
	NWC OT Cybersecurity Backup and Recovery Procedure	Page 1 of 17
	Document Type: Procedure	August 16, 2021
	Document Classification: Internal and Confidential	

NWC OT Cybersecurity Backup and Recovery Procedure	
Document Number:	A01001045-PRO-BKREC
Issue Date:	August 16, 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 Backup and Recovery Procedure	Page 2 of 17
	Document Type: Procedure	August 16, 2021
	Document Classification: Internal and Confidential	

Revision Details

Name	Title/Dept.	Signature	Date
Prepared by:			
Sidrat Mehreen	Senior OT Cybersecurity Analyst		August 03, 2021
Reviewed by:			
Sameen Ullah Khan	OT Cybersecurity Lead		August 05, 2021
Approved by:			
Farhan Rasheed	Operations Manager		August 09, 2021
Issued by:			
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.


	NWC OT Cybersecurity Backup and Recovery Procedure	Page 3 of 17
	Document Type: Procedure	August 16, 2021
	Document Classification: Internal and 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 Backup and Recovery Procedure	Page 4 of 17
	Document Type: Procedure	August 16, 2021
	Document Classification: Internal and 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 Backup and Recovery Procedure	Page 5 of 17
	Document Type: Procedure	August 16, 2021
	Document Classification: Internal and Confidential	

Table of Contents

1. Introduction	7
2. Roles and Responsibilities.....	7
3. Backup Procedure	9
4. Backup Process	13
5. Recovery Process	14
6. Process Flow Chart.....	16

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 Backup and Recovery Procedure	Page 6 of 17
	Document Type: Procedure	August 16, 2021
	Document Classification: Internal and Confidential	

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.
Backup	Copying data to protect against loss of Integrity or Availability of the original.
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.

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 Backup and Recovery Procedure	Page 7 of 17
	Document Type: Procedure	August 16, 2021
	Document Classification: Internal and Confidential	

1. Introduction

This document provides the guidance and procedure on developing, implementing, and maintaining effective backup and recovery procedure through NWC OT Environment.

This procedure is prepared considering aspect of business continuity where secure file transfer is not available.

Backup and Recovery procedure of NWC OT Asset are subject to NWC OT cyber security policies including but not limited to Backup and Recovery Policy, Acceptable Use Policy, etc.


This procedure is applicable only NWC OT infrastructure.

2. Roles and Responsibilities

Roles	NWC Representative	Responsibilities
Request Initiator	SCADA O&M Application Team Smart Operation Network Team Infrastructure Team Endpoint Support Team	Initiates the request for backup of OT Asset
Request Approver	Application Team Smart Operation Network Team Infrastructure Team Information Security Endpoint Support Team Backup Administrator	Requester's Line manager, Information Security and Backup Administrator evaluates and provides approval or rejection based on Business Continuity Plan/Disaster Recovery Plan.

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 Backup and Recovery Procedure	Page 8 of 17
	Document Type: Procedure	August 16, 2021
	Document Classification: Internal and Confidential	

Roles	NWC Representative	Responsibilities
Backup Administrator	Infrastructure Team	Designated person responsible for Backup Solution, its storage and Access and use for recovery.
Backup Operator	OT Users OT Asset Owner Authorized Contractor	Assigned person to perform Backup Operation e.g. Smart Operations Engineer or Authorized Contractor for PLCs/RTUs/Data Logger/Data Concentrator & etc. Backups, Network Engineer for Routers/Switches/Firewalls/Radios backups Infrastructure & Endpoint Engineer for servers and workstations System Image SCADA Engineer for SCADA Application backups Special Apps Engineer for 3 rd Party Applications backups (such as AD, McAfee, WSUS, Veritas BackupExec, SFT & etc.)
Incident Response Team	OT Users OT Asset Owner Authorized Contractor	Assigned person(s) to perform recovery activities to restore OT Asset functionality e.g. Smart Operation Engineer or Authorized Contractor for PLCs/RTUs/Data Loggers/Data Concentrators recovery.

