PASSWORD POLICY

Version 1.4 | Effective Date: March 1, 2025 | Classification: INTERNAL

1. PURPOSE

This policy establishes the standards for creation, protection, and management of strong passwords to protect TNO systems and data from unauthorized access.

2. SCOPE

This policy applies to all TNO employees, contractors, vendors, and any other individuals with access to TNO information systems.

3. POLICY REQUIREMENTS

3.1 Password Creation

1. All passwords must be at least 12 characters long.
2. Passwords must contain characters from at least three of the following categories:
   - Uppercase letters (A-Z)
   - Lowercase letters (a-z)
   - Numbers (0-9)
   - Special characters (e.g., !, @, #, $, %)
3. Passwords must not contain the user's name or username.
4. Dictionary words must not be used as passwords without modification.

3.2 Password Management

1. Passwords must be changed every 90 days.
2. New passwords must not be identical to any of the previous 10 passwords.
3. Initial or reset passwords must be temporary and changed at first login.
4. Passwords must not be shared with anyone, including IT support staff.

3.3 Account Lockout

1. User accounts will be locked after 5 consecutive failed login attempts.

2. Locked accounts will remain locked for a minimum of 15 minutes.

3. Accounts with administrative privileges will require administrator intervention to unlock.

4. COMPLIANCE

All TNO information systems must enforce these password requirements through technical controls where possible. Non-compliance with this policy may result in disciplinary action.

APPROVED BY:

Robert Bruce, IT Security Manager

Date: March 1, 2025