NWC OT Cybersecurity Access Control Management Procedure

Document Number:	A010045-PRO-AC
Issue Date:	June 22,2021
Revision Number:	00
Issued For:	Review

Revision Details

Name	Title/Dept.	Signature	Date
Prepared by:			
Sidrat Mehreen	Senior OT cybersecurity Analyst		June 18,2021
Reviewed by:			
Sameen Ullah Khan	OT Cybersecurity Lead		June 20,2021
Approved by:			
Farhan Rasheed	Operations Manager		June 20,2021

Issued by:			
Syed Ali Raza	Planning Engineer		June 22,2021

PROPRIETARY NOTICE

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

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						

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
Access Control	
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.
Change	The addition, modification, or removal of anything that could influence operations.
Change Management	The Process is responsible for controlling the lifecycle of all Changes. The primary objective of Change Management is to enable beneficial Changes to be made, with minimum disruption to OT process.
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.
Review and approval	The process steps are taken to ensure that policies and procedures are complied. The approval is the evidence that the review has been completed to satisfaction of the appropriate person e.g., CEO / Executive Committee / BOD.

1. Introduction

The purpose of this document is to establish a procedure for access control management. This procedure will ensure the process of following a standard procedure for all process complying with access and authentication in NWC.

2. Roles and Responsibilities

Roles	Responsibilities
OT Asset Owner	OT Asset Owner shall have the following responsibilities, but not limited to, • Initiate the request • Fill in the form • Make sure the business justification for privileged rights has been already discussed with the immediate Line Manager
OT Admin	OT Admin shall have the following responsibilities, but not limited to, • Review the request • Make sure the request is implemented • Maintain, update User Inventory List • Generate compliance report for users
Line Manager	Line Manger shall have the following responsibilities: • Check for completeness of the form submitted by OT Asset Owner • Initiate the request procedure to the Change Manager for further approval • Verifying and documenting the outcome of the requests
OT Cybersecurity Officer	OT Cybersecurity Officer shall: • Review final approval after change manager approval • Oversee the policies and procedures are complied

3. Access Control Procedures

3.1 Workstations Access Control Procedures

3.1.1 New User Creation

1. User initiate the request for new user creation by filling in the fields mentioned in User creation form attached in Appendix A:
    a. First, Middle, and Last name of the employee (correct spelling is crucial)
    b. Designation of employee
    c. Line Manager or Unit head
    d. Department of the user
    e. Primary Business unit and site of the employee
    f. User roles
    g. Office location
    h. Computer or Server need to be accessed
    i. Company email
    j. Account expiry date or account active duration
2. Upon receiving request, Line manager initiates the approval for the user creation and get an approval from the change manager for the new user on basis of:
    a. User must be created on the basis of least privileged rights.
    b. User must not assign default groups.
3. After approval, the request is evaluated by OT Cybersecurity Manager.
4. OT Admin creates a user account as per approved request.
5. OT Admin will update the user inventory list.
6. The user will then be notified of the outcome of their request.

3.1.2 Privileged Rights User request

By default, all NWC owned systems are granted "User" access level on their workstations. NWC provides local computer administrator access on requested basis only, on a valid business justification.

Business justification includes:

- Program installation and system reconfiguration, not for program use, unless it is otherwise impossible to operate the program.

1. User completes the Administrative Privilege Request form attached in Appendix A.

2. Request is submitted to Line Manager which is then forwarded to Change Manager.
3. After approval, the request is evaluated by OT Cybersecurity Manager.
4. After final evaluation, OT Admin assigns the Administrative Privileges.
5. OT Admin will update the user inventory list.
6. The user will then be notified of the outcome of their request.

3.1.3 User Deletion/Change

1. Line Manager initiates the request for deletion or changes in the user account created. The request made must have one of the following codes:
    a. Username
    b. Reason for revoke of permission
    c. User deletion
    d. User location change
2. OT Admin approves and updates the request and inventory sheet accordingly.

3.1.4 Process

Activities		Description
1.1	Request for User Creation/deletion	OT Asset Owner initiates the request by submitting the user creation/deletion/change form to the Line Manager.
1.2	Approval from Change Manager	Line Manager gets a formal approval from Change Manager complying to Change Management Procedure.
1.3	Evaluation of Request	After approval from Change Manager, OT Cybersecurity Manager reviews and evaluates the formal request.
1.4	Approval of Request	Approval is communicated to OT Admin to complete the process and create/delete/change the user as per approved request i.e., user, privileged user access.
1.5	Close and document the request	OT Admin will close the request by updating the user inventory list maintained and documented.

3.2 Field Devices Access Control Procedures

OT Asset Owner initiates the request for a user ID. Line Manager from SCADA O &M Team approves the request after analyzing the need. Once approved, OT Admin create the user id for OT Asset Owner. OT Admin is also responsible for maintaining and updating user inventory list (logs are maintained in SCADA server).

3.2.1 Process

Activities		Description
1.1	Request for User Creation	OT Asset Owner initiates the request by submitting the user creation/deletion form to the Line Manager
1.2	Approval from team Manager	Line Manager from SCADA O&M approves the request after analyzing the need.
1.3	Approval of Request	Approval is communicated to OT Admin to complete the process and user id for OT Asset Owner is created by OT admin.
1.4	Close and document the request	OT Admin will close the request by updating the user inventory list maintained and documented.

3.3 Physical Access Control Procedures

Depending on the location, there are three types of physical access that can be provided to user:

- Cards Scanner
- Written permits
- Biometrics

OT Asset Owner initiates the request for physical access. Depending upon the type of location, Corporate Support Services Department approves the request. Corporate Support Services Department is also responsible for providing access to the location.

