



|   |   |                        |
|---|---|------------------------|
|  | <b>NWC OT Cybersecurity System and Network Security Procedure</b> | <b>Page 1 of 24</b>    |
|   | <b>Document Type: Procedure</b>                                   | <b>August 16, 2021</b> |
|   | <b>Document Classification: Internal and Confidential</b>         |                        |

| <b>NWC OT Cybersecurity System and Network Security Procedure</b> |                   |
|---|-------------------|
| <b>Document Number:</b>   | A01001045-PRO-SNS |
| <b>Issue Date:</b>  | August 16, 2021   |
| <b>Revision Number:</b>   | 00                |
| <b>Issued For:</b>  | 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.


|   |   |                        |
|---|---|------------------------|
|  | <b>NWC OT Cybersecurity System and Network Security Procedure</b> | <b>Page 2 of 24</b>    |
|   | <b>Document Type: Procedure</b>                                   | <b>August 16, 2021</b> |
|   | <b>Document Classification: Internal and Confidential</b>         |                        |

## Revision Details

| Name                | Title/Dept.                     | Signature | Date            |
|---------------------|---------------------------------|-----------|-----------------|
| <b>Prepared by:</b> |                                 |           |                 |
| Sidrat Mehreen      | Senior OT Cybersecurity Analyst |           | August 08, 2021 |
|                     |                                 |           |                 |
|                     |                                 |           |                 |
|                     |                                 |           |                 |
| <b>Reviewed by:</b> |                                 |           |                 |
| Sameen Ullah Khan   | OT Cybersecurity Lead           |           | August 10, 2021 |
|                     |                                 |           |                 |
| <b>Approved by:</b> |                                 |           |                 |
| Farhan Rasheed      | Operations Manager              |           | August 12, 2021 |
| <b>Issued by:</b>   |                                 |           |                 |
| Syed Ali Raza       | Planning Engineer               |           | August 16, 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.


|   |   |                        |
|---|---|------------------------|
|  | <b>NWC OT Cybersecurity System and Network Security Procedure</b> | <b>Page 3 of 24</b>    |
|   | <b>Document Type: Procedure</b>                                   | <b>August 16, 2021</b> |
|   | <b>Document Classification: Internal and Confidential</b>         |                        |

## 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.

|   |   |                 |
|---|---|-----------------|
|  | <b>NWC OT Cybersecurity System and Network Security Procedure</b> | Page 4 of 24    |
|   | <b>Document Type: Procedure</b>                                   | August 16, 2021 |
|   | <b>Document Classification: Internal and Confidential</b>         |                 |

## Reference Documents


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

## Document Roles and Responsibilities

|  | Prepare/<br>Update/<br>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.


|   |   |                        |
|---|---|------------------------|
|  | <b>NWC OT Cybersecurity System and Network Security Procedure</b> | <b>Page 5 of 24</b>    |
|   | <b>Document Type: Procedure</b>                                   | <b>August 16, 2021</b> |
|   | <b>Document Classification: Internal and Confidential</b>         |                        |

## Table of Contents

|     |   |    |
|-----|---|----|
| 1.  | Introduction .....                            | 7  |
| 1.1 | L0-1 Device Security Procedure .....          | 7  |
| 1.2 | SCADA Security Procedure .....                | 9  |
| 1.3 | Windows Security Procedure .....              | 12 |
| 1.4 | Infrastructure Security Procedure.....        | 14 |
| 1.5 | Remote Access Security Procedure.....         | 16 |
| 1.6 | Removable Media Procedure.....                | 16 |
| 1.7 | Secure File Transfer Security Procedure ..... | 16 |
| 1.8 | Network Security Procedure .....              | 17 |
| 2.  | Process Flow Chart.....                       | 20 |

### PROPRIETARY NOTICE

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


|   |   |                        |
|---|---|------------------------|
|  | <b>NWC OT Cybersecurity System and Network Security Procedure</b> | <b>Page 6 of 24</b>    |
|   | <b>Document Type: Procedure</b>                                   | <b>August 16, 2021</b> |
|   | <b>Document Classification: Internal and Confidential</b>         |                        |

## Glossary

| Word or Phrase           | Explanation  |
|--------------------------|--|
| <b>Asset</b>             | General support system, major application, resources, high impact program, physical plant, or a logically related group of systems   |
| <b>Audit</b>             | Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures. |
| <b>Backup</b>            | Copying data to protect against loss of Integrity or Availability of the original.   |
| <b>Compliance</b>        | 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.                                      |
| <b>Removable devices</b> | Portable data storage medium that can be added to or removed from a computing device or network.   |
| <b>SFT</b>               | Secure File Transfer   |
| <b>USB</b>               | Universal Serial Bus   |
| <b>CAB</b>               | Change Approval Body   |

### PROPRIETARY NOTICE

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

|   |   |                 |
|---|---|-----------------|
|  | <b>NWC OT Cybersecurity System and Network Security Procedure</b> | Page 7 of 24    |
|   | <b>Document Type: Procedure</b>                                   | August 16, 2021 |
|   | <b>Document Classification: Internal and Confidential</b>         |                 |

## 1. Introduction

This document provides the procedure to address system and network security requirements required to protect the NWC systems and network infrastructure, services, and resources.

