
	NWC OT Endpoint Protection Management Procedure	Page 1 of 13
	Document Type: Procedure	July 15, 2021
	Document Classification: Internal & Confidential	

NWC OT Cybersecurity Endpoint Protection Management Procedure	
Document Number:	A01001045-PRO-EP
Issue Date:	July 29, 2021
Revision Number:	00
Issued For:	Review

PROPRIETARY NOTICE

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


	NWC OT Cybersecurity Endpoint Protection Management Procedure	Page 2 of 13
	Document Type: Procedure	July 15, 2021
	Document Classification: Internal & Confidential	

Revision Details

Name	Title/Dept.	Signature	Date
Prepared by:			
Sidrat Mehreen	Senior OT cybersecurity Analyst		July 12, 2021
Reviewed by:			
Sameen Ullah Khan	OT Cybersecurity Lead		July 13, 2021
Approved by:			
Farhan Rasheed	Operations Manager		July 13, 2021
Issued by:			
Syed Ali Raza	Planning Engineer		July 15, 2021

PROPRIETARY NOTICE

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


 المياه الوطنية	NWC OT Cybersecurity Endpoint Protection Management Procedure		Page 3 of 13
	Document Type: Procedure		July 15, 2021
	Document Classification: Internal & Confidential		

History Page

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

PROPRIETARY NOTICE

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

	NWC OT Cybersecurity Endpoint Protection Management Procedure	Page 4 of 13
	Document Type: Procedure	July 15, 2021
	Document Classification: Internal & Confidential	

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	

PROPRIETARY NOTICE

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



	NWC OT Cybersecurity Endpoint Protection Management Procedure	Page 5 of 13
	Document Type: Procedure	July 15, 2021
	Document Classification: Internal & Confidential	

Table of Contents

1. Introduction	8
2. Roles and Responsibilities	8
3. Patch Management Procedure	9
3.1 SCADA Servers and Workstations	9
3.2 Standalone Systems	10
3.3 Process	10
3.4 Security updates/signatures Frequency	11
4. Exception Handling	12
5. Security update Compliance	12
6. Process Flow Chart.....	13

PROPRIETARY NOTICE

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


	NWC OT Cybersecurity Endpoint Protection Management Procedure	Page 6 of 13
	Document Type: Procedure	July 15, 2021
	Document Classification: Internal & Confidential	

Glossary

Word or Phrase	Explanation
Asset	General support system, major applications, resources, high impact program, physical plant, or a logically related group of systems
Asset Register	Location, condition, owner, status, procurement dates, depreciation or values of the assets
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.
Backup	Copying data to protect against loss of Integrity or Availability of the original.
BU	Business Unit- Represents a specific line to the business and is a part of firm's value chain of activities including operations, accounting, HR, marketing and sales.
Central Endpoint Protection Management system	A database where all asset owners will update and maintain current level of security updates/signatures. It will also check compliance status when it comes to security updates/signatures.
Change Request Form	The change request form is the primary tool used for requesting, approving, and documenting changes to the project and is an important piece of the change management process (here referring to change management procedure)

PROPRIETARY NOTICE


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

	NWC OT Cybersecurity Endpoint Protection Management Procedure	Page 7 of 13
	Document Type: Procedure	July 15, 2021
	Document Classification: Internal & Confidential	

Word or Phrase	Explanation
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.
Integrity	The property of safeguarding the accuracy and completeness of assets.
Test Environment	A controlled Environment used to test Configuration Items, Software Builds, OT/IT Services, Processes, etc.
Asset	General support system, major applications, resources, high impact program, physical plant, or a logically related group of systems
Asset Register	Location, condition, owner, status, procurement dates, depreciation or values of the assets
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.
CAB	Change Approval Board
EPP	Endpoint Protection

PROPRIETARY NOTICE

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

	NWC OT Cybersecurity Endpoint Protection Management Procedure	Page 8 of 13
	Document Type: Procedure	July 15, 2021
	Document Classification: Internal & Confidential	

1. Introduction

This document provides the procedure necessary to maintain the availability and integrity of OT systems and data by applying the latest security updates/signatures in a timely manner, and to establish a baseline methodology and time frame for updates/signatures and confirming central endpoint protection management system compliance.


This procedure is applicable to all NWC OT infrastructure.

