


Information Security Incident Management Procedure

Ncell

Procedure

Approved Date:- 13/12/2019

	Ncell	Classification: Internal
	Information Security Incident Management Procedure	Owner: CIO/Head of IT
		Effective Date: 05-10-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

Procedure Name DOCID: PR-IT-IS-13


Copyright © Ncell. All rights reserved.

No part of this document may be reproduced or transferred in any form or by any means without prior permission in writing from Ncell.

These trademarks are the intellectual property of Ncell and are protected by applicable legislation.

All other products or company names are used for reference only and may be proprietary to their respective hold

Document Control

	Ncell	Classification: Internal
	Information Security Incident Management Procedure	Owner: CIO/Head of IT
		Effective Date: 05-10-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

i. Document Identification

Document Title and Version:	PR-IT-IS-13 Information Security Incident Management Procedure
Effective Date:	05-10-2019
Document Author:	Information Security Team
Owner:	CIO/Head of IT

ii. Distribution List

All Ncell Employees
Relevant External Parties and Auditor's (If Required)

iii. Document Roles and Responsibilities


Responsible	Information Security Team
Accountable	CIO/Head of IT
Consulted	Function Heads
Informed	All Employees and External Parties

iv. Digital Signature

CEO

CIO/Head Of IT

v. Revision History

	Ncell	Classification: Internal
	Information Security Incident Management Procedure	Owner: CIO/Head of IT
		Effective Date: 05-10-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

Rev	Date	Author	Description	Approved By	Date
0	05-10-2019	Information Security Team	Initial document	Vishal Mani Upadhyay	13-12-2019
1	13-12-2019	Information Security Team	Approval	Andy Chong	17-12-2019
2	22-10-2021	Information Security Team	Reviewed with no change	Vishal Mani Upadhyay	19-12-2021
3	19-12-2021	Tarani Prasad Chaudhary	Review-Formatting	Andy Chong	20-12-2019
4	28-09-2023	Information Security Team	Review and Updating – Period changed from annual to once every two years. Added Head of IT	Rajesh Lal Nyachhyon	27-12-2023
5	27-12-2023	Tarani Prasad Chaudhary	Minor Formatting Approval	Rajesh Lal Nyachhyon Jabbor Kayumov	27-12-2023
6	5-24-2024	Information Security	Re-branding	CIO/Head of IT	



	Ncell	Classification: Internal
	Information Security Incident Management Procedure	Owner: CIO/Head of IT
		Effective Date: 05-10-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

Table of Contents

Document Control	1
1. Purpose	5
2. Review and Updating	5
3. Scope	5
4. Roles and Responsibilities	5
5. Incident Response Team	5
5.1 Incident Management Leader (IML).....	5
5.2 Incident Coordinator (IC):.....	5
5.3 Incident Manager (IM):.....	6
5.4 Resolver Group:.....	6
5.5 IT Support Team:	6
6. Incident Categorization	7
7. Incident Prioritization	8
7.1 Resolution Time.....	8
7.2 Classification.....	8
8. Security Incident Management Lifecycle	10
8.1 Overview	10
8.2 Incident Preparation	10
8.3 Incident Identification.....	10
8.3.1 Information Security Incident Detection	10
8.3.2 Reporting a Suspected Incident	10
8.3.3 Initial Response	11
8.3.4 Categorizing and Prioritizing Incidents	11
8.3.5 Additional Requirements for Specific Classes of Compromised Data	11
8.4 Incident Containment	11
8.4.1 Overview of Incident Containment.....	11
8.4.2 Overview of Incident Containment.....	12
8.5 Incident Eradication.....	12
8.5.1 Guidelines for Incident Eradication	12
8.6 Incident Recovery	12
8.6.1 Selection Requirements for System Recovery	13
8.6.2 Guidelines for Incident Recovery	13
8.7 Closure and RCA	14
8.7.1 Root Cause Analysis Mechanism	14
9. Forensic Investigation	15
10. Escalation Matrix	16
11. Governance and Compliance	16
12. Associated Documents	16

	Ncell	Classification: Internal
	Information Security Incident Management Procedure	Owner: CIO/Head of IT
		Effective Date: 05-10-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

1. Purpose

This policy provides a framework for reporting and managing:

- security incidents affecting Ncell's information and information systems
- loss, disclosure, or corruption of information or devices
- near misses and information security concerns

2. Review and Updating

This procedure shall be reviewed once every two years or whenever significant changes occur in the organization.