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 Backup and Recovery Procedure	Page 9 of 17
	Document Type: Procedure	August 16, 2021
	Document Classification: Internal and Confidential	

Roles	NWC Representative	Responsibilities
		<p>Network Engineer for Routers/Switches/Firewalls/Radios recovery</p> <p>Infrastructure & Endpoint Engineer for servers and workstations image restore</p> <p>SCADA Engineer for SCADA Application Installation, Configuration and Re-Deployment</p> <p>Special Apps Engineer for 3rd Party Application restore (such as AD, McAfee, WSUS, Veritas BackupExec, SFT & etc.)</p>


3. Backup Procedure

Guidance Notes:

1. All backups and recoveries actions shall be documented and tracked.
2. Disaster Recovery plan shall define the data backup strategy identifying the systems to backup, files to backup, the storage media, the locations of the storage and the storage retention, and these shall be the input for backup and recovery process.
3. NWC shall evaluate (along with all relevant stakeholders) & determine criticality of OT Asset and assign backup and recovery strategy to minimize operational impact due to OT Asset unavailability.
4. NWC shall consider the technologies such as redundant arrays of independent disks (RAID), automatic failover, UPS, server clustering, and mirrored systems along with Backup and Recovery when developing an OT recovery strategy.
5. NWC OT Asset shall be backed up regularly and shall specify the minimum frequency and scope of backups (e.g., Quarterly or Annually, incremental or full) based on OT Asset and data criticality and the frequency of OT Asset data changes.
6. NWC shall maintain minimum 2 versions (n and n-1) (to be set for each OT Asset type based on criticality) of system/image full backups of OT Assets which are within 6 months old (to be set for each OT Asset type), and these backups shall be stored in on-premises and off-

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 Backup and Recovery Procedure	Page 10 of 17
	Document Type: Procedure	August 16, 2021
	Document Classification: Internal and Confidential	

premises either on networked storage devices or secure portable storage devices based on critically of backup availability.

7. Network Device's and SCADA System's projects and configuration backups shall be collected during each change or every 6 month and stored in on-premises and off-premises either on networked storage devices or secure portable storage devices based on critically of backup availability and all backups shall be encrypted to avoid unauthorized access and use.
8. NWC shall consider System-level and User-level information of all the critical OT Assets while developing backup strategy. System-level information includes system state information, operating system software, middleware/drivers, application software and configuration, logs, and licenses of Windows nodes, Network devices and virtualization nodes, etc. User-level information includes information other than system-level information.
9. NWC shall collect system and data backups by centralized Tiered backup solution based on backup schedule of OT Asset while they are online and normal operation. The backups must be verified for correctness using the backup & recovery software verification tool.
10. Three common methods for performing system backups. Combination of backup operations shall be used depending on system configuration and recovery requirements. Full back up shall be taken weekly and Incremental / differential backups on each evening.
 - Full back up
 - Captures all files on the disk or within the folder selected for backup.
 - All the backed-up files are recorded to a single media or media set, locating a file or group of files is simple during recovery.
 - Time required to perform a full backup is lengthy.
 - Multiple iterations of full backups that do not change frequently could lead to excessive, unnecessary media storage requirements.
 - Incremental backup
 - Captures files that were created or changed since the last backup, regardless of backup type.
 - more efficient use of storage media, and backup times are reduced.
 - media from different backup operations are required to recover a system.
 - Differential backup
 - Capture files that were created or modified since the last full backup.
 - takes less time to complete than a full backup.

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 Backup and Recovery Procedure	Page 11 of 17
	Document Type: Procedure	August 16, 2021
	Document Classification: Internal and Confidential	

- take longer to complete than incremental backups because the amount of data since the last full backup increases each day until the next full backup is executed.
 - only the full backup media and the last differential media would be needed to recover.
11. NWC shall designate the location of stored data, file-naming conventions, media rotation frequency, and method for transporting data offsite.
 12. Backups shall be stored in electronic vaulting, network attached storage (NAS) or storage area network (SAN) and tape library systems or secure portable storage devices based on system and data availability, and integrity requirements.
 13. NWC shall store one copy of backed-up data at off-premises location. Backup data storage facilities shall be specially designed to archive media and protect data from threatening elements. Data is backed up at the NWC facility and then labeled, packed, and transported to the off-premises storage facility. Only specific backup data shall be transported from off-premises storage to NWC facility in case of recovery or testing purposes.
 14. NWC shall consider the following criteria while selecting an offsite storage facility,
 - Geographic area: distance from NWC off-premises backup storage site and the probability of the storage site being affected by the same disaster as the NWC site.
 - Accessibility: length of time necessary to retrieve the data from off-premises backup storage site and the storage facility's operating hours.
 - Security: security capabilities of the shipping method, storage facility, and personnel. All must meet the data's security requirements.
 - Environment: structural and environmental conditions of the storage facility (i.e., temperature, humidity, fire prevention, and power management controls).
 15. NWC shall implement redundancy and fault tolerance processes to store data on more than one drive and eliminate loss of data from single drive failures.
 16. Backups shall be encrypted and protected in both on-premises and off-premises from unauthorized access or use.
 17. NWC shall consider the following factors when choosing the appropriate backup solution
 - Equipment interoperability
 - To facilitate recovery, the backup device must be compatible with the platform operating system and applications and should be easy to install onto different models or types of systems.
 - Storage volume

