1.0 PURPOSE
This document sets out Durham University’s standards for password security and password management. The Password Standard is a subsidiary document to the University’s Information Systems Security Policy which is approved by UEC.

Passwords are the primary form of user authentication used to grant access to University information and systems. To reduce the risk of weak or insecure password use leading to an information security incident or system compromise, passwords must be carefully created and used.

2.0 SCOPE & RESPONSIBILITIES
2.1 What this standard applies to

- Durham University user accounts
- IT administrator and system accounts
- All University IT facilities
- Local device passwords including your own devices such as laptops and smartphones

This standard applies to user accounts and IT facilities, including IT equipment with local user accounts that are used to store, transmit, or process University information, except where that information is PUBLIC Information. This includes non-University-owned equipment including private equipment.

Specifically it applies to:
- Staff and Student (CIS) user accounts, non-personal accounts and shared accounts;
- Service, system and systems administrator accounts;
- CIS, departmental and college IT facilities;
- IT equipment with local device passwords and PINS, including personal equipment;
- Desktops and mobile devices such as PDAs, smart phones, tablets, computers, laptops, portable storage;
- Mainframes, servers, network infrastructure and other equipment that provides computing capabilities;
- Encryption keys, including password protected encrypted memory sticks and storage;
- Cloud applications or storage services provided by third parties.

2.2 Who needs to comply with this standard

This standard applies to all staff and students, as well as others who use University IT facilities.
All individuals and organisations that connect to or use the IT Facilities provided or arranged by Durham University are responsible for ensuring that the passwords they use comply with the Password Standard.

2.3 Who holds specific responsibility

Information Owners are responsible for confirming that systems used to process or store information for which they are responsible comply with the Password Standard.

System Managers are responsible for implementing technical controls to enable user compliance.

IT Staff are responsible for deploying and advising and supporting users when applying technological measures in order to comply with the Password Standard.

3.0 PASSWORD STANDARD

3.1 Protecting your password

- Do keep passwords confidential: don’t share them with others
- Don’t use the same password for multiple accounts/systems

Passwords must be used and stored in a secure manner, as such:

- Passwords must not to be written down and stored or communicated insecurely;
- If there is a requirement to store passwords electronically a CIS approved method using strong encryption, such as password management software, must be used;
- Passwords must be treated as confidential information and must not be disclosed to anyone, including CIS. Where a specific business need requires an account to be accessed by a pool of people the password must only be shared with the pool members;
- You must change passwords whenever there is suspicion they may have been compromised;
- You must log off or lock the screen before leaving a computer or device unattended;
- Passwords should be unique to Durham University systems;
- You should never use the same password for more than one account;
- Passwords should not be saved in autocomplete in web browsers and other applications;
- Do not respond to phishing email requests for usernames and passwords;
- Be cautious of others observing you entering passwords or PINs;
- Be suspicious of unknown devices such as key loggers connected to devices you are using.

3.2 User Password Composition

- Do ensure your password is at least 10 characters long, has a mix of random letters, numbers and special characters and is not easy to guess
- Longer passwords are generally stronger than shorter complex passwords
- Do change shared account passwords promptly if someone leaves or changes role
- Do ensure any device used to process or store University information (e.g. your email) is protected with a password [or PIN code], that complies with the length and complexity requirements even if this is your personal property

Password length must have a minimum of 10 characters. Its content must not be easily guessable by others (e.g. your name, a pet's name, your house name). You should use a mix of random letters, numbers and special characters or long combinations of words and special characters
Password complexity passwords must use of a mixture of upper and lower case letters, numbers, and special characters (at least one number, letter and special character is required).

Password reuse is not permitted within 8 password refreshes. Reuse includes the use of the exact same password or the use of the same root password with appended or prepended sequential characters.

Password change requires passwords to be changed no less than every 90 days.

Shared Account passwords must be changed promptly whenever an employee or other individual with access to these passwords changes role or leaves the University.

Account lockout shall occur after 5 failed password attempts within 10 minutes, resulting in a block to the account for a period of 15 minutes. Should a user require access within this 15 minute period, they will be required to contact the IT Service Desk to unlock their account for central University IT facilities.

System timeout shall occur after a device has been inactive for 20 minutes and shall require the user to re-enter their password in order to regain access to the system. Users shall, however, routinely lock equipment before moving out of its sight in accordance with the Workspace Standard.

3.3 User PIN Composition

- Do ensure any device used to process or store University information (e.g. your email) is protected with a password [or PIN code], even if this is your personal property

A long complex password can greatly reduce the risks associated with unauthorised access to systems and information and so should always be preferred over using a PIN number, 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 and should comprise a minimum of 6 where possible. It must not by easily guessable by others for example by using simple patterns 1234, 4321

3.4 Privileged and System Password Composition

The standard for accounts with privileged or system access is the same as for user accounts apart from:

Password length must comprise a minimum of 16 characters.