Following are the procedures that are the part of system and network security procedure:

- L0-1 Device Security Procedure
- SCADA Security Procedure
- Windows Security Procedure
- Infrastructure Security Procedure
- Remote Access Procedure
- Removable Media Procedure
- Secure File Transfer Procedure
- Network Security Procedure

### 1.1 L0-1 Device Security Procedure

This procedure addresses the security aspects of L0-1 device access, Engineering station and application.

For L0-1 device security guidelines, Refer to L0-1 Device Security Standard.


All L0-1 device changes to be perform using change management procedure, for details refer to change management procedure.

#### 1.1.1 Roles and Responsibilities

| <b>Roles</b>             | <b>NWC Representative</b> | <b>Responsibilities</b>  |
|--------------------------|---------------------------|--|
| <b>Request Initiator</b> | Smart Operation           | Initiates request for: <ul style="list-style-type: none"> <li>• Accessing L0-1 device</li> <li>• Changes in L0-1 device application</li> <li>• Engineering Station used for changes in L0-1 devices</li> <li>• Provide time to perform the activity</li> </ul> |
| <b>Request Approver</b>  | Application Team          | Requester's Line manager, Security manager and change manager analyses   |

#### PROPRIETARY NOTICE

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

|   |   |                        |
|---|---|------------------------|
|  | <b>NWC OT Cybersecurity System and Network Security Procedure</b> | <b>Page 8 of 24</b>    |
|   | <b>Document Type: Procedure</b>                                   | <b>August 16, 2021</b> |
|   | <b>Document Classification: Internal and Confidential</b>         |                        |

|   |   |   |
|---|---|---|
|   | Smart Operation<br>Information Security<br>Change Manager | and accepts or rejects the request based on the justification provided by request initiator and business needs                                  |
| <b>Smart Operations Engineer or Authorized contractor</b> | Smart Operations  | Smart Operations Engineer or Authorized contractor will perform the requested activities and notify relevant stakeholders about task completion |
| <b>Request tracking and closing</b>                       | Information security                                      | Information security will ensure that all LO-1 device access and permission requests are tracked, closed and recorded.                          |


Following steps shall be taken for procedure:

1. The access request for LO-1 device, Engineering station and application by requestor is submitted to the line manager who analyses and approves or rejects the request based on justifications/business needs.  
Request shall include following (but not limited to below):
  - LO-1 device details
  - Engineering station details
  - Application/configuration change details
  - Change impact on process
  - Schedule and time duration of change
2. After line manager approval, Smart Operation must approve or reject the request.
3. Security manager must approve or reject the request based on the security risk associated with the request and business needs.
4. After security manager approval, change manager will analyze and approve or reject the request.
5. Once the activity is complete, the requestor will notify all relevant stakeholders and will close the access request.

#### PROPRIETARY NOTICE

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



|   |   |                 |
|---|---|-----------------|
|  | <b>NWC OT Cybersecurity System and Network Security Procedure</b> | Page 9 of 24    |
|   | <b>Document Type: Procedure</b>                                   | August 16, 2021 |
|   | <b>Document Classification: Internal and Confidential</b>         |                 |

6. Information security shall track, close, and record all L0-1 devices access and permission request.

#### 1.1.2 Process

| Activity |                                    | Procedure   |
|----------|------------------------------------|---|
| 1.1      | Request Initiation                 | Request initiator initiates request for accessing, changing, engineering stations and time required to perform activity                         |
| 1.2      | Approval of Request                | The request is analyzed and approved by line manager, security manager and Change Manager   |
| 1.3      | Performing the security activities | Smart Operations Engineer or Authorized contractor will perform the requested activities and notify relevant stakeholders about task completion |
| 1.4      | Request Tracking and Closing       | Information security will ensure that all L0-1 device access and permission requests are tracked, closed, and recorded                          |

### 1.2 SCADA Security Procedure


This procedure addresses the security aspects of SCADA Server & Client, SCADA Application, SCADA Database, SCADA Configuration, SCADA Deployment and SCADA Interface Drivers.

For accessing SCADA, refer to access control procedure.

For all changes in SCADA, refer 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.

|   |   |                 |
|---|---|-----------------|
|  | <b>NWC OT Cybersecurity System and Network Security Procedure</b> | Page 10 of 24   |
|   | <b>Document Type: Procedure</b>                                   | August 16, 2021 |
|   | <b>Document Classification: Internal and Confidential</b>         |                 |

### 1.2.1 Roles and Responsibilities


| <b>Roles</b>                        | <b>NWC Representative</b>  | <b>Responsibilities</b>   |
|-------------------------------------|--|---|
| <b>Request Initiator</b>            | Smart Operations<br>SCADA O&M  | Initiates request for: <ul style="list-style-type: none"> <li>• SCADA Server &amp; Client Access</li> <li>• SCADA Application Launch permission</li> <li>• SCADA Database access and permission</li> <li>• SCADA Configuration access and permission</li> <li>• SCADA Deployment permission</li> <li>• SCADA Interface Drivers access and permission</li> </ul> |
| <b>Request Approver</b>             | SCADA O&M<br>Smart Operation<br>Information Security<br>Change Manager | Requester's Line manager, Security manager and change manager analyses and accepts or rejects the request based on the justification provided by request initiator and business needs   |
| <b>SCADA Admin</b>                  | SCADA O&M  | SCADA Admin will provide SCADA access and permission as per approved request and notify request approvers and requestor.  |
| <b>Request tracking and closing</b> | Information security   | Information security will ensure that all SCADA access and permission requests are tracked, closed and recorded.  |