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 Backup and Recovery Procedure	Page 12 of 17
	Document Type: Procedure	August 16, 2021
	Document Classification: Internal and Confidential	

- To ensure adequate storage, the amount of data to be backed up should determine the appropriate backup solution.
 - Media life
 - Each type of medium has a different use and storage life beyond which the media cannot be relied on for effective data recovery.
 - Backup Software
 - When choosing the appropriate backup solution, the software or method used to back up data should be considered.
 - the backup solution can be as simple as a file copy using the operating system file manager.
 - In case of image backups and larger data transfers, a third-party application shall be implemented to automate and schedule the file backup.
 - Third party application used for image backups and larger data transfers shall be evaluated for performance impact over low throughput networks.
- 18. Backups shall be validated regularly using backup and recovery software, and sample OT Asset image backup and latest data backups shall be tested by restoring them in a test environment to ensure reliable and quick restoration in case of service disruption.


Following steps shall be taken to perform backup of NWC OT Asset:

1. OT Asset Owner shall initiate Backup Request for OT Asset as per Backup Strategy or Disaster Recovery Plan, Backup Request shall minimum contain following:
 - a. OT Asset Details
 - b. Scheduled or On-Demand backup request
 - c. Pre-Approved Backup Method Statement (if any available)
2. Backup Operator shall prepare & submit backup method statement for specific OT Asset for approval.
3. OT Asset Owner, Information Security and Backup Admin shall evaluate and approve backup method statement for the OT Asset.
4. Backup Operator will perform OT Asset Backup.
5. Backup Operator will store OT Asset Backup at pre-defined location.
6. Backup Operator will update backup collection record and notify OT Asset Owner.

Following steps shall be taken to perform recovery of NWC OT Asset (in case of disaster recovery):

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 Backup and Recovery Procedure	Page 13 of 17
	Document Type: Procedure	August 16, 2021
	Document Classification: Internal and Confidential	


1. OT Asset Owner will initiate incident request for Recovery of an OT Asset. Request shall minimum contain following:
 - a. OT Asset Details
 - b. Nature of failure
 - c. OT Asset Backups Details
2. Incident Response Committee will evaluate Incident Request and will deploy incident response team (comprising of Network, Smart Operations, SCADA O&M Application, Infrastructure Team, Endpoint Support & etc.)
3. Incident Response Team will prepare, test & submit recovery method statement for approval.
4. Backup Administrator, Information Security and OT Asset Owner will evaluate and approve recovery method statement. It may include following, but not limited to it:
 - a. Recovery of system state image (online & offline)
 - b. Recovery of configuration (online & offline)
 - c. Clean installation and configuration
5. Backup Administrator will authorize collection of Backup from off-site or on-site storage location either via network or secure portable storage device.
6. Incident Response Team will execute recovery operation.
7. Incident Response Team will notify of successful OT Asset function restore.
8. Incident Response Team will submit IR Report to Information Security for analysis and record keeping.

4. Backup Process

Activity		Responsible	Description
1.1	Initiate Backup Request	OT Asset Owner	
1.2	Prepare & Submit Backup Method Statement	Backup Operator	Backup Operator prepares OT Asset Backup method statement based on vendor recommendations and submits along with Backup Request for approval

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 Backup and Recovery Procedure	Page 14 of 17
	Document Type: Procedure	August 16, 2021
	Document Classification: Internal and Confidential	


1.3	Backup method statement evaluation & approval	OT Asset Owner Backup Administrator Information Security	Backup method statement for OT Asset is evaluated and either approved or rejected.
1.4	Backup Operation	Backup Operator	Backup Operator will arrange all necessary tools (as per approved method statement) to perform backup operations on OT Asset as per Backup Request. Backup Operator will notify backup status.
1.5	Backup Storage	Backup Operator	Backup Operator will store OT Asset Backup at predefined location and will notify OT Asset Owner and Backup Administrator
1.6	Backup Request Closing	Backup Operator	Backup Operator will close backup request and notify request initiator.