3. Scope

This document is applicable to all Ncell applications and supporting infrastructure.

4. Roles and Responsibilities

- Global Security Operations Centre:** The GSOC shall monitor logs for the integrated devices for anomalies. It shall perform an initial analysis to determine the category and priority of the incident. GSOC shall notify Ncell of all detected security incidents.
- Information Security Team:** The Information Security Team shall analyse the events triggered in the Data Loss Prevention Solution. After first level analysis, if the event is found to be an incident, then the Information Security team will log an information security incident in the ticketing tool. The Information Security team shall also assist in analysing and resolving the incident where required.
- Unit Heads:** Unit Heads shall analyse and resolve the incident tickets assigned to them within the assigned SLAs.
- Employees:** Employees shall report any identified information security by raising an information security incident in the ticketing tool with Incident type as an 'Internal Security Incident.'
- NOC/Surveillance Team:** The NOC/Surveillance team shall log a ticket as per the information received from GSOC and assign it to the concerned stakeholder for resolution.

5. Incident Response Team


The Incident Response Team (IRT) is formed to address any incidents and initiate immediate action to resolve the same. The Incident Response Team defines procedures to proactively address potential threats/risks arising out of incidents. Such teams are formed ad hoc; and are based on the severity and impact of the incidents. But most incidents are to be handled at the Incident Manager level. The team should consist of the following members:

5.1 Incident Management Leader (IML)

- The Head of IT is the IML and should be responsible for overall management of the high severity incidents.
- The IML is responsible for taking critical decisions regarding business operations/process changes during/after an incident. The IML or a person designated by him only can deal with the media/external stakeholders in case of any incidents.

5.2 Incident Coordinator (IC):

- IC is responsible for coordinating with the other Department heads to manage and resolve the incident. He should try and obtain as much information as possible from the person reporting the incident.
- IC should identify the technology/business areas affected by the incident and perform a detailed impact analysis.
- The IC should work with the Resolver Group to contain the damage caused by the incident and

	Ncell	Classification: Internal
	Information Security Incident Management Procedure	Owner: CIO/Head of IT
		Effective Date: 05-10-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

should be the focal point for recovery efforts.

- iv. IC should delegate action on incidents to relevant personnel such as Information Security Committee (ISC) in discussion with Incident Manager.
- v. Wherever needed, he/she must also meet the person reporting the incident for obtaining further information.

5.3 Incident Manager (IM):


- i. The Information Security and Privacy Officer should be IM for all information security incidents
- ii. The IM should be the 'one-point contact' for all the users for all incidents. IM is responsible for complete ownership of Critical Incidents and their coordination and resolution.

5.4 Resolver Group:

- i. The resolver group in co-ordination with the Incident Response Team is responsible for the resolution of the security event or security incident and restore the normal operations quickly and efficiently

5.5 IT Support Team:

- i. Answering, evaluating, and prioritizing the incoming telephone, e-mail, and in-person requests for assistance from users experiencing problems with hardware, software, networking, security and other computer-related technologies
- ii. Escalate problems to help desk support engineers
- iii. Escalate any security incidents/problem to information security team
- iv. Contact software and hardware vendors to request service regarding defective products
- v. Log and track calls and maintain history records/related problem documentations
- vi. Provide all logs related to the incident to the IRTL

	Ncell	Classification: Internal
	Information Security Incident Management Procedure	Owner: CIO/Head of IT
		Effective Date: 05-10-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