Prerequisite to get SCADA access are:

- Requestor shall be OT User

#### PROPRIETARY NOTICE

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

|   |   |                 |
|---|---|-----------------|
| <br>المياه الوطنية | <b>NWC OT Cybersecurity System and Network Security Procedure</b> | Page 11 of 24   |
|   | <b>Document Type: Procedure</b>                                   | August 16, 2021 |
|   | <b>Document Classification: Internal and Confidential</b>         |                 |

- Requestor shall have OT User Account in OT Domain
- OT User shall have attended OT Security Awareness Training

Following steps shall be taken for procedure:


1. The access request for SCADA Server & Client, SCADA Application, SCADA Database, SCADA Configuration, SCADA Deployment and SCADA Interface Drivers by the requestor is submitted to the requestor line manager who analyses and approves or rejects the request based on business needs.
2. After line manager approval, SCADA O&M must approve or reject the request based on the justification provide and business needs.
3. Security manager must approve or reject the request based on the security risk associated with the request.
4. After security manager approval, change manager will analyze and approve or reject the request.
5. SCADA Admin shall provide access and permission as per approved request and notify request approvers and requestors.
6. Once the activity is complete, the requestor will notify all relevant stakeholders and will close the access request.
7. Information security shall track, close, and record all SCADA access and permission request.

### 1.2.2 Process

| <b>Activity</b> |                     | <b>Procedure</b>   |
|-----------------|---------------------|--|
| 1.1             | Request Initiation  | Request initiator from SCADA O&M and smart operations initiates request for accessing configurations, deployment, drivers, databases, and application launch permissions |
| 1.2             | Approval of Request | Requester's Line manager, Security manager and change manager analyses and accepts or rejects the request based on the justification                                     |

### PROPRIETARY NOTICE

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

|   |  |                 |
|---|--|-----------------|
| <br>المياه الوطنية | NWC OT Cybersecurity System and Network Security Procedure | Page 12 of 24   |
|   | Document Type: Procedure                                   | August 16, 2021 |
|   | Document Classification: Internal and Confidential         |                 |

|     |                                 |  |
|-----|---------------------------------|--|
|     |                                 | provided by request initiator and business needs   |
| 1.3 | Granting Access and Permissions | SCADA Admin will provide SCADA access and permission as per approved request and notify request approvers and requestor. |
| 1.4 | Request Tracking and Closing    | Information security will ensure that all SCADA access and permission requests are tracked, closed, and recorded.        |

### 1.3 Windows Security Procedure

This procedure addresses the security aspects of OT Servers and Client, OT Software, Patch Management and Removable media.


For changes in windows access and permissions, refer to access control procedure.

#### 1.3.1 Roles and Responsibilities

| Roles                    | NWC Representative   | Responsibilities   |
|--------------------------|--|--|
| <b>Request Initiator</b> | SCADA O&M<br>Infrastructure Team<br>Smart Operations                         | Initiates request for: <ul style="list-style-type: none"> <li>OT Servers and Client Access</li> <li>OT Software Installation (Source and License)</li> <li>Patch Management (Source)</li> <li>Removable media Access (Source, Destination, File source)</li> </ul> |
| <b>Request Approver</b>  | SCADA O&M<br>Infrastructure Team<br>Smart Operations<br>Information Security | Line manager, Security manager and change manager analyses and accepts or rejects the request based on the justification provided by request initiator and business needs  |

#### PROPRIETARY NOTICE

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

|   |   |                 |
|---|---|-----------------|
| <br>المياه الوطنية | <b>NWC OT Cybersecurity System and Network Security Procedure</b> | Page 13 of 24   |
|   | <b>Document Type: Procedure</b>                                   | August 16, 2021 |
|   | <b>Document Classification: Internal and Confidential</b>         |                 |

|                                     |   |  |
|-------------------------------------|---|--|
|                                     | Change Manager<br>Endpoint Support Team |  |
| <b>Request tracking and closing</b> | Information security                    | Information security will ensure that all OT server access and permission requests are tracked, closed and recorded. |

Following steps shall be taken for procedure:


1. The access request for Servers and Client Access, OT Software, Patch Management, Removable media by the initiator is submitted to the line manager who analyses and approves or rejects the request based on business needs.
2. After line manager approval, ePO Admin must approve or reject the request based on the justification provide and business needs.
3. Security manager must approve or reject the request based on the security risk associated with the activity and business needs.
4. After security manager approval, change manager will analyze and approve or reject the request.
5. Once the activity is complete, the requestor will notify all relevant stakeholders and will close the access request.
6. Information security shall track, close, and record all OT server access and permission request.

