1. Introduction
   1.1. This document gives additional details about implementing the "Passwords" policy outlined in Use of Computers Policy (ISP-S9).

2. Password based access control
   2.1. This document specifies the main password policy parameters to use for University computer accounts. The intention is that sufficiently strong password based access control is enforced.

   2.2. There may be circumstances where a password system cannot be configured to enforce the minimum requirements outlined here. In such cases:
   - Use of other configurations, that may enforce password security weaker than recommended here, must be considered and approved by management.
   - As far as possible the minimum requirements should be implemented, even where they cannot be enforced by computer configuration settings.

   2.3. There are different policy parameters for computer accounts depending on how they are used. They differ between
   - Regular user accounts, which are issued to an individual user so they can access University systems or services.
   - Service accounts, which are used by systems, applications or devices that need to interact with other systems or applications. Service accounts are never issued to or used directly by users. Service accounts are also not subject to regular password expiry requirements (as doing so would cause disruption to the services that use them.)

3. Password length and complexity
   3.1. The minimum password length and complexity requirements, as specified below, must be used in combination to help ensure that passwords chosen by computer users are very difficult to guess.

   3.2. For regular user accounts, passwords should be at least 8 characters long.

   3.3. For service accounts, with the absence of password expiry and the fact that passwords do not need to be entered regularly, the length requirement is
greater. Passwords for these types of account should be a minimum of 14 characters long.

3.4. In both cases, password complexity rules must be set that require passwords to contain at least one character from 3 of the 4 character sets i.e. uppercase, lowercase, numerical digits and non-alphanumeric characters.

4. Account lockout parameters

4.1. An account lockout is intended to impede password guessing attacks by automatically locking an account after a number of failed authentication attempts. The maximum number of failed login attempts permitted before lockout is known as the “lockout threshold”. The account lockout may be temporary for a period known as the “lockout duration”. The time window during which multiple failures leading to lockout must occur is called the “observation window”.

4.2. For accounts to which account lockout can and should apply, it is recommended that the lockout threshold should be set to 10 and the lockout duration set to 30 minutes. The observation window setting should be 30 minutes. (It is safe to reduce the lockout duration to 5 minutes if inconveniently long lockouts are clearly being caused by failures of legitimate automated login processes. Lockouts may result from automated login processes having not being reconfigured following an account password change.)

5. Password history and maximum and minimum password age settings

5.1. “Password history” can be set to prevent users from repeatedly using the same passwords they used in the past. The “maximum password age” limits the time for which a given password is valid. Expiring use of a password after a certain time helps to reduce the chance that a cracked password is still in use. It also helps avoid the possibility that an intruder would be able to continue accessing a compromised account indefinitely. “Minimum password age” can be used with password history to prevent a user from repeatedly changing a password until they are able to reuse their original password.

5.2. Using password age based expiry of passwords and the password history mechanism is recommended. (It is, however, recognised that automatic expiry of passwords may not be practical for services with large numbers of users because it may increase the workload of the support staff that need to perform password resets.)

5.3. Password aging should not be enabled for accounts which are authenticated against by automatic processes (such as Microsoft Windows scheduled tasks).

5.4. It is recommended that, for accounts where it is applicable, password history should be set to 24, minimum password age set to 1 day and maximum password age set to 90 days. (Practicalities of account management for some services may, however, require users to be able to reset temporary
passwords within a day, in which case a minimum password age setting of 0 days is acceptable.)

**Failure to comply with University Policy may lead to disciplinary action.**

---

**Document history:**

30 July 2009 (C. Nelson) Began first draft.

6 August 2009 (C. Nelson) Automatic password expiry is recommended, however, not compulsory on the basis that in some situations user support costs may exceed the security benefits.

24 September 2009 (C. Nelson) A 15+ character password requirement to protect against weak LAN Manager (LM) hashes was dropped on the basis that LM should be set to disabled by domain policy and is disabled by default in Windows Server 2008 and Vista. Also use 8+ password characters instead of 7+ for good measure.

8 January 2009 (C. Nelson) The minimum password age may need to be 0 days if account management procedures require users to immediately reset temporary passwords.

01 March 2010 (C. Nelson) Approved by the InfoSec Policy Steering Group.

10 May 2018 (C. Tilbury) Updated to reflect the requirement for stronger passwords for service user accounts than regular user accounts.

---

The official version of this document will be maintained on-line. Before referring to any printed copies please ensure that they are up-to-date.