6. Incident Categorization

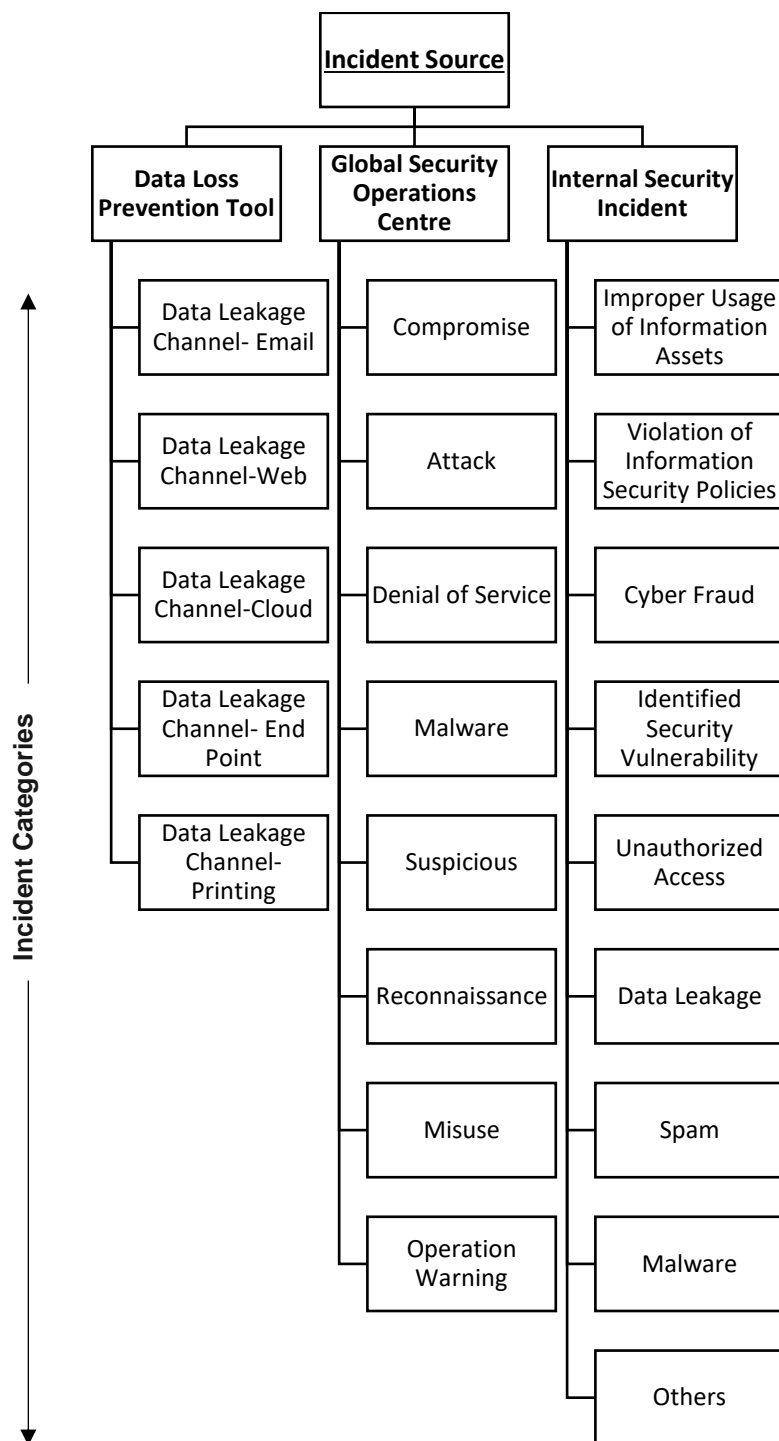



Figure 1. Categorization of Information Security Incidents

	Ncell	Classification: Internal
	Information Security Incident Management Procedure	Owner: CIO/Head of IT
		Effective Date: 05-10-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

7. Incident Prioritization

7.1 Resolution Time

Priority / Incident Type	Resolution Time		
	Data Loss Incident	Prevention Security Operations Incident	Internal Security Incident
P1 – Critical	8 hours	15 minutes	8 hours
P2 – High	12 hours	30 minutes	24 hours
P3 – Medium	48 hours	45 minutes	72 hours
P4 – Low	72 hours	45 minutes	10 working days

7.2 Classification

i. DLP incidents shall be prioritized based on the following criteria:

DLP Policy	0-2 Events	3-5 Events	6-10 Events	More than 10 Events
Subscriber Data – PII	High	High	High	Critical
Database files	High	High	High	Critical
Encrypted/Password Protected files	Low	Medium	High	Critical
Financial Information	Medium	Medium	High	Critical
Microsoft license Key	Low	Medium	High	Critical
Network Security Information	Medium	Medium	High	Critical


ii. GSOC incidents shall be prioritized by the GSOC team based on impact and severity. GSOC shall provide the priority of the incident.

iii. Internal security incidents shall be prioritized based on impact. Priority should be determined as follows:


- Insignificant or Minor: Low
- Moderate: Medium
- Major: High
- Catastrophic: Critical

The below guidelines can serve as an input in determining the impact of the security incident.