### 1.3.2 Process

| <b>Activity</b> |                    | <b>Procedure</b>  |
|-----------------|--------------------|---|
| 1.1             | Request Initiation | Request initiator from SCADA O&M, Smart Operations and Infrastructure team initiates request for OT Servers and Client Access, OT Software Installation, Patch Management, and Removable media Access |

#### PROPRIETARY NOTICE

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

|   |   |                 |
|---|---|-----------------|
|  | <b>NWC OT Cybersecurity System and Network Security Procedure</b> | Page 14 of 24   |
|   | <b>Document Type: Procedure</b>                                   | August 16, 2021 |
|   | <b>Document Classification: Internal and Confidential</b>         |                 |

|     |                              |  |
|-----|------------------------------|--|
| 1.2 | Approval of Request          | The request is analyzed and approved by line manager, security manager, Endpoint support team and Change Manager       |
| 1.3 | Request Tracking and Closing | Information security will ensure that all LO-1 device access and permission requests are tracked, closed, and recorded |

#### 1.4 Infrastructure Security Procedure

This procedure addresses the security aspects of Physical and Virtual Server, OS installation, Driver installation, BIOS upgrade, Firmware upgrade, Domain joining, Patch installation and Backup & Recovery.

For server access control, refer to access control procedure.


For all configuration changes, refer to change management procedure.

##### 1.4.1 Roles and Responsibilities

| Roles                    | NWC Representative   | Responsibilities   |
|--------------------------|--|--|
| <b>Request Initiator</b> | SCADA O&M<br>Infrastructure Team<br>Smart Operations<br>Infrastructure Team<br>Endpoint Support Team | Initiates access and permission request for: <ul style="list-style-type: none"> <li>Physical and Virtual Server Access and permission</li> <li>Domain joining permission</li> </ul> Initiate maintain request: <ul style="list-style-type: none"> <li>OS installation (Media and licensing)</li> <li>Driver installation (Source)</li> <li>Patch installation (Source)</li> <li>BIOS upgrade (Source)</li> </ul> |

#### PROPRIETARY NOTICE

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

|   |   |                 |
|---|---|-----------------|
|  | <b>NWC OT Cybersecurity System and Network Security Procedure</b> | Page 15 of 24   |
|   | <b>Document Type: Procedure</b>                                   | August 16, 2021 |
|   | <b>Document Classification: Internal and Confidential</b>         |                 |


|                                     |   |   |
|-------------------------------------|---|---|
|                                     |   | <ul style="list-style-type: none"> <li>Firmware upgrade (Source)</li> <li>Backup &amp; Recovery</li> </ul>  |
| <b>Request Approver</b>             | SCADA O&M<br>Infrastructure Team<br>Smart Operations<br>Information Security<br>Change Manager<br>Endpoint Support Team | Line manager, Security manager and change manager analyses and accepts or rejects the request based on the justification provided by request initiator and business needs |
| <b>Info Admin</b>                   | Infrastructure Team   | Info Admin will perform the requested activities and notify relevant stakeholders about task completion   |
| <b>Request tracking and closing</b> | Information security  | Information security will ensure that all OT server access and permission requests are tracked, closed and recorded.  |

Following steps shall be taken for procedure:

1. The access request for Physical and Virtual Server Access, OS installation, Driver installation, Domain joining and Patch management by the initiator is submitted to the line manager who analyses and approves or rejects the request based on business needs.
2. After line manager approval, ePO Admin must approve or reject the request based on the justification provide and business needs.
3. Security manager must approve or reject the request based on the security risk associated with the activity and business needs.
4. After security manager approval, change manager will analyze and approve or reject the request.
5. Once the activity is complete, the requestor will notify all relevant stakeholders and will close the access request.
6. Information security shall track, close and record all OT server access and permission request.

#### PROPRIETARY NOTICE

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

|   |   |                        |
|---|---|------------------------|
|  | <b>NWC OT Cybersecurity System and Network Security Procedure</b> | Page 16 of 24          |
|   | <b>Document Type: Procedure</b>                                   | <b>August 16, 2021</b> |
|   | <b>Document Classification: Internal and Confidential</b>         |                        |

#### 1.4.2 Process

| <b>Activity</b> |                                | <b>Procedure</b>  |
|-----------------|--------------------------------|---|
| 1.1             | Request Initiation             | Request initiator from SCADA O&M and smart operations, Infrastructure, Endpoint team initiates request for accessing physical and virtual servers, OS installation, driver and patch installation, BIOS upgrade, Firmware upgrade and backup & recovery |
| 1.2             | Approval of Request            | Requester's Line manager, Security manager and change manager analyses and accepts or rejects the request   |
| 1.3             | Performing security Activities | Info Admin will perform the requested activities and notify relevant stakeholders about task completion   |
| 1.4             | Request Tracking and Closing   | Information security will ensure that all OT server access and permission requests are tracked, closed, and recorded.   |

#### 1.5 Remote Access Security Procedure

Refer to remote access procedure for remote access security procedure.

#### 1.6 Removable Media Procedure

Refer to removable media procedure for removable media procedure.


#### 1.7 Secure File Transfer Security Procedure

Refer to secure file transfer procedure for secure file transfer security 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.



|   |   |                 |
|---|---|-----------------|
| <br><b>NWC</b><br>المياه الوطنية | <b>NWC OT Cybersecurity System and Network Security Procedure</b> | Page 17 of 24   |
|   | <b>Document Type: Procedure</b>                                   | August 16, 2021 |
|   | <b>Document Classification: Internal and Confidential</b>         |                 |

### 1.8 Network Security Procedure

This procedure addresses the security aspects of OT network devices (Switches, routers, firewalls, Nozomi etc.), Routing Tables Update, Traffic controlling, Traffic Shaping, Network Segmentation & VLAN and Network Monitoring.

For server access control, refer to access control procedure.


For changes in server, refer to change management procedure.

