NWC OT Cybersecurity Password Management Procedure

Document Number:	A01001045-PRO-PM
Issue Date:	August 16, 2021
Revision Number:	01
Issued For:	Approval

Revision Details

Name	Title/Dept.	Signature	Date
Prepared by:			
Sidrat Mehreen	Senior OT Cybersecurity Analyst		August 07, 2021
Reviewed by:			
Sameen Ullah Khan	OT Cybersecurity Lead		August 08, 2021
Approved by:			
Farhan Rasheed	Operations Manager		August 10, 2021

Issued by:			
Syed Ali Raza	Planning Engineer		August 16, 2021

History Page

Issue No.	Issue Date	Prepared By (Name)	Reviewed By (Name)	Owned By (Name)	Endorsed By (Name)	Approved By (Name)
00	July 15, 2021	Sidrat Mehreen	Sameen Ullah Khan			Farhan Rasheed Khan
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

Glossary

Word or Phrase	Explanation
Asset	General support system, major application, resources, high impact program, physical plant, or a logically related group of systems
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures.
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.
Recovery	Actions necessary to restore data files of an information system and computational capability after a system failure.

1. Introduction

This procedure is applicable to all NWC OT infrastructure.

2. Roles and Responsibilities

Roles	Responsibilities
OT Admin	• OT Admin shall only create/update/modify/Unlock user • Reset password
OT User	• Initiates access request
System Administrator	• Users/Computers which are manage or maintain using Active Directory, for those users, system administrator is OT admin • For network devices, system administrator is network team • For L0-1 devices, system administrator is smart operations team • For SCADA application, system administrator is SCADA O&M team • For ePO application, system administrator is ePO Admin

3. Password Management

3.1 Password Change

As per acceptable use policy in all devices in NWC OT domain.

Password change is done according to access management policy and procedure.

3.2 Minimum Standards for Windows based Machines

1. Following are the minimum standards for password management on all multi-user windows based. Systems include:
   - all the engineering and operating workstations
   - Monitoring screens
   - Servers

Password Characteristics	Details
Minimum password length	12 characters or max available EWS/OWS 14 characters
Maximum password length	Not defined
Special Characteristics	Six or more special characters or the maximum complexity supported by the IACS.
Password expiry period	For Windows based system, 45 days expiry period
History requirement	10 different values
Maximum log-in attempts	10 attempts

Table 3.2.1: Windows Machines

3.3 Minimum Password Standards for Non-Windows Machines

1. Following are the minimum standards for password management on all multi-user non-windows machines. Systems include:
   - Network Devices
   - Controllers and field devices
   - Standalone Machines

3.3.1 Network devices

Password Characteristics	Details
Minimum password length	A minimum password length that is at least twelve characters
Maximum password length	The maximum length supported by the IACS asset

Specific Characteristics	Symbols, Alphanumeric characters
Password Expiry period	Automatically expire every 2 months maximum for IACS
History requirement	24 password histories
Maximum log-in attempts	Log-in attempts will be three

Table 3.3.1: Non-Windows Machines (Network devices)

3.3.2 Controllers and field devices

Password Characteristics	Details
Minimum password length	Level 0-1 devices as per vendor requirement
Maximum password length	Level 0-1 devices as per vendor requirement
Specific Characteristics	Level 0-1 devices as per vendor requirement
Password Expiry period	Level 0-1 devices as per vendor requirement
History requirement	SCADA events are logged in SCADA servers whereas other devices do not hold a history.

Table 3.3.2: Non-Windows Machines (Controller & Field devices)

3.3.3 Standalone Machines

Password Characteristics	Details
Minimum password length	For windows-based, refer to table 3.2.1 of document. For non-windows-based, refer to table 3.3.1 & 3.3.2 of document.
Maximum password length	For windows-based, refer to table 3.2.1 of document. For non-windows-based, refer to table 3.3.1 & 3.3.2 of document.
Specific Characteristics	For windows-based, refer to table 3.2.1 of document. For non-windows-based, refer to table 3.3.1 & 3.3.2 of document.
Password Expiry period	For windows-based, refer to table 3.2.1 of document. For non-windows-based, refer to table 3.3.1 & 3.3.2 of document.
History requirement	For windows-based, refer to table 3.2.1 of document. For non-windows-based, refer to table 3.3.1 & 3.3.2 of document.

3.4 Password Recovery

1. Failed log-in attempts or expiry for passwords results in account lock-out.
2. OT User requests the recovery of password to OT Admin by submitting access control form. The justification for account lockout is to be communicated correctly through that form.