Impact	1-Insignificant	2-Minor	3-Moderate	4-Major	5-Catastrophic
Disruption to Service:					
Localised**	• < 1 hour	• 1 hour – 3 hours	• 3 hours – 10 hours	• 10 hours – 48 hours	• > 48 hours
Regional**	• 0 – 15 min	• 15 min – 1 hour	• 1 hour – 3 hours	• 3 hours – 10 hours	• > 10 hours
Nationwide**	• Nil	• 0 – 15 min	• 15 min – 1 hour	• 1 hour – 3 hours	• > 3 hours
Injuries	• Nil	• Minor injury • Minor treatment (first aid)	• Minor injury • Requires outpatient treatment	• Extensive bodily injuries / permanent disability • Hospitalisation required	• Extensive bodily injuries / permanent disability requiring hospitalisation • Death

	Ncell	Classification: Internal
	Information Security Incident Management Procedure	Owner: CIO/Head of IT
		Effective Date: 05-10-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

Financial*	<ul style="list-style-type: none"> • < 1% variance against targets / budget financial indicators 	<ul style="list-style-type: none"> • 1% < 5% variance against targets / budget financial indicators <p>or</p> <ul style="list-style-type: none"> • (222k to <22m) BDT 	<ul style="list-style-type: none"> • 5% < 10% variance against targets/budget financial indicators <p>or</p> <ul style="list-style-type: none"> • (>=22m to <111m) BDT 	<ul style="list-style-type: none"> • 10% < 15% variance against targets /budget financial indicators <p>or</p> <ul style="list-style-type: none"> • (>=111 m to <222 m) BDT 	<ul style="list-style-type: none"> • >= 15% variance against targets / budget financial indicators <p>or</p> <ul style="list-style-type: none"> • (>=222 m) BDT
Reputation	<ul style="list-style-type: none"> • Customer complaints generally restricted to hotline / emails 	<ul style="list-style-type: none"> • Customer complaints generally restricted to hotline / emails 	<ul style="list-style-type: none"> • Customer complaints include negative posts online (e.g. blogs, twitter, etc.) 	<ul style="list-style-type: none"> • Widespread negative publicity online (e.g. blogs, twitter, YouTube etc.) • Corporate image significantly affected 	<ul style="list-style-type: none"> • Widespread negative publicity online (e.g. blogs, twitter, YouTube etc.)
	<ul style="list-style-type: none"> • Estimated time to restore reputation: 1 week 	<ul style="list-style-type: none"> • Estimated time to restore reputation: 3 months 	<ul style="list-style-type: none"> • Estimated time to restore reputation: 1 year 	<ul style="list-style-type: none"> • Estimated time to restore reputation: 1 year < 3 years 	<ul style="list-style-type: none"> • Long-standing reputation damage • Criminal prosecutions • Political intervention
Media Attention	<ul style="list-style-type: none"> • None 	<ul style="list-style-type: none"> • Media enquires only 	<ul style="list-style-type: none"> • One-off newspaper article / radio / television / online mention 	<ul style="list-style-type: none"> • Sustained media attention for > 3 days 	<ul style="list-style-type: none"> • Sustained media attention for > 5 days
Legal and Regulatory	<ul style="list-style-type: none"> • Litigation or non-compliance issues that has no litigation consequences • Issuance of advice letter 	<ul style="list-style-type: none"> • Minor non compliances or breaches of contract, Act, regulations, consent conditions • Issuance of reprimand/ warning letter 	<ul style="list-style-type: none"> • Breach of regulatory or contractual obligations is widespread • Litigation and increased scrutiny from regulators. • Multiple issuance of reprimand/ warning letters 	<ul style="list-style-type: none"> • Major breach of contract, act, regulations or consent conditions • Expected to attract regulatory attention • Investigation, prosecution and / or possibility of action taken against specific member(s) of the senior management team. 	<ul style="list-style-type: none"> • Serious breach of contract or legislation • Potential for litigation including class actions • Future approvals / registration / licensing in jeopardy • Possibility of criminal action involving a felony against senior enterprise management or Ncell