#### 1.8.1 Roles and Responsibilities

| Roles                    | NWC Representative   | Responsibilities  |
|--------------------------|--|---|
| <b>Request Initiator</b> | Network Team<br>SCADA O&M<br>Infrastructure Team<br>Smart Operations<br>Infrastructure Team<br>Endpoint Support Team | Initiates request for access: <ul style="list-style-type: none"> <li>Access control of network devices</li> </ul> Initiate request for configuration changes, it include following (but not limited to following): <ul style="list-style-type: none"> <li>Routers: Routing table update, traffic controlling</li> <li>OT asset IP assignment</li> <li>Firewall: Traffic shapping</li> <li>Switches: Network Segmentation &amp; VLAN</li> <li>Nozomi: OT Network Monitoring</li> </ul> |
| <b>Request Approver</b>  | Network Team<br>SCADA O&M<br>Infrastructure Team<br>Smart Operations<br>Information Security<br>Change Manager       | Line manager, Security manager and change manager analyses and accepts or rejects the request based on the justification provided by request initiator and business needs   |

#### PROPRIETARY NOTICE

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

|   |   |                 |
|---|---|-----------------|
|  | <b>NWC OT Cybersecurity System and Network Security Procedure</b> | Page 18 of 24   |
|   | <b>Document Type: Procedure</b>                                   | August 16, 2021 |
|   | <b>Document Classification: Internal and Confidential</b>         |                 |


|                                     |                              |   |
|-------------------------------------|------------------------------|---|
|                                     | Endpoint Support Team<br>CAB |   |
| <b>Network Admin</b>                | Network Team                 | Network team will perform the requested activities and notify relevant stakeholders about task completion                     |
| <b>Request tracking and closing</b> | Information security         | Information security will ensure that all OT network devices access and permission requests are tracked, closed and recorded. |

Following steps shall be taken for procedure:

1. The access request for control of network devices (Switches, routers, firewalls, Nozomi), Routing Tables Update, Traffic controlling Traffic Shaping, IP assignment, Network Segmentation & VLAN and Network Monitoring by the initiator is submitted to the line manager who analyses and approves or rejects the request based on business needs. For example, Requestor wants traffic controlling, he will provide following for Traffic controlling:
  - Traffic Details
  - Source IP Details
  - Destination IP Details
  - Source Port Details
  - Destination Port Details
  - Protocol Details
  - Application Details
  - Change required in existing routing tables (any static route)
2. After line manager approval, Security manager must approve or reject the request based on the security risk associated with the activity and business needs.
3. After security manager approval, CAB will analyze and approve or reject the request.
4. Once the activity is complete, the requestor will notify all relevant stakeholders and will close the access request.
5. Information security shall track, close and record all OT network device access and permission request.

#### PROPRIETARY NOTICE

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


|   |   |                 |
|---|---|-----------------|
| <br>المياه الوطنية | <b>NWC OT Cybersecurity System and Network Security Procedure</b> | Page 19 of 24   |
|   | <b>Document Type: Procedure</b>                                   | August 16, 2021 |
|   | <b>Document Classification: Internal and Confidential</b>         |                 |

### 1.8.2 Process

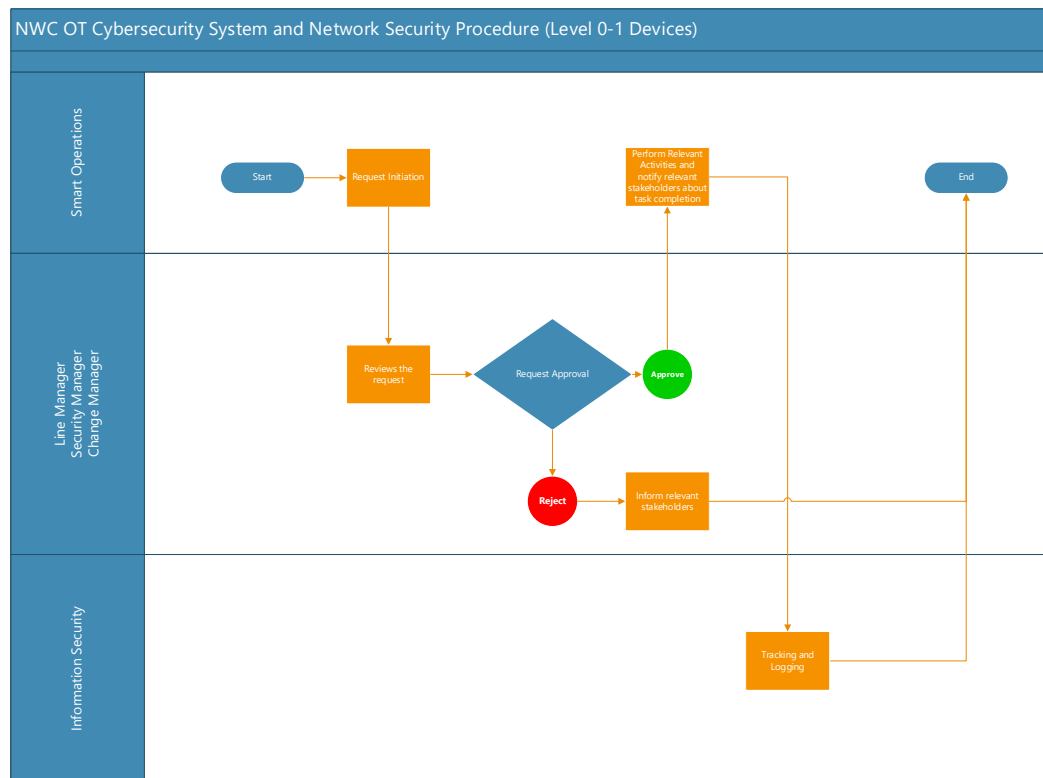
| <b>Activity</b> |                                | <b>Procedure</b>  |
|-----------------|--------------------------------|---|
| 1.1             | Request Initiation             | Request initiator from SCADA O&M smart operations, Infrastructure, Endpoint and Network team initiates request for accessing control of network devices |
| 1.2             | Approval of Request            | Requester's Line manager, Security manager and change manager analyses and accepts or rejects the request   |
| 1.3             | Performing security Activities | Network Admin will perform the requested activities and notify relevant stakeholders about task completion  |
| 1.4             | Request Tracking and Closing   | Information security will ensure that all OT server access and permission requests are tracked, closed, and recorded.                                   |