2. Roles and Responsibilities

Roles	Responsibilities
OT EPP Admin	OT EPP Admin shall have the following responsibilities, not limited to: <ul style="list-style-type: none"> • Get the latest security updates/signatures from IT EPP admin • Provide list of latest security updates/signatures to SCADA O&M Team • Get the approval from change management for security updates/signatures • Push vendor approved security updates/signatures provided by SCADA O&M Team on servers and workstations
SCADA O&M Team	SCADA O&M Team shall have the following responsibilities, not limited to: <ul style="list-style-type: none"> • Provide list of vendor approved security updates/signatures to OT EPP Admin • Confirm and provide details of all the exclusions • Provide Timing at which the updates/signatures is to be done manually • Provide grouping of SCADA systems based on Asset location, Operating System & Installed Softwares for deployment approval • All security updates/signatures to be deployed using Change Management Process

PROPRIETARY NOTICE

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

	NWC OT Cybersecurity Endpoint Protection Management Procedure	Page 9 of 13
	Document Type: Procedure	July 15, 2021
	Document Classification: Internal & Confidential	

Roles	Responsibilities
Infrastructure Team	Infrastructure Team shall: <ul style="list-style-type: none"> • Assist OT EPP Admin through the process • Install approved security updates/signatures on servers and workstations
IT Helpdesk	<ul style="list-style-type: none"> • Backup and Recovery Mechanisms

3. Endpoint Protection Management Procedure

Note1: Endpoint Protection Management procedure shall follow change management process.

Note2: All security updates/signatures must be done after approval of change request.

Note3: All security updates/signatures must be done after establishing backup and recovery mechanism.

Note4: Record of all updates/signatures shall be maintained in central endpoint protection management system.

Note5: All security updates/signatures must be done as per OEM and vendor recommendations.

Note6: All security updates/signatures must be scheduled to reduce operational impact.


Note7: All the updates/signatures installed are logged and updated manually in central endpoint protection management system whether successful or not.

3.1 Servers and Workstations

1. OT EPP Admin will get the list of latest security updates/signatures from IT EPP Admin.
2. OT EPP Admin will shared those latest security updates/signatures with SCADA O&M Team for vendor approval.
3. SCADA O&M Team will get the approved list of security updates/signatures from vendor and provide it to OT EPP Admin with all the exclusions.
4. OT EPP Admin will initiate change request for deployment and installations of the applicable vendor approved security updates/signatures.

PROPRIETARY NOTICE

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

 المياه الوطنية	NWC OT Cybersecurity Endpoint Protection Management Procedure	Page 10 of 13
	Document Type: Procedure	July 15, 2021
	Document Classification: Internal & Confidential	

5. IT helpdesk will create backup and recovery mechanisms. IT helpdesk must take manual backups before deployment and installation of critical updates.
6. OT EPP Admin will push applicable vendor approved security updates/signatures to workstations and servers.
7. Infrastructure Team will assist OT EPP Admin through this activity and install approved security updates/signatures on servers and workstations.
8. IT Helpdesk shall restore OT workstations and servers to its original state in case of major failures by any restoration mechanism adopted in step 5.
9. Update Central Endpoint Protection Management System.

3.2 Standalone Systems


1. Standalone systems in OT environment will be segregated upon the type, as follows:
 - a. Laptops/ workstations
 - b. Servers
2. A list of vendor approved security updates/signatures as published by the vendor will be obtained from SCADA O&M team.
3. OT EPP Admin will be responsible for pushing security updates/signatures using approved medium.
4. IT helpdesk must take manual backups installation of critical updates.
5. In case of any failure during update process, backup and recovery is implemented, already documented, and communicated to OT Asset Owners.
6. Update central endpoint protection management system.

3.3 Process

Activity		Procedure
1.1	Receive Latest Security updates/signatures	OT EPP Admin will get the latest updates/signatures from IT EPP Admin and share it with SCADA O&M Team for vendor approval
1.2	Vendor approved security update list	SCADA O & M will provide a list of vendor approved security updates/signatures as published by the vendor with all the exclusions

PROPRIETARY NOTICE

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

	NWC OT Cybersecurity Endpoint Protection Management Procedure	Page 11 of 13
	Document Type: Procedure	July 15, 2021
	Document Classification: Internal & Confidential	


1.3	Initiate security update process	OT EPP Admin initiates the process for security updates/signatures by submitting a change request form.
1.5	Change Management Approval	Change Manager will approve the change request form upon receiving the form and evaluates security updates/signatures with compliance to Change Management Procedure
1.6	Backup and Recovery process	IT helpdesk will create backup and recovery mechanisms. IT helpdesk must take manual backups for critical updates
1.5	Pushing security updates/signatures	OT EPP Admin will push applicable vendor approved security updates/signatures on servers, workstations and standalone machines
1.5	Implement the Security updates/signatures	The security updates/signatures will be implemented by Infrastructure Team on all the systems.
1.6	Backup and Recovery process (In case of failure)	If security updates/signatures are unsuccessful due to any reason, backup and recovery of the system will be performed with informing respective Team.
1.7	Close the process	The process will be closed by updating the central endpoint protection management system

3.4 Security updates/signatures Frequency

Stakeholders shall determine frequency of security updates/signatures based on criticality, vulnerabilities, location, and other aspects for every asset in OT Asset Inventory. Typically security updates/signatures installation will be performed after every 2/3 days.