	Ncell	Classification: Internal
	Information Security Incident Management Procedure	Owner: CIO/Head of IT
		Effective Date: 05-10-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

8. Security Incident Management Lifecycle

8.1 Overview

This section describes each serial phase of the Incident Management Lifecycle, as illustrated in Figure 1, and outlines the requirements for each phase. It also describes the three parallel processes that occur throughout the Incident Management Lifecycle.

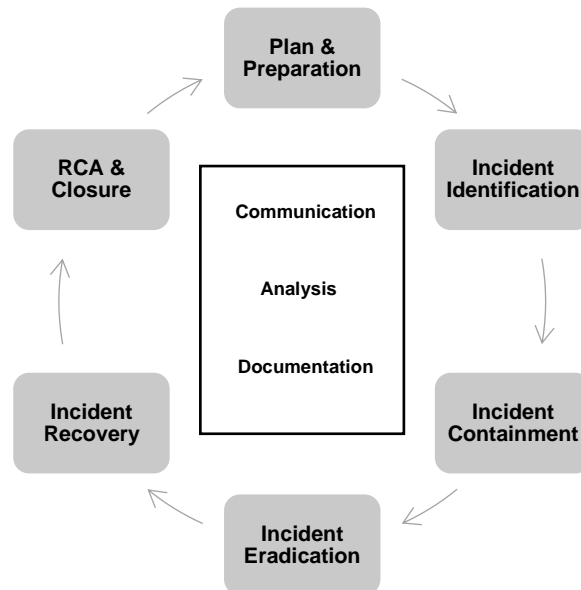


Figure 2. Security Incident Management Lifecycle

8.2 Incident Preparation

When the Information Security incident management process has not been activated, Ncell is in a state of preparation. Incident Preparation is characterized by several activities:

- Establishing, organizing, and maintaining Incident Response Teams.
- Acquiring and maintaining the necessary tools and resources for incident response activities.
- Keeping the Incident Response Team familiar with their environment through exercises like frequent log reviews to better identify unexplained entries.
- Keeping all clients, servers, and other device clocks synchronized to strengthen event correlation.
- Training users in recognizing and reporting IT security incidents

8.3 Incident Identification

8.3.1 Information Security Incident Detection


Information security incidents at Ncell can be detected and reported through one of the following channels:

- Notification from GSOC
- DLP tool notification
- Internal employee / third party

8.3.2 Reporting a Suspected Incident

A report of an Information Security incident is the signal that Incident Preparation activities must be suspended and that the traditional Incident Management process must begin. An Information Security Incident Report should contain all of the following information, if it is available at the time of the report, remaining information shall be reported as it becomes available:

- Submitter Name
- Submitter Phone Number
- Submitter Email Address

	Ncell	Classification: Internal
	Information Security Incident Management Procedure	Owner: CIO/Head of IT
		Effective Date: 05-10-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

- iv. Victim IP Address
- v. Victim Hostname / Domain Name
- vi. Victim Building and Room Number
- vii. Sensitivity and Description of Information Residing on Victim System (PII/non-PII)
- viii. Attacker IP Address
- ix. Attacker Country, City
- x. Attacker Hostname / Domain Name
- xi. Incident Summary
- xii. Date / Time Incident Occurred
- xiii. Date / Time Incident Discovered (when the user detected the problem)
- xiv. Exploit Used or IDS/Anti-Virus Alert
- xv. Incident Category
- xvi. Cost of Downtime
- xvii. User's Role with Ncell
- xviii. Systems or Networks the User Connected to Lately
- xix. Symptoms (if user noticed anything strange about the computer)
- xx. User Activity When Problem First Noticed
- xxi. User Location When Incident Occurred
- xxii. Detailed Description of Incident

8.3.3 Initial Response

Once an Information Security incident has been reported, Incident Management processes begin immediately with Incident Identification. Identification is the process of determining whether or not an incident has occurred, and if so, determining the nature of the incident, categorizing the incident, and prioritizing incident response. The IRM or designee shall assign a person to be responsible for handling the incident. The IRM or designee shall perform analysis to determine if there has actually been an incident and if so to understand its scope.