#### PROPRIETARY NOTICE

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


|   |  |  |                 |
|---|--|--|-----------------|
| <br>المياه الوطنية | NWC OT Cybersecurity System and Network Security Procedure |  | Page 20 of 24   |
|   | Document Type: Procedure                                   |  | August 12, 2021 |
|   | Document Classification: Internal and Confidential         |  |                 |

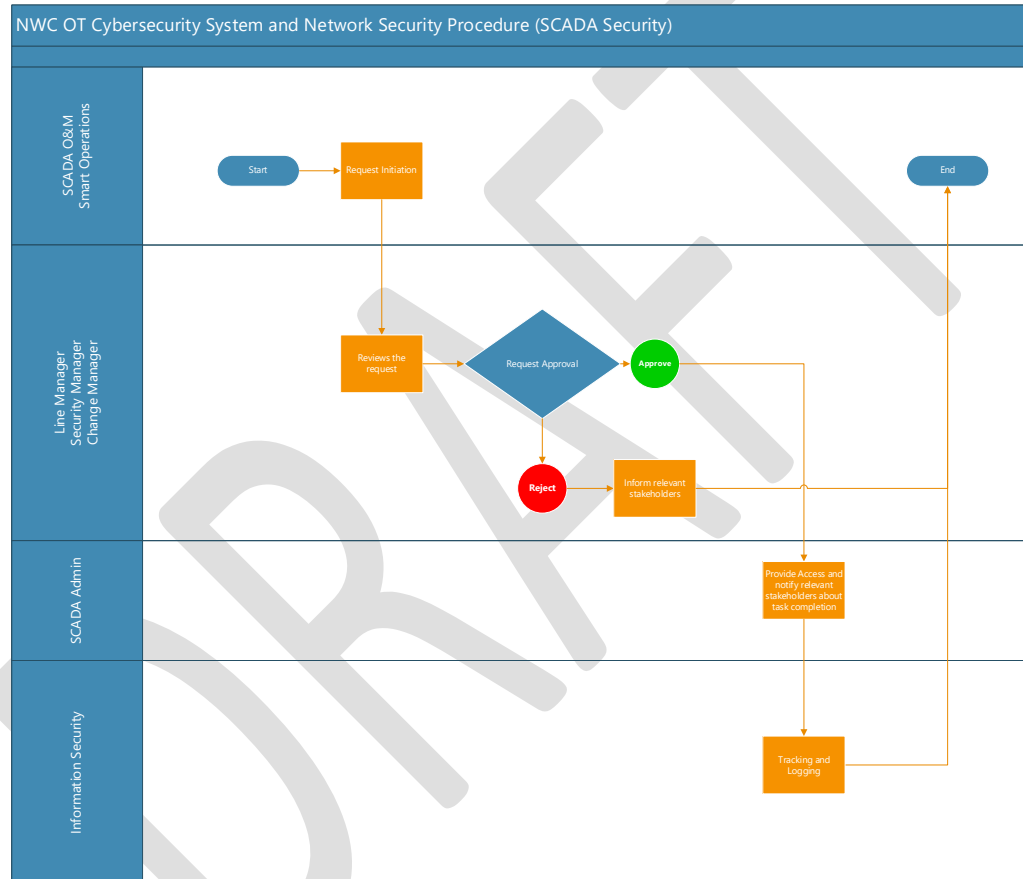
## 2. Process Flow Chart



### PROPRIETARY NOTICE


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

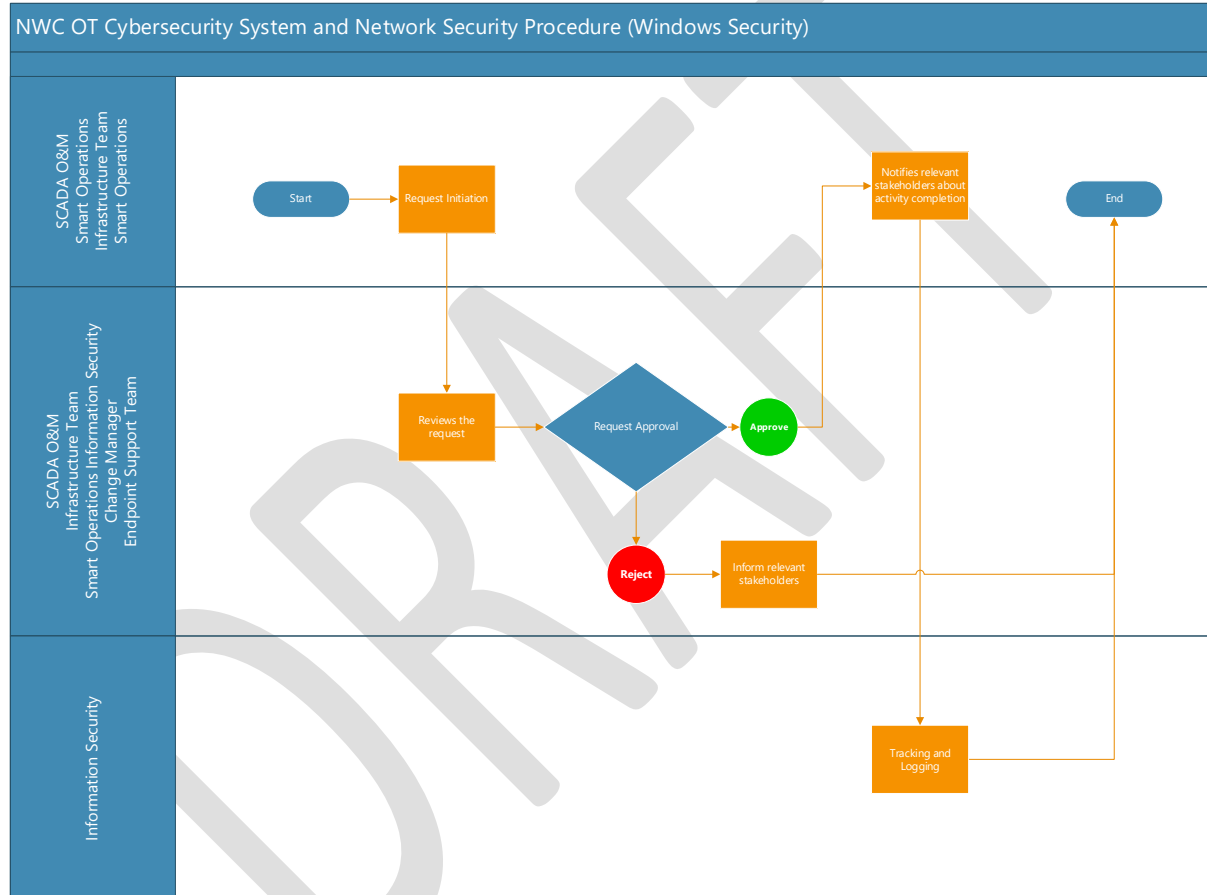
|   |   |                        |
|---|---|------------------------|
|  | <b>NWC OT Cybersecurity System and Network Security Procedure</b> | <b>Page 21 of 24</b>   |