Log repository for cards/biometric is maintained automatically by srever while for locks, keys and written permits, manual logbooks are maintained.

3.3.1 Process

Activities		Description
1.1	Request for User Creation	OT Asset Owner initiates the request by submitting the user creation/deletion form to the Line Manager
1.2	Approval from team Manager	Corporate Support Services Department approves the request after analyzing the need.
1.3	Approval of Request	Corporate Support Services Department will provide the access credentials to the user after approving request.
1.4	Close and document the request	Corporate Support Services Department will close the request by updating the user inventory list maintained and documented.

3.4 Access Control Procedure for third party

Depending on the system (windows, field devices, physical access, or network devices), respective team will initiate the request for access. OT Admin is responsible for providing the user access for third party.

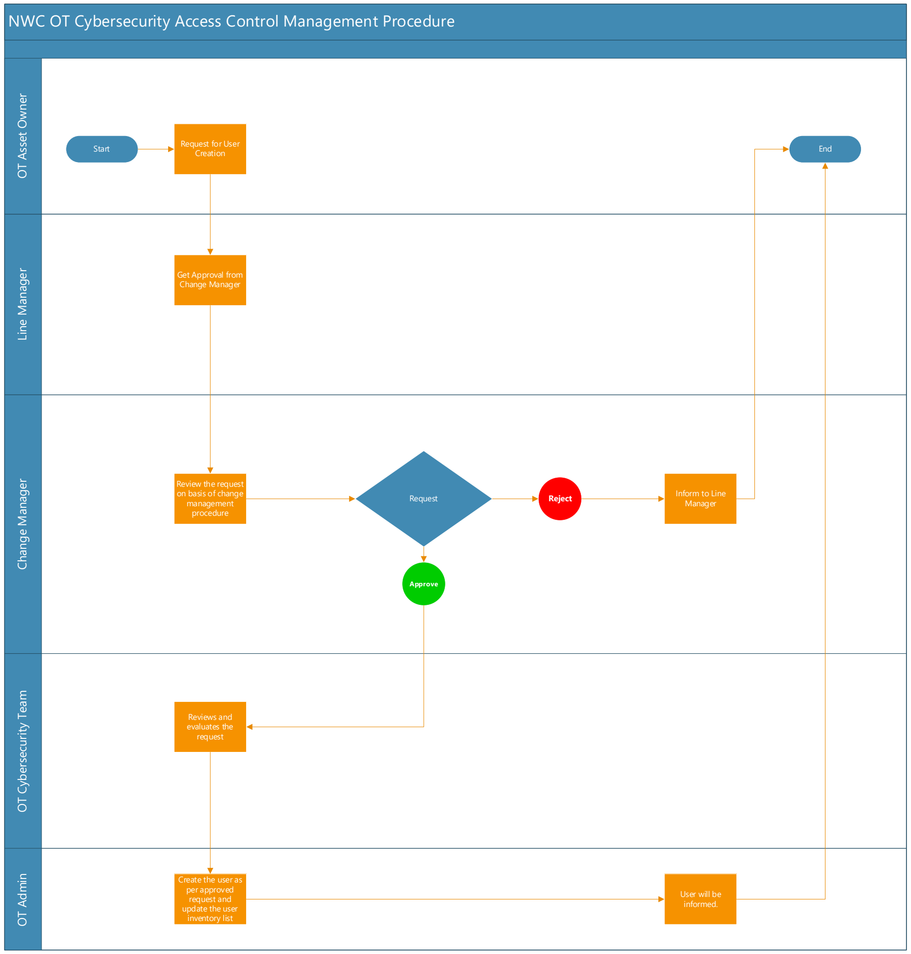
3.4.1 Process

Activities		Description
1.1	Request for User Creation	Respective Department initiates the request for user id creation.
1.2	Approval from team Manager	OT Admin approves the request after analyzing the need.
1.4	Close and document the request	OT Admin will close the request by updating the user inventory list maintained and documented.

4. Compliance Criteria

1. Access Management Compliance shall be done using User Inventory list.
2. OT Admin will generate and review compliance reports at least monthly from the user inventory list and logs for users created, deleted or changed.
3. In reviewing the reports, OT Admin will identify unnecessary user accounts and their privileges and notify to the respective Line Manager if found any exception.
4. OT Cybersecurity Manager will review the generated reports on quarterly basis.

5. Process Flowchart


NWC OT Cybersecurity Access Control Management Procedure
OT Asset Owner
Line Manager
Change Manager
OT Cybersecurity Team
OT Admin
Start
Request for User Creation
End
Get Approval from Change Manager
Review the request on basis of change management procedure
Request
Reject
Inform to Line Manager
Approve
Reviews and evaluates the request
Create the user as per approved request and update the user inventory list
User will be informed.

Appendix A

User Request Form

User Request Details								
Date of Request					**Request ID:**			
Access Requested	Production □	Development □	Test □	Training □	**Action Requested**	New User □	Add Role □	Change Role □
Requester Name:						Deactivate User □	Restore User □	
Department:					**Requester Signature:**			
Line Manager Name, Signature and Date:								

Select the Appropriate Role:	Line Manager □	Supervisor □	OT Admin □	Maintenance Engineer □	Testing Engineer □	User □
System Access Required:						
Date of Expiry:						

Change Management Approval			
Change Manager Signature, Date:			
Change Management Decision:	Approved □	Not Approved □	Required Changes □
Change Manager Comments:			

Final Approval or Rejection				
Request Status	□	Accepted	□	Rejected

Implementer Sign off:		**Date:**	