8.3.4 Categorizing and Prioritizing Incidents

Once it has been confirmed that an Information Security incident has occurred, the incident shall be categorized according to Section 5. The incident shall then be prioritized per Section 6 and shall be responded to in order of priority.

8.3.5 Additional Requirements for Specific Classes of Compromised Data

Once it has been confirmed that an Information Security incident has occurred, and if it is determined that sensitive information may be involved, the IRM shall ensure the appropriate functional Subject Matter Expert is involved in the response processes.

8.4 Incident Containment

8.4.1 Overview of Incident Containment

The overall purpose of Incident Containment is to limit the damage that an incident may cause while at the same time causing the least possible impact to mission-critical processes. The Containment phase of the Incident Management Lifecycle requires critical decision-making (e.g., determining whether to shut down a system, disconnect it from the network, monitor its activity, or disable functions such as remote file transfer) and consists of short-term, planned actions that may remove access to compromised systems, limit the extent of current damage to a system, and prevent additional damage from occurring. The specific steps that should be followed depend on the type of incident (intrusion, virus, theft, etc.), and whether the incident is in progress (e.g., an intrusion, disruption of service) or is discovered after the action (e.g., a theft of equipment or a discovery within a log audit). Limiting the scope and magnitude of the incident as quickly as possible is a higher priority than allowing the incident to continue in order to gain evidence for identifying or prosecuting the perpetrator.

Ncell	Ncell	Classification: Internal
	Information Security Incident Management Procedure	Owner: CIO/Head of IT
		Effective Date: 05-10-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

8.4.2 Overview of Incident Containment

- i. When an Information Security incident affects mission-critical information or computing services, the IRM in consultation with the Head of IT and other key affected parties shall decide how to address the incident while at the same time minimizing impact to mission-critical processes.
- ii. In the case of a low-risk incident, the IRM may decide to move quickly to eradicate the incident without shutting down the affected system. In the case of a high-risk incident affecting a system with sensitive information or applications, the IRM may direct that the system be shut down or at least be temporarily isolated from the network. If there is a reasonable chance that letting a system continue to run as normal without risking serious damage, disruption, or compromise of data, or to identify a perpetrator, the IRM may determine that operations can continue under close monitoring.

8.5 Incident Eradication


Eradication is the application of sufficient technical measures on an affected system to eliminate the causes and effects of an intrusion or attack to a point where the risk of re-emergence of the cause is reduced to zero or mitigated to a minimal or acceptable level. Once all containment procedures and actions have been completed, and all data which may be useful to performing an ongoing analysis of the compromise is collected, eradication may proceed.

8.5.1 Guidelines for Incident Eradication

- i. **Review Incident Analysis:** Data collected and analyzed shall be used to understand the exploited vulnerability and may inform the minimum requirements for eradication.
- ii. **Perform a Vulnerability Analysis:** A vulnerability analysis tool (such as an automated vulnerability assessment tool) shall be used to scan exposed systems, services, and applications that are connected to the affected systems. Special attention may be paid to web servers/services, databases, or other complex architectures such as Service Oriented Architectures (SOA), mainframes, and e-commerce systems.
- iii. **Improve Security Controls on the affected System and other Systems:** Appropriate protection techniques shall be implemented in the environment where appropriate. These techniques may consist of activities such as: applying security patches, changing the system name or IP address, securing and protecting boundary defense hardware and software, implementing Network Admission Control (NAC), implementing two-factor authentication, or in extreme cases, porting the functions to a more secure operating system.
- iv. **Focus on Removing Malignant Artifacts:** The IRT shall concentrate on the eradication of malignant artifacts (e.g., Trojan horses), and may concentrate on the eradication of benign artifacts if they present serious risk.
- v. **Thoroughly Remove Artifacts From all Media:** The IS Lead, or designee, shall ensure that all malicious artifacts are removed from all systems and media (including CD-ROMs, USB drives and backup media) by using one or more proven commercial eradication applications or by manual surgical removal following an in-depth malware analysis which has identified the entirety of the malware package or by re-baseline the affected host.

