shall be kept secret and not shared. Guidelines to ensure password secrecy include:

    a. Do not reveal a password over the phone to ANYONE;

    b. Do not reveal a password to a co-worker or line manager for any reason;

    c. Do not talk about a password in front of others;

    d. Do not hint at the format of a password (e.g., "my family name");

    e. Do not reveal a password on questionnaires or security forms;

f. Do not share a password with family members;

g. Do not write passwords down and store them where they can be found or accessed by others;

h. Passwords shall not be inserted into email messages or other forms of electronic communication.

2. Suspicion that a password has been compromised must be reported as soon as is possible to the Information Services Service Desk.

3. University Information Services shall adhere to the password characteristics defined below unless authorised to deviate by the Deputy Director of Finance and Information Services (Information Services).

4. All Administrator Account passwords shall be stored securely in a location independent of the production systems administrator; Procedures for access to same will exist and be available to management of the organisation unit which owns and operates the production system.

5. Information Services is authorized to take monitoring, investigative and other actions necessary to ensure compliance with this standard.

6. Information Services is authorized to require that passwords not complying with this standard are changed.

***Password characteristic standards***

1. A password must be at least eight characters long (10 characters for system accounts);

2. A password must contain at least three from:

a. Uppercase alphabetic (A – Z);

b. Lowercase alphabetic (a – z);

c. Digit (0 – 9);

d. Non-alphabetic, from (!, $, £, #, %, ~ etc.).

3. University Account passwords will not ordinarily require periodic change, but immediate change is required in the case of suspected or evidenced compromise.

4. Passwords shall not be re-used. Systems administration capabilities shall be used to enforce, and where possible to disable or limit, the re-use of old passwords;

5. Accounts are monitored for failed login attempts. Users will be informed of failed login attempts above a certain threshold. Continued or high-volume failed logins will result in accounts being locked.

### *Application Development Standards*

Application developers must ensure their programs do not transmit or store passwords in clear text or in any easily reversible form.

### *Guidelines for good practice*

Staff should be aware that use of features of client applications which allow storage of passwords on Personal Computers or other computing devices to achieve automated entry of credentials (Username and Password) and thus automated access to University Information Systems are an Information Assurance risk. Such features include, for example, the “Remember Password” feature of Web Browser clients such as Internet Explorer or Mozilla Firefox and of email clients.

It is advised that University staff be aware of the risks involved in using such application features. It is recommended that University staff should not use these features unless other additional security techniques are routinely applied e.g.

1) Physical security of client computer

2) Routine locking or automated locking of the Computing Device and/or User Account

## PURPOSE AND SCOPE

The purpose of this document is to define University standards for password management and passwords which are used for authentication to gain access to University networks, systems and services.

The scope of this standard includes all individual user accounts connecting to University networks, systems or services with the exception of system administration and database administration accounts covered within the scope of the Systems Administrators Code of Practice which introduces additional security measures.

## DEFINITIONS

“User Account” is used to refer to an established relationship between a user (individual) and a computer or information service. User Accounts are normally identified by a Username or account identifier which is unique to the computer or information service.

“System Account” is used to refer to an account that is not associated with an individual, but could be used by multiple users for specific functions, or used by automated systems. These can consist of:

- Application/Database Accounts
- Administrator Account

Ultimately, an individual or automated process can be identified with a specific individual use of the account through system logs.

“Application/Database Account” is used to refer to an application or database account used by an application to connect to another application, web service or database.

“Administrator Account” is used to refer to an account with sufficient privileges to enable necessary systems management, systems administration or engineering activities.

“Password” is used to refer to a secret word or string of characters that is used for authentication, to prove identity or gain access to a resource. With regard to Information Services, a password is normally used in conjunction with a Username or other account identifier which (in the case of User Accounts) uniquely identifies the person and/or role associated with user account.

“Authentication” is used to refer to the process of verifying the use of an account.

“University Information Service” is used to refer to any information system or service that resides on a University of Ulster owned or operated data communications network.

“Associates” is used to refer to all individuals who are not staff, students or visitors, and who are given a user account on one or more computer or information services.

“University Information Service” is used to refer to any network, information system or service that resides on a University of Ulster owned or operated data communications network.