PROPRIETARY NOTICE

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

	NWC OT Cybersecurity Endpoint Protection Management Procedure	Page 12 of 13
	Document Type: Procedure	July 15, 2021
	Document Classification: Internal & Confidential	

4. Exception Handling


1. Exceptions must be approved during the change management process.
2. Risk assessment/Vulnerability will be a part of the change management but subject to approval from CAB.

5. Security update Compliance

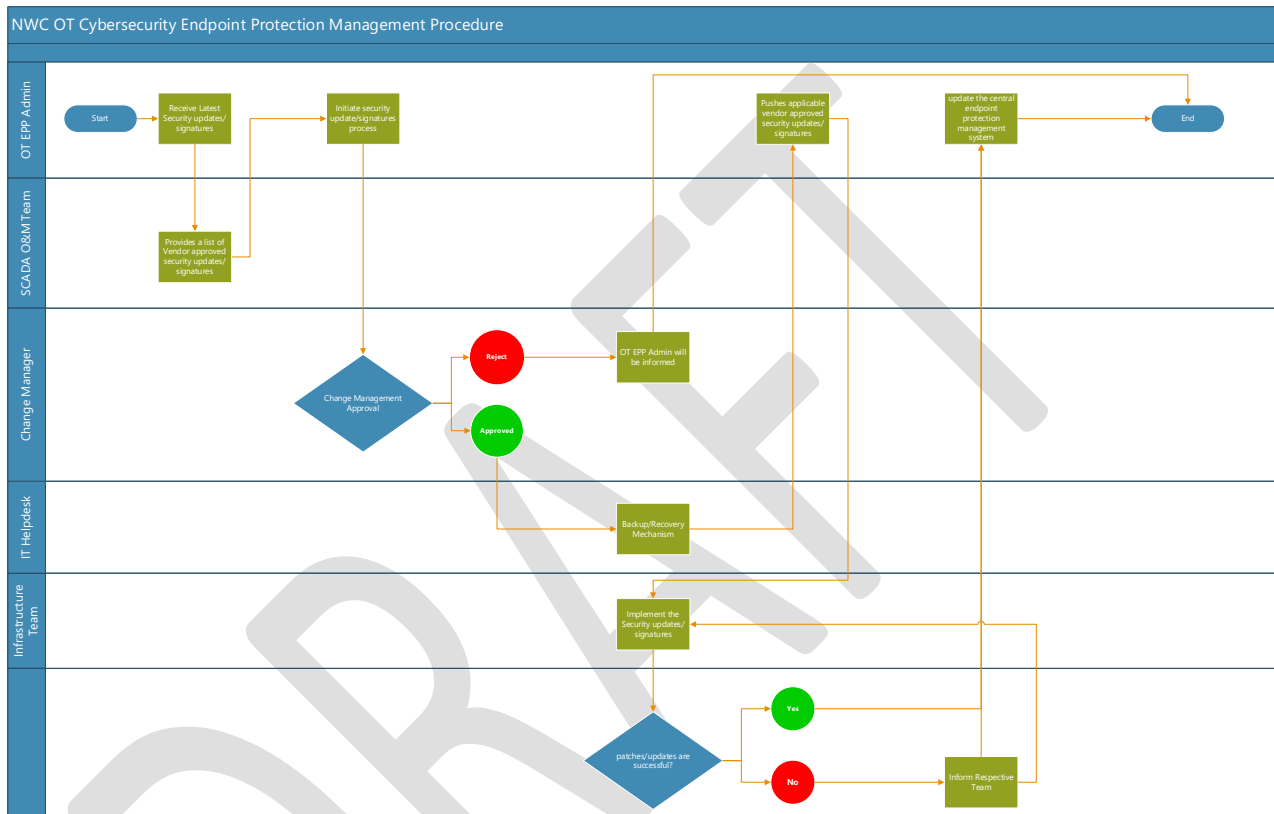
1. Updates/signatures report shall be originated for compliance.
2. In reviewing the report, respective stakeholders will identify non-updated machines.
3. The compliance of the Central Endpoint Protection Management System shall be done annually.

PROPRIETARY NOTICE

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

	NWC OT Cybersecurity Endpoint Protection Management Procedure	Page 13 of 13
	Document Type: Procedure	July 15, 2021
	Document Classification: Internal & Confidential	

6. Process Flow Chart



PROPRIETARY NOTICE

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