|  |  |
| --- | --- |
| **NWC OT Cybersecurity Incident Response Policy** | |
| **Document Number:** | A01001045-POL-IR |
| **Issue Date:** | 22-Aug-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 |  | August 22, 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. OT Incident Response 11](#_Toc80535093)

[1.1 Purpose 11](#_Toc80535094)

[1.2 Scope and Applicability 11](#_Toc80535095)

[1.3 Guidance 11](#_Toc80535096)

[1.4 Terminology 11](#_Toc80535097)

[1.5 Policy 11](#_Toc80535098)

[Compliance 13](#_Toc80535099)

[Exception Criteria 13](#_Toc80535100)

**Glossary**

| **Word or Phrase** | **Explanation** |
| --- | --- |
| **Access** | Ability to make use of any information system resource. |
| **Application** | A software program hosted by an information 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. |
| **Asset Register** | A list of all information assets, which includes their ownership, location, description, name, and value. |
| **Asset Owner** | A person or group of people who have been identified by management as having responsibility for the maintenance of the confidentiality, availability, and integrity of that asset. The asset owner may change during the lifecycle of the asset. |
| **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. |
| **Availability** | Ensuring timely and reliable Access to and use of information. |
| **Backup** | Copying data to protect against Loss of Integrity or Availability of the original. |
| **Business Continuity Plan (BCP)** | A Plan defining the steps required to Restore Business Processes following a disruption. The Plan will also identify the triggers for Invocation, people to be involved, communications, etc. |
| **Change** | The addition, modification, or removal of anything that could have an effect on 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. |
| **Confidentiality** | The property that information is not made available or disclosed to unauthorized individuals, entities, or processes. |
| **Cryptography** | The art of protecting information by transforming it (encrypting it) into an unreadable format. |
| **End point protection** | Safeguards implemented through software to protect end-user machines such as workstations and laptops against attack (e.g., antivirus, antispyware, anti-adware, personal firewalls, host-based intrusion detection and prevention systems, etc.). |
| **Encryption** | The translation of data into a secret code. Encryption is the most effective way to achieve data security. |
| **Immediate Line Manager** | An individual responsible for network resources (people, data, processing capability) who is charged with conducting business of an organization. |
| **Incident** | Vulnerability and threat together result in an incident. An information security incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security. |
| **Integrity** | The property of safeguarding the accuracy and completeness of assets. |
| **Network** | A network is a group of two or more computer systems linked together. |
| **Owner** | The organization unit department/activity/ business unit which has its own policies and procedure and is responsible for its development and implementation.  The owner will be the head of the department/area/activity/business unit that is responsible for developing and implementing the policy or procedure. |
| **Patch** | A fix to a program that eliminates a vulnerability exploited by malicious hackers. See vulnerability and patch. |
| **Perimeter** | The continuous line forming the boundary of a closed geometrical figure. |
| **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** | Is 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. |
| **Risk** | The possibility of suffering harm or Loss. In quantitative Risk Management, this is calculated as how likely it is that a specific Threat will exploit a particular vulnerability.  A combination of the probability of an event and its consequence. |
| **Risk Analysis** | The systematic use of information to identify sources and to estimate risk. |
| **Risk Assessment** | The overall process of risk analysis and risk evaluation. |
| **Risk Management** | The Process is responsible for identifying, assessing and managing Risks. Risk Management can be quantitative (based on numerical data) or qualitative. |
| **Incident Response Team** | An ad-hoc team created to handle a security incident. |
| **Supplier** | A Third Party responsible for supplying goods or services that are required to deliver IT/OT services. Examples of suppliers include commodity hardware and software vendors, network and telecom providers, and outsourcing Organizations. |
| **Threat** | A threat is anything that might exploit Vulnerability. Any potential cause of an Incident can be considered to be a Threat. For example, a fire is a threat that could exploit the Vulnerability of flammable floor coverings. This term is commonly used in Information Security Management and IT/OT Service Continuity Management but also applies to other areas such as Problem and Availability Management.  A potential to cause an unwanted incident which may result in harm to a system. |
| **Test Environment** | A controlled Environment used to test Configuration Items, Software Builds, OT/IT Services, Processes, etc. |
| **Virus** | A program that enters a computer usually without the knowledge of the operator. Some viruses are mild and only cause messages to appear on the screen, but others are destructive and can wipe out the computer's memory or cause more severe damage |

# OT Incident Response

## Purpose

This document outlines Incident Response Security Policy in the Operational Technology (OT) environment of National Water Company (NWC). Although there is a convergence between Operation Technology and Information Technology, the standard practices of Information Technology (IT) are not directly applicable to OT, as OT generally requires stricter access control of external information. 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 access control specifically focused on NWC OT Environment.

## Scope and Applicability

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

This Policy applies to all NWC BU/Departments that use or have Access to NWC OT systems, devices, applications, and 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 document shall be developed and maintained for OT Incident response plan and implemented in response to Incidents.*
2. *Appropriate responsibilities and procedures shall be established to ensure an effective response against incidents or events.*
3. *A formal reporting procedure for incident shall be established.*
4. *Depending on Incident Criticality, Incident Response Committee shall form Incident Response Team comprising of subject Matter Experts for incident handling & remediation actions.*
5. *Exercising the incident recovery plan periodically*
6. *Incident Recovery Plan shall be prepared, documented, updated, and reviewed periodically.*
7. *Incident Recovery plan shall be reviewed regularly using business impact and risk assessment methodologies.*
8. *Incident Recovery Plans shall be updated with relevant changes, managed through the change management process.*

# 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 Incident Response. 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.*