5. Recovery Process

Activity		Responsible	Description
1.1	Initiate Recovery of OT Asset Incident Request	OT Asset Owner	
1.2	IR Evaluation and formation of Incident Response Team (IR)	Incident Response Committee (IRC)	IRC Team will evaluate OT Asset Incident and accordingly form incident response team.
1.3	Recovery Method Statement Preparation	IR Team	IR Team will prepare and submit Recovery Method Statement for approval.

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 Backup and Recovery Procedure	Page 15 of 17
	Document Type: Procedure	August 16, 2021
	Document Classification: Internal and Confidential	

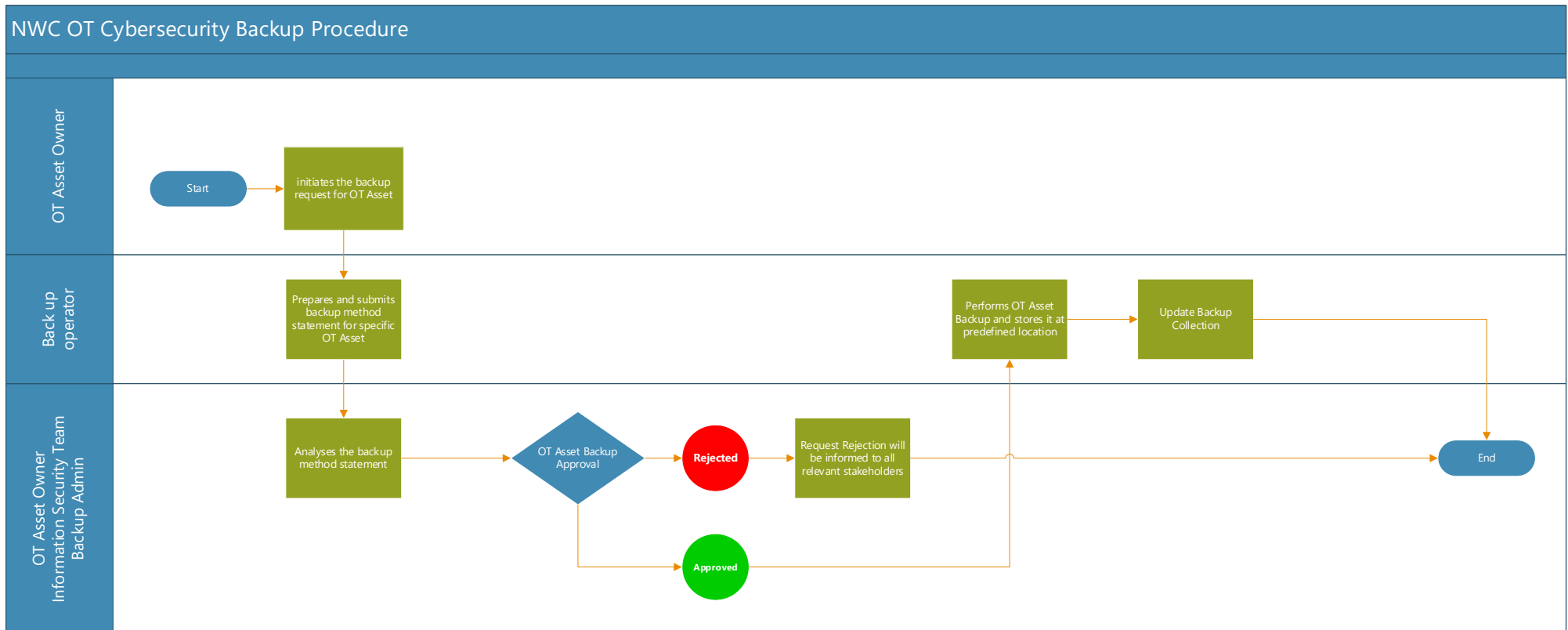
1.4	Recovery Method Statement Approval	IRC Information Security OT Asset Owner	Recovery Method Statement will be evaluated and approved.
1.5	Collection of OT Asset Backup	IR Team	IR Team will get approval from Backup Administrator to collect OT Asset Backup for recovery.
1.6	Recovery Operation	IR Team	IR Team will arrange all necessary tools (as per approved method statement) to perform recovery operations on OT Asset as per OT Incident Request. IR Team will notify recovery status.
1.7	Recovery Request Closeout	IR Team	IR Team will prepare and submit Recovery Report