Vendor Default passwords must always be changed, including operating system, software, application, system accounts and community strings.

3.5 Encryption Key Composition

Encryption keys should be treated as privileged or system passwords except that:

Key change may be less frequent and expiry should be set by the Information Owner in consultation with the Information Systems Security Manager.

Refer to the Encryption Standard for further guidance regarding encryption key management.
4.0 PASSWORD MANAGEMENT

4.1 Password Storage and Transmission

- Physical copies of passwords must be kept in secure storage, for example a locked safe.
- Electronic copies must be strongly encrypted, for example being kept in an approved electronic password safe.

Storage and management of passwords must meet business continuity requirements. In some circumstances it will be necessary for a password to be stored or shared, for example as part of business continuity arrangements or as an adjustment agreed by Occupational Health. Where this is necessary physical or technical security measures appropriate for confidential information must be put in place:

- Passwords must not be sent using the same method of transmission used for the information they protect, or for any related credential e.g. username;
- Any physical copies must be kept in secure storage, for example a locked safe;
- Any electronic copies must be strongly encrypted, for example being kept in CIS approved password management software.

Where password management software is used:

- A strong complex master password of 16 or more characters must be used;
- Password management software must use strong encryption;
- You should set the software’s timeout feature to lock after a short idle period, such as five minutes;
- You should clear the buffer after the password is copied and pasted (many password management software programs do this automatically).

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.

4.2 Issuing passwords

**Newly created passwords** set on a user’s behalf shall be set to pre-expire, and the user shall be required to change their password to one of their own choosing when they first successfully logon.

4.3 Reset/Forgotten Passwords

**Reset/Forgotten** passwords shall be reset to a temporary password rather than recovering the old password and the user shall be required to change their password to one of their own choosing when they next successfully authenticate.

Forgotten CIS passwords may be reset by the CIS self-service password reset website [https://www.dur.ac.uk/cis/passwords/change/](https://www.dur.ac.uk/cis/passwords/change/) or the IT Service Desk.

The IT Service Desk will verify your identity before resetting or re-enabling your account.

4.4 Suspected Password Loss or Misuse

If you’re are suspicious that your user account password has been lost, stolen or misused or a device that is logged on with or stores your password is lost or stolen you must report this to the IT Service Desk.
5.0 COMPLIANCE

5.1 Exceptions
Exceptions may be granted for systems and accounts where there is a justifiable reason for non-compliance. Exceptions must be sought from, and granted by, the Information Systems Security Manager (ISSM).

For cases where the minimum standard outlined in this document cannot be met due to technical limitations an “equivalent strength” alternative may be used, noting password length rather than complexity generally results in passwords that are more difficult to break or guess.

A log of all exceptions will be maintained by the ISSM and shall be reviewed annually.

5.2 Password Audit
The University shall perform periodic tests of password strength to ensure that password security is adequate. Where passwords fail a test, users shall be required to change their passwords immediately. These tests will monitor strength alone and will not reveal the password itself to any party.

All breaches of the standard shall be reported to the ISSM for investigation via the IT Service Desk.

5.3 Review and Update
This standard shall be reviewed and updated annually to ensure that it remains appropriate in light of any relevant changes to the law, organisational policies or contractual obligations.

5.4 Non-Compliance
Staff and students are reminded that breaches of this standard may lead to accounts being suspended or disciplinary action. Serious breaches of this standard, including causing damage to the reputation of the University, may constitute gross misconduct and lead to dismissal or being required to withdraw.
## GLOSSARY