|   | <b>Document Type: Procedure</b>                                   | <b>August 16, 2021</b> |
|   | <b>Document Classification: Internal and Confidential</b>         |                        |



## PROPRIETARY NOTICE


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

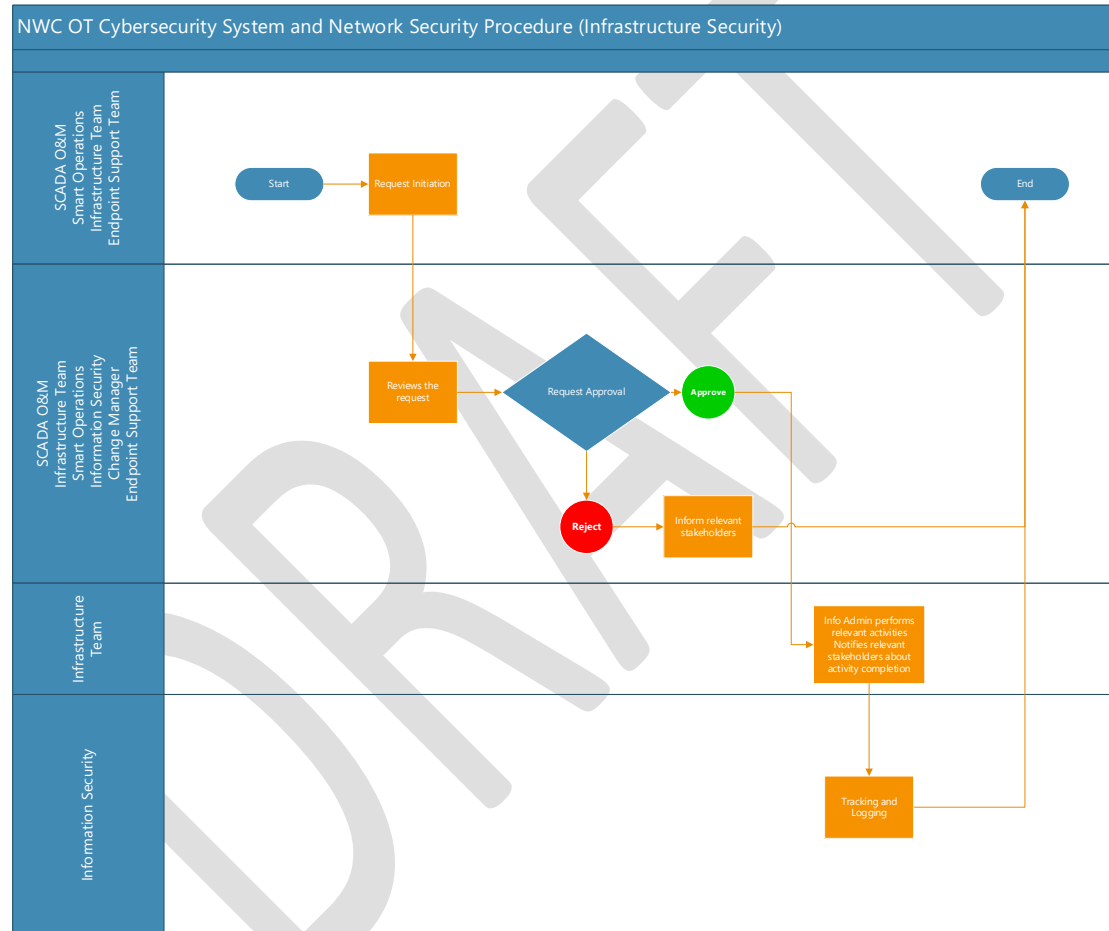
|   |   |                        |
|---|---|------------------------|
|  | <b>NWC OT Cybersecurity System and Network Security Procedure</b> | <b>Page 22 of 24</b>   |
|   | <b>Document Type: Procedure</b>                                   | <b>August 16, 2021</b> |
|   | <b>Document Classification: Internal and Confidential</b>         |                        |



