March 2018

Information Technology

James King

Password Policy

1. Overview

Passwords are an important aspect of Information Security. A poorly chosen password may result in unauthorised access and/or exploitation of City, University of London (hereafter "City") resources. All users, including contractors and vendors with access to City's systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2. Purpose

This document describes the acceptable standards for password creation and management.

3. Scope

This policy applies to all persons who have any form of computer account requiring a password on the organisations network as well as any internal or external services and applications.

Systems and services accounts which require elevated privileges are not in scope of this document and are covered by a separate password policy relating to that particular system or service.

The scope excludes Alumni (email for life) accounts at this time.

4. Policy

4.1 All passwords must conform to the Password Construction Guidelines in Appendix A.

4.2 You must not use the same password for City accounts as for other non-City systems (e.g. personal email account, online banking etc.).

4.3. Your passwords must be changed once a year.

4.4 Failure to change the password within 30 days of expiry will result in the account being disabled.

4.5 Passwords must not be reused.

4.6 Passwords may not be shared with anyone.

4.7 Do not leave passwords unsecured anywhere.

4.8 Never use the "Remember Password" feature of applications.

4.9 All passwords should be treated as sensitive and confidential information.

4.10 Any user suspecting that his/her password may have been compromised must report the incident to the IT Service Desk.

5. Consequences

Failure to observe this policy or related polices, codes and procedures will be considered a serious matter by City and may result in formal disciplinary action, which could result in a formal warning or dismissal. All such cases will be fully investigated according to the University's Disciplinary Procedure. In the case of a criminal offence City will involve the appropriate authority.

Any exceptions to this policy must be approved in advance and in writing, by the Information Security Manager.

Appendix A:

Password Construction Guidelines

Acceptable Methods to Create a Strong Password

1. Use a minimum of 8 characters. These should not be based on dictionary words/ common names.
2. Choose a password that no one will easily guess or hack.

Tips for Creating a Strong Password

1. Avoid words, numbers, or known or public information associated with you (e.g. names, family names, birthdays, phone numbers; etc.).
2. Avoid using your login name or any variation of your login name as your password.
3. Substitution should not be used on common words or with common substitution (e.g. 3=E, 4=A, 1=l, o=0, etc.).
4. When changing a password, change to an entirely new password. Do not just rotate through a list of favourite passwords.