WILEY

Password Management Policy

1. Introduction

1.1. Policy Purpose:

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of Wiley's resources. All users, including contractors and vendors with access to Wiley systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The objective of this Password Security Policy is to define the required minimum configurations for passwords associated with Wiley accounts, applications and devices which are utilized for authentication and authorization.

1.2. Policy Scope

This policy applies to all Wiley systems, applications, data including contracted/hosted services and all users (e.g., employees, contractors, consultants, suppliers, customers, government, academic agencies, and all personnel affiliated with third parties) worldwide who access and/or use Wiley devices and data.

2. Policy

2.1. Password Management

2.1.1. Password Requirements

The following sections describe the password requirements users must follow to promote strong authentication credentials and the protection of these credentials.

a. General Password Settings:

A minimum password length must be set, passwords must contain at least three password complexity requirements (One lower case letter, one upper case letter, one number, one special character) including, the requirement of 8 characters or greater. Account shall be locked out after continuous unsuccessful login attempts; the lockout duration and idle session time out will be set.

b. Password Expiration or Password lifetime

Passwords must be set to expire at the maximum password age unless the account has Multi-Factor Authentication (MFA), or Two-Factor Authentication (2FA) configured.

c. Password History

The new password cannot be the same as the current password and history of passwords are maintained.

d. Initial or First-Time Passwords

- Systems must require users to change the password according to password complexity and general password settings at first logon and except for verbal communications, passwords must not be delivered in the same message with the account name.
- The initial password must be randomly generated and follow the policy for password complexity.
- The initial password must not be obvious (e.g., NewYork123).
- Each user must be provided with a unique password.
- Initial (or reset) passwords must be communicated in a way that ensures no misuse or interception.

e. Other Password Constraints

- Passwords shall not be stored/transmitted in clear text or in any easily reversible form.
- Personal accounts and passwords are not to be used or embedded in any application or system to run services or for automated logon. Service accounts must be used to run services / automated processes.
- Identification and authentication systems shall allow users to change their own personal account passwords.
- Passwords must never be shared or revealed to anyone other than the authorized personnel.

f. Multi Factor Authentication

Multi Factor Authentication must be implemented and used wherever possible.

g. Other password requirements

- All applications and system manufacturer default accounts and passwords must be deleted, passwords should be masked, reset passwords must be validated and changed after the first use.

- Users must report all suspected password security incidents.

3. Revision History:

Document Properties

Policy	Password Management Policy
Last Review Date	21st June 2024
Approved by	Robyn Wright – CISO & DPO
Classification	**Public** (Can be externally shared)