#### PROPRIETARY NOTICE


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

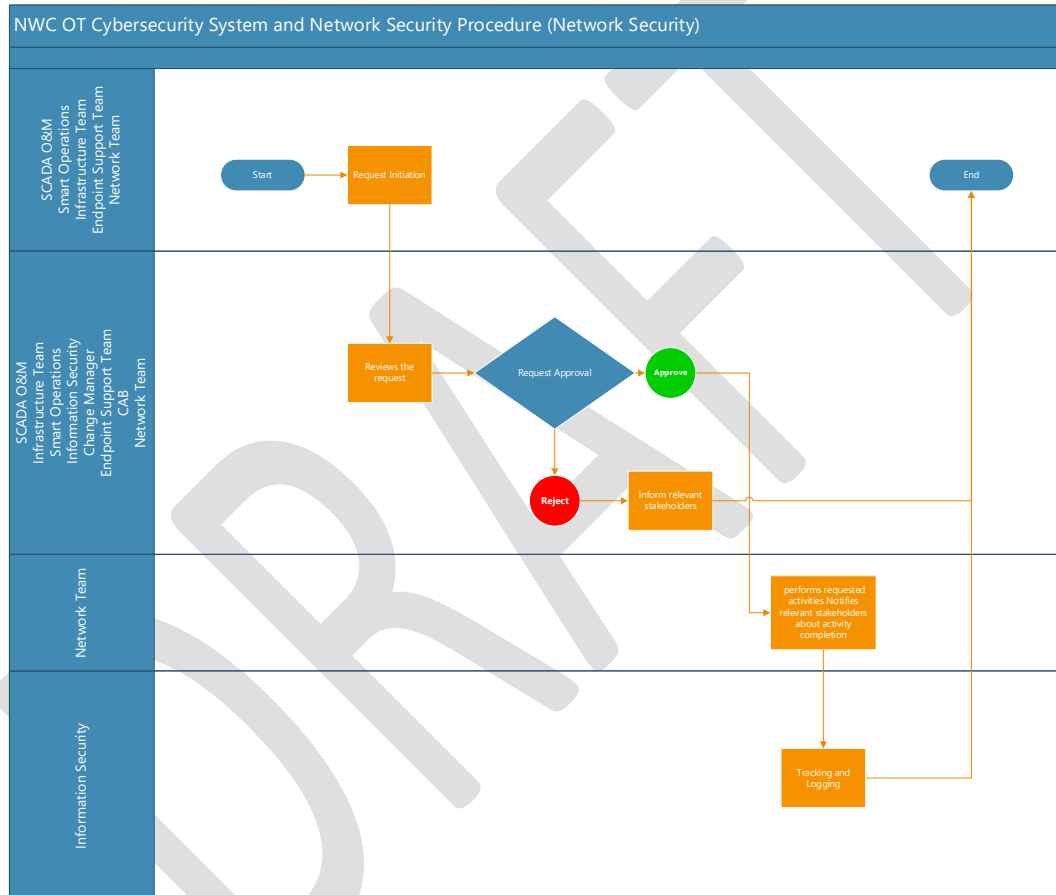
|   |   |                        |
|---|---|------------------------|
|  | <b>NWC OT Cybersecurity System and Network Security Procedure</b> | <b>Page 23 of 24</b>   |
|   | <b>Document Type: Procedure</b>                                   | <b>August 16, 2021</b> |
|   | <b>Document Classification: Internal and Confidential</b>         |                        |



#### PROPRIETARY NOTICE

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

|   |   |                        |
|---|---|------------------------|
|  | <b>NWC OT Cybersecurity System and Network Security Procedure</b> | <b>Page 24 of 24</b>   |
|   | <b>Document Type: Procedure</b>                                   | <b>August 16, 2021</b> |
|   | <b>Document Classification: Internal and Confidential</b>         |                        |



## PROPRIETARY NOTICE

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