Password Policy

PP01

This policy establishes guidelines to ensure the security of user passwords and protect against unauthorised access to organisational systems and data.

This policy applies to all employees, contractors, and third-party users with access to organisational IT resources.

Password Protection Measures

1. Authentication Mechanisms

All user accounts must implement at least one of the following protective measures:

Multi-Factor Authentication (MFA)

Throttling Login Attempts: The organisation will implement rate limiting on login attempts. Users will be required to wait longer between attempts after each unsuccessful login. Access will be limited to a maximum of 10 guesses within a 5-minute window.

Account Lockout: Accounts will be locked after a maximum of 10 unsuccessful login attempts to prevent brute-force attacks.

2. Password Quality Management

The organisation will employ technical controls to ensure the quality of passwords:

Minimum Password Length: Passwords must be at least 12 characters long, with no maximum length restrictions OR at least 8 characters long, with no maximum limit and the automatic blocking of common passwords using a deny list.

3. User Education

To support users in creating unique and secure passwords, the organisation will:

Educate on Common Password Pitfalls: Training sessions will be conducted to educate users on avoiding commonly used passwords (e.g., pet names, keyboard patterns, previously used passwords).

Promote Strong Password Creation Techniques: Encourage users to create longer, memorable passwords using at least three random words, following the National Cyber Security Centre (NCSC) guidance.

Provide Password Management Resources: Users will be provided with secure password storage solutions, such as password managers, and guidance on how to use them effectively.

4.Password Storage

Passwords must be stored securely using an organisation-approved password manager or in a secure locked cabinet. Access to these storage solutions will be restricted to authorised personnel.

Responsibilities

IT Security Team: Responsible for implementing protective measures, monitoring compliance, and providing necessary training.

All Staff: Required to adhere to this policy and participate in training sessions related to password security.

Policy Author: J Short	**Approved by**: Jonathan Smith (CEO)	**Version:** 1
	Approved date: 17/10/2024	**Next revision date**: 1710/2025