|  |  |
| --- | --- |
| **NWC OT Cybersecurity Password Management Policy** | |
| **Document Number:** | A01001045-POL-PM |
| **Issue Date:** | 08-Dec-21 |
| **Revision Number:** | 00 |
| **Issued For:** | Review |

**Revision Details**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | | **Title/Dept.** | **Signature** | | **Date** |
| **Prepared by:** | | | | | |
| Sidrat Mehreen | Senior OT Cybersecurity Analyst | |  | July 27, 2021 | |
|  |  | |  |  | |
|  |  | |  |  | |
|  |  | |  |  | |
| **Reviewed by:** | | | | | |
| Sameen Ullah Khan | | OT Cybersecurity Lead |  | July 31, 2021 | |
|  | |  |  |  | |
| **Approved by:** | | | | | |
| Mubarik Mustafa | | Cybersecurity Consultant |  | August 03, 2021 | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Issued by:** | | | |
| Syed Ali Raza | Planning Engineer |  | Dec 08, 2021 |

**History Page**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Approved By**  **(Name)** | **Endorsed By (Name)** | **Owned By**  **(Name)** | **Reviewed By**  **(Name)** | **Prepared By**  **(Name)** | **Issue Date** | **Issue**  **No.** |
|  |  |  |  |  |  |  |
|  | | | | | **Change Description** | |
|  |  |  |  |  |  |  |
|  | | | | | **Change Description** | |
|  |  |  |  |  |  |  |
|  | | | | | **Change Description** | |
|  |  |  |  |  |  |  |

**Reference Documents**

|  |  |
| --- | --- |
| **Document Number** | **Document Title** |
| ECC-1:2018 | National Cybersecurity Authority  Essential Cybersecurity Controls (NCA ECC) |

**Document Roles and Responsibilities**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Prepare/ Update/ Amend** | **Review** | **Approve** | **Publish** |
| **Owner** | YES | YES |  |  |
| **Cybersecurity Steering Committee** |  | YES |  | YES |
| **Corporate Strategy & Performance Management VP** |  |  | YES |  |

**Table of Contents**

[1. Password Management 7](#_Toc89882705)

[1.1 Purpose 7](#_Toc89882706)

[1.2 Scope and Applicability 7](#_Toc89882707)

[1.3 Guidance 7](#_Toc89882708)

[1.4 Terminology 8](#_Toc89882709)

[1.5 Policy 8](#_Toc89882710)

[2. Compliance 9](#_Toc89882711)

[3. Exception Criteria 9](#_Toc89882712)

**Glossary**

| **Word or Phrase** | **Explanation** |
| --- | --- |
| **Application** | A software program hosted by an asset/system. |
| **Asset** | A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems. |
| **Compliance** | Ensuring that a Standard or set of Guidelines is followed. A means of conforming to a rule, such as a specification, Policy, standard or law. |
| **Password** | A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization. |
| **Policies** | Reference documents and rules with the clear aim/goal to guide decisions and achieve desired outcomes.  Policies may be at an organization or company level, and These are used to implement the decisions and to organize the procedures and work process which have been defined by the respective departments according to the approved template and are aligned with the business objectives of the organization. |
| **Procedures** | the way of carrying out a process or activity. |
| **Purpose** | The business reason for the document and or the associated process. |
| **Review and approval** | The process steps are taken to ensure that policies and procedures are accurate and support the organization in meeting its objectives in an appropriate manner. The approval is the evidence that the review has been completed to satisfaction of the appropriate person e.g. CEO / Executive Committee / BOD. |
| **Standalone machines** | Individually managed devices (e.g., desktops, laptops, smartphones, tablets). |

# Password Management

## Purpose

This document outlines Password Management Policy in the Operational Technology (OT) environment of National Water Company (NWC). OT generally requires stricter protection regarding the information and hence should be protected with strong passwords. The compromise of such information could have a more significant impact.

OT Security Operations policies aim to define the purpose, direction, principles, and basic rules for OT cybersecurity management for NWC.

This Policy provides necessary guidance on procedures and protocols required for an effective Password Management specifically focused on NWC OT Environment.

## Scope and Applicability

The Policy governs the Password Management for all NWC OT systems, devices, or applications and information deployed to support the NWC OT Environment.

Systems include, but are not limited to control systems, as well as National Water Company, NWC electronic services, systems, and servers for information deployment in support of NWC OT Environment at any level.

## Guidance

The Policy statements are in italics, where required, in <…>. It’s the rationale for each paragraph, clause, or section is non-italics, where required, in [….].

## Terminology

|  |  |
| --- | --- |
| **Term** | **Definition** |
| *SHALL* | *This term is used to state* ***Mandatory*** *requirements* |
| *SHOULD* | *This term is used to state* ***Recommended*** *requirements* |
| *MAY* | *This term is used to state an* ***Optional*** *requirement.* |

## Policy

1. *A formal documentation for password procedure shall be documented for different type of OT assets in scope including (not limited to) windows and no-windows based machines, standalone machines, controllers, and field devices.*
2. *The documentation shall be formally communicated and enforced throughout NWC.*
3. *NWC shall ensure that all user accounts are protected by strong passwords, where applicable and that the strength of the passwords meets the minimum-security requirements of the system.*
4. *Passwords shall be securely transmitted to the individual through Password Management Procedure.*
5. *Wherever possible NWC shall implement system password polices (not specific to ICS field devices).*
6. *Password’s log shall be maintained.*
7. *A password storage management solution shall be implemented to store passwords in a central encrypted database secured by a master password.*
8. *Password recovery and expiry policies shall be implemented to all OT systems in scope whether standalone or within OT Domain.*
9. *Password recovery and change procedure shall be documented.*
10. *Passwords where applicable on OT systems shall abide by this policy.*

# Compliance

1. *This Policy shall be reviewed and updated regularly by the OT Cybersecurity Committee. NWC (if required) shall ensure that it remains appropriate in the light of any relevant changes to the law, organizational policies, or contractual obligations.*
2. *This Policy shall be reviewed and audited by an auditor external to National Water Company.*
3. *NWC may create additional regulations to cover specific areas beyond the scope of this Policy.*
4. *OT Cybersecurity Committee comprises representatives from all relevant parts of the organization. It shall oversee the creation of cybersecurity and subsidiary policies.*

# Exception Criteria

1. *This Policy addresses cyber security requirements related to Password Management. If needed, exceptions shall be formally submitted to the OT Cybersecurity Committee, including justification and benefits attributed to the exception.*
2. *The policy waiver period has a maximum period of one year and shall be re-assessed and re-approved, if necessary, for a maximum of three consecutive terms.*
3. *No Policy shall be provided an exception for more than three consecutive terms.*