8.6 Incident Recovery

Recovery is defined as restoration of affected systems to normal operational status. The recovery phase procedures for resumption of normal operations contained in this section provide a framework for use when recovering from an incident. The recovery process begins when the cause of the incident has been eradicated, or mitigated to a degree of risk determined to be acceptable by the ISO and the IRM

	Ncell	Classification: Internal
	Information Security Incident Management Procedure	Owner: CIO/Head of IT
		Effective Date: 05-10-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO


8.6.1 Selection Requirements for System Recovery

- i. For systems categorized with a Low or Moderate Security classification as per the Information Security Categorization Standard, if the analyses conducted through the lifecycle has provided a high degree of confidence that the incident did not affect the software or the information stored on the system, then there may only be a minimal amount of effort required to provide assurance that the system is properly recovered. In this case, only simple countermeasures shall be needed to protect the system against future occurrences.
- ii. If the system has a High Security classification as per the Information Security Categorization Standard, or in a case where the analyses conducted through the lifecycle has not provided a high degree of confidence that the incident did not affect the system software or data, then there may be a more complex recovery solution requiring a complete restoration of the system to a normal operating condition.

8.6.2 Guidelines for Incident Recovery

The required guidelines for conducting Recovery are:

- i. **Document the Recovery Phase:** Documentation of the recovery steps can assist in maintaining focus as the recovery process proceeds. All documentation associated with the incident shall be noted in the incident report for later review and reporting.
- ii. **Decide the System Restoration Procedure:** Several restoration options may be available depending on the severity of the incident, the sensitivity of the system affected, and the backup systems available. The selection of the best option may require the involvement and authorization of the application/data owner, the IRM, and/or senior management.
- iii. **Validate Data Restored from Untrustworthy Sources:** In restoring files other than the operating system and applications files, only the most trusted backup files shall be used. Restored system data and user files shall be investigated for altered data or other signs of compromise.
- iv. **Validate the Restored System before Returning to Service:** Validation of the restored system shall be performed by executing a known series of development tests when prior test results are available for comparison. Prior to restoration of network connectivity, the IRM or designee shall verify that all known vulnerabilities have been mitigated.
- v. **Get Authorization and Communicate with Users before Restoring Service:** IRM's authorization shall be obtained before reconnecting the recovered system to the network to resume normal operations, and any organizations that would be affected shall be notified.
- vi. **Conduct a review of the security controls:** The IRM shall verify that the system is configured in accordance with the current configuration management guidelines; that logging, auditing, and accounting programs are functional; and any security tools are functioning. The IRM delegate is responsible for ensuring discrepancies are corrected.
- vii. **Monitor the Restored System:** So as to maintain a high-level confidence in the security of the restored system it shall be monitored to prevent additional intrusion, or a recurrence of the incident. Any knowledge gained through analysis should be used to provide insight into an attacker's techniques and/or methods to develop better monitoring techniques. Some items to be monitored may include but not limited to: failed login attempts, attempts to access back doors, attempts to re-exploit the original vulnerability, and attempts to exploit any new vulnerabilities of the system.
- viii. **Only Perform "Rapid Restoration" When Mission-Critical:** If it is decided to return to operation or maintain the affected system in operational use without completion of the recovery process due to mission-critical requirements, the recovery process may continue in parallel with operational use. Incident analysis and the elimination of vulnerabilities should continue in parallel with rapid restoration to mitigate the risk further incidents. Should system vulnerabilities exist, the

	Ncell	Classification: Internal
	Information Security Incident Management Procedure	Owner: CIO/Head of IT
		Effective Date: 05-10-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

system shall be updated as quickly as possible to preclude a recurrence of the same type of incident, the level of monitoring shall be increased and, and if applicable, intrusion detection shall be employed to ensure that a new incident is detected rapidly. It is preferred that mission-critical operations continue on unaffected, fail-over components when possible.

