University of Dundee
Password Best Practice

1.0 Overview
Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of University resources.
All users, including contractors and visitors, with access to University systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.0 Scope
The scope of this document includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any University of Dundee facility, has access to the University network, or stores any non-public University information.

Out of scope for this document:
Mobile phones or tablets that use pin locks and biometric authentication, are covered by the University mobile device policy.

3.0 Password Best Practice
- A standard is a mandatory requirement and cannot be deviated from in any way.
- A baseline is a minimum level of security that must be adhered to.
- All passwords may be audited for strength and complexity on a regular basis.
- Any employee found to have violated the password standards may be subject to disciplinary action.

4.1 Password Standard
Use of Passwords
- Passwords must not be shared with anyone. Anyone requesting a user’s password should be referred to this document and the incident reported to UoD-IT.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Never write down your password.
- Passwords should only be stored electronically, after being encrypted or hashed.
- Do not use your UoD password for any other accounts outside of your work. i.e Online banking, social media sites such as Facebook and twitter or personal email accounts such as Gmail and Sky Email.
- Change passwords immediately, if you suspect that your password may have been compromised and inform UoD-IT.

Password Age and History
- Passwords of all new accounts must be changed on first use.
- All default system passwords (e.g. SNMP strings) must be changed.
• New passwords must not be similar to previous passwords, e.g. passwords that increment (mypassword1, mypassword2, mypassword3 ...) are not strong.

Password Complexity
• Does not contain your user name, real name, or company name.
• Free of consecutive identical, all numeric or all alphabetic characters.

4.2 Password Baseline

Password Age and History
• Passwords must be changed at least once a year.
• Password history - should store at least the last eight passwords to reduce the user’s ability to recycle old passwords.

Password Complexity
• Minimum of 14 characters.

Online Password Cracking Mitigation
• Maximum of 15 unsuccessful attempts should trigger a 10 minute suspension before being allowed to authenticate again.