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Auto complete</strong></td>
<td>A software feature that attempts to replay previously text for example by automatically using a password without the user re-entering it.</td>
</tr>
<tr>
<td><strong>Cloud Application</strong></td>
<td>A cloud application is a software application program hosted on the internet.</td>
</tr>
<tr>
<td><strong>Information Owner</strong></td>
<td>A senior member of staff that has overall responsibility for the information.</td>
</tr>
<tr>
<td><strong>IT administrator account</strong></td>
<td>An account with elevated privileges than can make changes to other user accounts</td>
</tr>
<tr>
<td><strong>ISSM</strong></td>
<td>Information System Security Manager. This role is described in the Information Systems Security policy.</td>
</tr>
<tr>
<td><strong>IT facilities</strong></td>
<td>&quot;IT Facilities&quot; include but are not limited to:</td>
</tr>
<tr>
<td></td>
<td>- IT hardware that Durham University provides, such as PCs, laptops, tablets, smart phones, printers and peripherals;</td>
</tr>
<tr>
<td></td>
<td>- Software that the institution provides, such as operating systems, office application software, web browsers etc. It also includes software that the institution has arranged for you to have access to, for example, special deals for students on commercial application packages;</td>
</tr>
<tr>
<td></td>
<td>- Data that Durham University provides, or arranges access to. This might include online journals, data sets or citation databases;</td>
</tr>
<tr>
<td></td>
<td>- Access to the network provided or arranged by the institution. This would cover, for example, network connections in colleges, on-campus wireless, connectivity to the internet from University PCs;</td>
</tr>
<tr>
<td></td>
<td>- Online services arranged by the institution, such as Office 365, JSTOR, or any of the Jisc online resources;</td>
</tr>
<tr>
<td></td>
<td>- IT credentials such as your Durham University username and password, campus card or any other token for authentication issued by the University to identify yourself when using IT facilities.</td>
</tr>
<tr>
<td><strong>Key logger</strong></td>
<td>Malicious software that captures keyboard strokes allowing a 3rd party to unauthorised access to information (passwords etc)</td>
</tr>
<tr>
<td><strong>Mainframe</strong></td>
<td>A bulk data processing computer system used by large organisations often running proprietary software.</td>
</tr>
<tr>
<td><strong>Non-personal accounts</strong></td>
<td>Non-personal accounts include accounts for software application maintenance (packages) and for various miscellaneous accounts such as departmental web services.</td>
</tr>
<tr>
<td><strong>Non-University-owned equipment</strong></td>
<td>Any device that is not owned by the University, or purchased under research grant or other funding obtained under the auspices of the University, which can be used to store, transmit or process information. Such equipment may include, but is not limited to, PDAs, Smart Phones, Tablets, Computers, Laptops, Memory Sticks, External Hard Drives and portable media devices.</td>
</tr>
<tr>
<td><strong>Password management software</strong></td>
<td>A software application used to store, organise and manage passwords.</td>
</tr>
<tr>
<td><strong>Phishing</strong></td>
<td>An illegal attempt to acquire sensitive information by masquerading as a trusted entity using electronic communication software (email etc).</td>
</tr>
<tr>
<td><strong>PIN</strong></td>
<td>A Personal Identification Number, a numeric password shared between a user and a system used as part of the authentication process.</td>
</tr>
<tr>
<td><strong>Privileged accounts</strong></td>
<td>These accounts are used for direct administration of the University’s IT systems. Access to them is limited to a small number of people.</td>
</tr>
<tr>
<td><strong>PUBLIC Information</strong></td>
<td>Information that the University actively places in the public domain. See the Information Security Classification Standard for further information.</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Shared account</strong></td>
<td>An account owned by an individual but used by multiple others to perform business function (shared email etc.). All users may know the account password.</td>
</tr>
<tr>
<td><strong>Strong encryption</strong></td>
<td>A cryptographic system that is considered by the security community to be highly resistant to being broken and uses well proven mathematically sound algorithms and key lengths.</td>
</tr>
<tr>
<td><strong>System account</strong></td>
<td>An account local to a machine that may have extensive privileges on the local machine.</td>
</tr>
</tbody>
</table>
| **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. |
| **User accounts**      | These accounts are provided to all users of the University's IT facilities. |

**DOCUMENT ADMINISTRATION**

**Current Status**

<table>
<thead>
<tr>
<th><strong>Version:</strong></th>
<th>2.0</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Approval date:</strong></td>
<td>9 February 2016</td>
</tr>
<tr>
<td><strong>Approved by:</strong></td>
<td>Chief Information Security Officer</td>
</tr>
<tr>
<td><strong>Owner:</strong></td>
<td>Information Systems Security Manager</td>
</tr>
<tr>
<td><strong>Review date:</strong></td>
<td>February 2017</td>
</tr>
</tbody>
</table>

**Related Documents**
- Encryption Standard
- Workspace Standard

**Revision history**

<table>
<thead>
<tr>
<th><strong>Version</strong></th>
<th><strong>Changes</strong></th>
</tr>
</thead>
</table>
| 2.0         | - Adjustments to ensure clarity, and consistency in terminology, roles and responsibilities and approach across the set of Information Security standards.  
- Additional section 3.5 on Encryption Key Composition  
- Additional sentence in 4.1: Storage and management of passwords must meet business continuity requirements.  
- Change to 4.1: Replaced 'Passwords should not be sent via email or instant message' with 'Passwords must not be sent using the same method of transmission used for the information they protect, or for any related credential e.g. username.' |