APPENDIX B. PASSWORD SYSTEM STANDARDS

The following standards apply to all passwords used to access Department systems.

Exceptions include:

- All Department legacy systems which cannot technically comply with these standards (i.e. legacy applications are outdated or obsolete but are still being used until a suitable replacement is found). These are to be noted with the non-compliance details and mitigated as technology allows.

- All Department essential applications (non-legacy) which cannot technically comply with these standards. These are to be noted with the non-compliance details and mitigated as technology allows.

- New applications which do not or cannot comply with these standards must be approved through the Change Management process.

All exceptions must include mitigation controls to reduce the risk of exploitation by cyber criminals.

A.1. DEFAULT ACCOUNTS

Category	Standard (Where technically feasible)
Default accounts	Default accounts are to be disabled, renamed or have their passphrase changed.
Length	The minimum length for all passwords is 10 characters.
Composition	Systems should allow users to choose passwords that contain any characters, numbers, punctuation, or other keyboard symbols (e.g. spaces). Passwords: • must not start or end with a number; • cannot contain three or more consecutive identical characters; • must not contain the username, first or last name or any part of the business unit name; and • on the password blocklist cannot be used. Users should use a number of random words for their password. This is also known as a passphrase (see Table 1 for example passphrases), which tends to be easier to remember and harder to crack than passwords. Choosing a common phrase is likely to result in the password being revealed during password security audits, resulting in a forced password change.
Complexity	Systems should not enforce password complexity, however, if 10 characters is the default, then complexity must be applied.
Blocklists	A password blocklist must be maintained. This blocklist will contain common weak passwords and weak passwords obtained as part of the password security audit. The Department password blocklisting system must confirm that users cannot choose a password that is on the password blocklist. Where a system does not use the Department central authentication system and does not enforce password blocklisting, the password length requirement will be set to at least 12 characters.

Repetition	Passwords will not be identical to any of the user's previous 10 passwords.
Multi-factor authentication	MFA shall be required for remote access or administrative access.
Expiry	Passwords of 15 characters or more shall not expire periodically. However, users will change their passwords if compromised as revealed by password security audit, through threat intelligence, or some other security threat. Passwords with 10 or more, but less than 15 character shall expire after 90 days, or sooner if compromised as described above.

Table 1: Example Passphrases

A passphrase meeting the requirements of this standard may look like this: "This passphrase contains special characters, numbers and is 78 characters long".
Passphrases do not need to be grammatically correct or be a proper sentence; for example: "Brunnea Lazuli Unhappy Estuary" Less complex than the first passphrase, but still stronger than the 12 character password below. Additionally, the user can associate it to memory as the acronym "BLUE", as all items of the passphrase are somehow related to that word.
A 12 character complex password may look like this: "Hgc?Rfkzh94*"

A.2. SERVICE ACCOUNTS

Category	Standard (Where technically feasible)
Composition and length	Service account holders must choose a secure password that meets the following criteria: • The length of the password is a minimum of 20 characters. • The password contains a minimum of three random words. • The password must be changed when a user of the account has left the Department or no longer requires access to that account. Service account passwords must not be written down (unless they are secured in a safe or an approved encrypted USB storage device).

A.3. ADMINISTRATOR ACCOUNTS

Category	Standard (Where technically feasible)
Composition and length	Administrator account holders must choose a secure password that meets the following criteria: • The length of the password is a minimum of 20 characters. • The password contains a minimum of three random words. • The password is not the same as the administrator's normal user account password. • The password is not the same as any password that the administrator has used on any external or internet system. Administrator account passwords must not be written down (unless they are secured in a safe or an approved encrypted USB storage device).