Password Protocol

This Password Protocol applies to all employees (and workers, as applicable) and students of The University of Northampton including any wholly owned subsidiaries. As part of our GDPR compliance, we are required to ensure we have appropriate safeguards. Despite technological advances in user authentication the first line of defence still in most cases involves password.

The protocol ensures a consistent and secure approach for the use of passwords for user authentication prior to access to the University of Northampton's systems and data. In addition, to protect the University employees from being locked out of their user accounts and allowing the recovery of forgotten or compromised password.

1 DEFINITIONS

Users
All parties who have been granted access to the University's IT Resources. This includes students, all workers and employees of the University including those within wholly owned subsidiaries, contractors, agency workers, consultants, suppliers, customers and business partners.

Single Sign On
Single sign on (SSO) is an authentication process which allows users to provide their username and password once to a trusted service and to have their identity securely and consistently provided to multiple applications, without having to log in more than once per session.

GDPR
A regulation in EU law on data protection and privacy for all individuals within the EU.

Authentication
A process that ensures and confirms a user's identity.

2 KEY PRINCIPLES

To ensure passwords are not easily guessable or breakable by brute force, the following minimum rules need apply:

All systems shall use strong passwords. Passwords should be made up of at least 8 characters or more and is a combination of 3 of the following components:

- At least one lowercase alpha character
- At least one uppercase alpha character
- At least one numeric
- At least one symbol

The following are practises that weaken the strength of passwords and must be avoided:

- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
- Names of family, pets, friends, co-workers, fantasy characters, etc.
- Computer terms and names, commands, sites, companies, hardware, software.
- The words "University of Northampton", or any derivation.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns (such as qwerty or 12345).
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

- Passwords for administrator accounts and Finance department accounts shall be changed every 90 days and for general users every 180 days.

- Passwords cannot be reused from a password history of 6 previous passwords.

- Passwords cannot be changed more than once per day. If this is required, it shall be made through the support desk.

- Initial passwords shall be first-time use only and force a password change.

- If a computer has been left idle for 15 minutes, they will be required to re-authenticate their details to reactivate the computer.

- Do not use the same password for University of Northampton accounts as for other non-University of Northampton accounts (e.g., personal account, forum logons etc.). Where possible, don't use the same password for various University of Northampton access needs, unless single sign on is available. For example, select one password for your internal email account and a separate password for IT systems that are not included in single sign on.

- Keep your passwords secret from EVERYONE. IT Services can reset passwords if necessary.

- Passwords for any documentation should not be communicated in the same email communication as an attached document. Passwords should be communicated via an alternative method of communication, such as text message, instant messaging or at the very least, a separate, delay email communication.

- User accounts that have system-level privileges must have a unique password from all other accounts held by that user.

- If a password is entered incorrectly, the user will be locked out of their account after 5 unsuccessful login attempts.

3 PROCEDURES

3.1 Users using UoN IT supplied devices can reset their password by:
Select [Ctrl]+[Alt] +[Del] and select 'Change password'.

If users use their own device, users are required to go to:

http://www.northampton.ac.uk/user and log in using your username and current password.
Once logged in, click 'Change Password' on the left-hand side. It will now ask you to enter your old password, and the new password you wish to create.

3.2 If users suspect an account or password has been compromised, they should report the incident to IT Services via the IT Services Portal or calling x3333 and change all passwords immediately.

4 EQUALITY IMPACT ASSESSMENT

An Equality Impact Assessment must accompany this document.

5 VERSION CONTROL

Version Control		**Approval record**	
Author:	IT Services	Approval:	ITSG Approval
Date written:	June 2018	Updates:	
Current status:	Live		
Record of Amendments			
Date	Details of Change		Approval