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 Removable Media Procedure	Page 16 of 17
	Document Type: Procedure	August 09, 2021
	Document Classification: Internal and Confidential	

6. Process Flow Chart

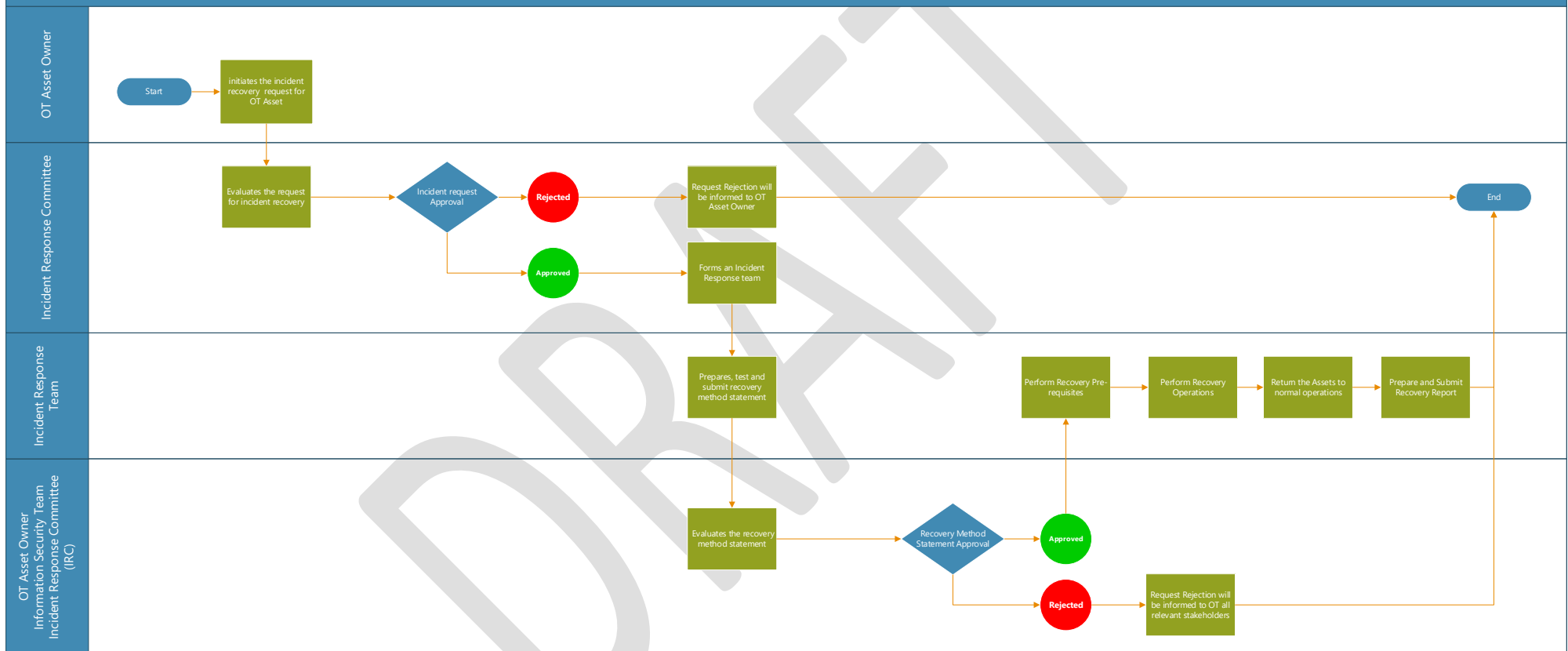


PROPRIETARY NOTICE

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

	NWC OT Cybersecurity Backup and Recovery Procedure	Page 17 of 17
	Document Type: Procedure	August 16, 2021
	Document Classification: Internal and Confidential	

NWC OT Cybersecurity Recovery 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.