4. Process

Activities for Password recovery and Password change is as follows:

Activity		Description
1.1	Password recovery/change request initiator	OT User initiates the process of password change/password recovery in case of • Forgotten password • Account lock-out due to several attempts • Password expiry
1.2	Request approver	Line manager evaluates and approve or reject the request
1.3	Change performer	Respective team's system administrator performs changes
1.5	Close the request	Initiated request is closed and logged.

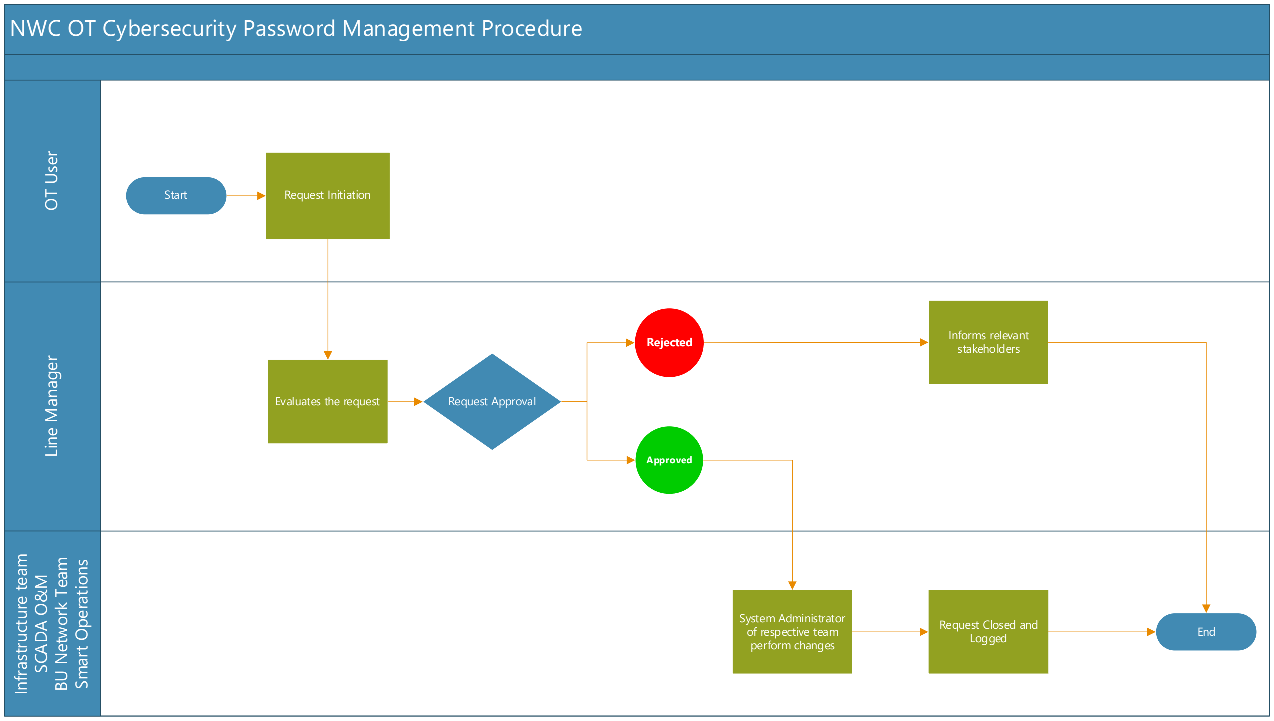
5. Audit and Compliance

1. Password logs will be enabled in Domain Controller for windows machine for audit and compliance.
2. For SCADA machines, password logs will be enabled in SCADA servers.

6. Exceptions

1. Exceptions will be documented for each machine installed in OT environment for password enabling.
2. Field devices which do not support password features will be documented and communicated to Smart Operations and SCADA O&M Team prior installation.

5. Process flowchart


NWC OT Cybersecurity Password Management Procedure
OT User
Line Manager
Infrastructure team
SCADA O&M
BU Network Team
Smart Operations
Start
Request Initiation
Evaluates the request
Request Approval
Rejected
Approved
Informs relevant stakeholders
System Administrator of respective team perform changes
Request Closed and Logged
End

PROPRIETARY NOTICE

THIS DOCUMENT CONTAINS INFORMATION PROPRIETARY TO NWC. ANY DISCLOSURE OR USE THEREOF IS EXPRESSLY PROHIBITED EXCEPT UPON THE WRITTEN PERMISSION OF NWC.