INFORMATION SECURITY:
PASSWORD AND CREDENTIAL STANDARD

1.0 PURPOSE

This document sets out Durham University's standards for secure password, passphrase and PIN management. To reduce the risk of weak or insecure use leading to an information security incident or system compromise, passwords, passphrases and PINs must be carefully created and used.

2.0 SCOPE

2.1 When this standard applies

This applies to all credentials including passwords, PINs and Passphrases (hereby known as credentials) and encryption keys.

2.2 Who needs to comply with this standard

Everyone using credentials that secure University information or University IT Facilities.

3.0 PASSWORD STANDARD

3.1 Protecting Credentials

- Credentials must be treated as Confidential University information and must not be disclosed to anyone, including CIS;
- A Password Manager should be used to generate and store credentials securely;
- If there is a requirement to store credentials electronically a CIS approved password manager must be used;
- If there is a requirement to write down credentials the written copy must be physically secured to the same standard as Confidential University information and remain confidential from others;
- Credentials must be changed or revoked whenever there is suspicion they may have been compromised, revealed to unauthorised parties or someone with knowledge of the credential leaves the organisation or changes positions;
- Credentials should not be saved in autocomplete in web browsers and other applications;
- Do not let others observe you entering credentials;
- Avoid use of unknown devices and be suspicious of unknown peripherals (USBs, chargers etc.) connected to devices you are using when entering credentials.

3.2 Password Composition

- Credentials must have a minimum length of 10 characters;
- Credentials should have a minimum of 16 characters (e.g. four random four letter words);
- Credentials must be hard for others to guess (e.g. not your name, a pet's name);
- A mix of random upper and lower case letters, numbers and special characters or long combinations of randomly chosen words should be used;
- Credentials must not be reused to form a new credential when changed. Reuse includes the use of the exact same credential or the use of the same root credential with appended or pre-pended sequential characters for another account or system.

3.3 PIN Composition

- Long complex passwords should be used in preference to PINs, however it is recognised that not all devices support passwords and instead only support use of PIN numbers;
- PIN length must comprise a minimum of 4 digits;
- PIN length should comprise a minimum 6 digits.

3.4 Privileged and System Credential Composition

In addition to the above, for accounts with privileged or system access:

- Credentials must comprise a minimum of 16 characters.

3.5 Encryption Key/Passphrase Composition

- Passphrase length must comprise a minimum of 16 characters.

Losing or forgetting the key/passphrase used to encrypt information will likely render the encrypted information completely unrecoverable or the device itself unusable.

- A secure copy of the encryption key therefore should be kept.

4.0 PASSWORD MANAGERS

Where a password manager is used:

- A master credential with a minimum of 16 or more characters must be used in addition to the other requirements of this standard;
- The software should timeout and lock after a short idle period, such as five minutes;
- The buffer should be cleared after the password is copied and pasted (many password managers do this automatically).

5.0 SHARING OF CREDENTIALS

Shared credentials are different to individually allocated personal credentials, such as your CIS username and password that are handled as Confidential information and known only to you:

- Where a specific business need requires an account or credential to be accessed by a pool of people the credential must only be shared with the pool members;
- When sharing credentials they must not be sent using the same method of transmission as the file, information or content that they protect;
- Credentials must not be sent using the same method of transmission as for sharing a related credential e.g. username;
- Both sender and recipient must delete temporary shared copies of the credential.

6.0 ENCRYPTION PASSPHRASE/KEY MANAGEMENT

- Keys used to encrypt other keys must be at least as strong and long as the keys they protect;
- Keys must be unique for each set of information encrypted;
- Key-encrypting keys must be stored separately from data-encrypting keys;
- Keys determined as secure for a period of time should be periodically changed when the end of that time period is reached;
- Where necessary set activation and deactivation dates for keys;
- For retired or replaced keys that need to be retained they must be securely archived (for example, by using a key-encryption key);
- Any keys retained after retiring or replacing are not to be used for encryption operations;
- Keys that are no longer used or needed must be revoked and/or destroyed.

Split key management may be required for some highly sensitive activities to enforce separation of duties and prevent one individual from acting alone. In such instances split keys/passwords should be used where each individual only knows half of the full key and both parties are required to participate during authentication without revealing their half to the other party.

7.0 SUSPECTED LOSS, MISUSE OR COMPROMISE

If you are suspicious that credentials or accounts have been lost, stolen, misused or compromised you must change or revoke it immediately and report this to the IT Service Desk.

7.1 Audit

The University shall perform periodic tests of credential strength to ensure that security is adequate. Where a test results in a fail you must comply with CIS requests to change the credential. These tests will monitor strength alone, not to reveal the actual credential itself to any party.

GLOSSARY

Term	Definition
Autocomplete	A software feature that attempts to replay previously text for example by automatically using a password without the user re-entering it.
Credential	Typically a username and password used to authenticate to an IT system to gain access to resources.
Encryption	Encryption uses a secret key (often derived with a passphrase) to change information into a scrambled value which unauthorised parties cannot access or convert back into a usable form without a secret key. Encryption does not necessarily protect the integrity (correctness) or authenticity (genuineness) of information rather it protects the confidentiality of the information.
Encryption key	A piece of information that determines the functional output of a cryptographic algorithm
Passphrase	A sequence of words or other text. A passphrase is similar to a password in usage, but is typically longer for added security.
Password Manager	Software for generating and retrieving complex passwords and storing them securely in an encrypted form. Typically unlocked using a complex passphrase.
PIN	A Personal Identification Number is a numeric or alpha-numeric password used for authenticating a user.
University Information	University Information includes but is not limited to: • Any data and information created by an employee in their work capacity. • Any research or course work that may contain data and information that are personal and/or commercially confidential to Durham University.
University IT Facilities	All IT Facilities provided by Durham University, whether owned or hired by the University, or provided by other organisations as a result of a contract or other arrangement with the University. This includes IT Facilities purchased through research grants or other funding obtained under the auspices of the University.
USB	An industry standard to define cables, connectors and protocols for connection, communication, and power supply between computers and peripheral devices.

DOCUMENT ADMINISTRATION

Version: 3.0
Classification: Public
Publication date: July 2020
Owner: Chief Information Officer
Review date: July 2021