- ix. **Replace the Affected System with a Backup System When Possible:** Employment of a backup system for operational use while the affected system is under examination may be permissible. Because data stored to backup may already be contaminated before the incident is actually reported and addressed, backup tapes shall be carefully examined to ensure the integrity of the data. The compromised system should first be isolated from the network and from all backup systems. The backup system data may then be restored from trusted system backup files rather than using possibly contaminated data files from the affected system. If system mirroring is employed, backup tapes shall be examined to determine at what point the restore should occur in order to ensure the integrity of the data restoration process.
- x. **Restore the System Offline Whenever Operations Allow:** Restoration of the operational system while it is kept off-line may provide the greatest opportunity for recovery of incident data and for determining the cause and extent of the incident. Operating the system in a stand-alone, single user status may prevent other users, intruders, and malicious processes from accessing or changing the compromised system.
- xi. **Restore the Operating System from Trusted Media Whenever Operations Allow:** Installation of a new operating system may be performed on the affected system only if the activity is conducted with the original software media because compromise of the system may have occurred in many areas including binary and running process files.

8.7 Closure and RCA

- i. Conduct a detailed root cause analysis of the information security incident.
- ii. Obtain learnings from the incidents.
- iii. Identify measures that can be taken to prevent the incident from happening in the future.
- iv. Create an action plan with timelines for implementation of the identified measures.
- v. Update the Known Error database.
- vi. Complete post-facto documentation.

8.7.1 Root Cause Analysis Mechanism

The NIST defines Root Cause Analysis as: “a principle-based, systems approach for the identification of underlying causes associated with a particular set of risks.” The following approach can be adopted for conducted a root cause analysis of any security incident.

- i. **Define the Problem:** This step has two questions;
 - a. “What” is happening.
 - b. “What” are the symptoms?
- ii. **Collect Data:** This step has three questions;
 - a. “What” proof do you have that the problem exists?
 - b. “How” long has the problem existed?
 - c. “What” is the impact of the problem?
 - d. This Step also involves meetings with people who are familiar and understand the situation. The situation needs to be viewed from different perspectives of those involved.
- iii. **Identify Possible Causal Factors:** Three specific questions for this step are:
 - a. “What” sequence of events leads to the problem?
 - b. “What” conditions allow the problem to occur?
 - c. “What” other problems surround the occurrence of the central problem?
 - d. This Step also involves identifying causal factors. Four methods to use are:
 - e. ask “so what?” of all the facts. This determines possible consequences of a fact.
 - f. ask “why?” five times to get to the root of the problem. This moves from symptoms to causes.
 - g. “drill down,” break down a problem into small and detailed parts.
 - h. formulate “cause and effect diagrams.” It is a chart showing where the trouble possibly

Ncell	Ncell	Classification: Internal
	Information Security Incident Management Procedure	Owner: CIO/Head of IT
		Effective Date: 05-10-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

began, leading to possible causal factors.

iv. **Identify the Root Cause(s):** This Step has two questions:

- "Why" does the causal factor exist?
- "What" is the real reason for the problem? The same methods used in Step #3 are used. However, the stress is on the "why" question. Cause and effect are further analyzed.

v. **Recommend and Implement Solutions:** This Step has four questions:

- What can be done to prevent the problem from happening again?
- How will the solution be implemented?
- Who will be responsible for it?
- What are the risks of implementing the solutions? This is when you analyze cause and-effect processes. With that, you can identify the system changes needed. These changes will then have analyses of risk and impact.

9. Forensic Investigation

Forensic investigation may need to be conducted depending on the severity and criticality of the incident. Cyber forensics is the application of investigation and analysis techniques to collect evidences from computing devices, while preserving its integrity for examination and reporting. Care is taken to ensure that the evidences gathered are legally admissible. It enables Ncell to perform investigation in a structured and documented manner while maintaining a documented chain of evidence to identify what exactly happened and who/ what was responsible for it.

Typical forensic analysis includes a manual review of material on the media, reviewing the Windows registry for suspect information, discovering and cracking passwords, keyword searches for topics related to the crime, and extracting e-mail and pictures for review. It also involves development of an Incident Response procedures on Windows Forensics/Mobile Forensics which includes SIM Card Forensics, Memory Card Forensics, Hard Disk Forensics and Dead Box forensics, etc. It helps in validating the RCA findings on various cyber security incidents affecting Windows OS and mobiles.

Phases of forensics investigation can be broadly categorized as:

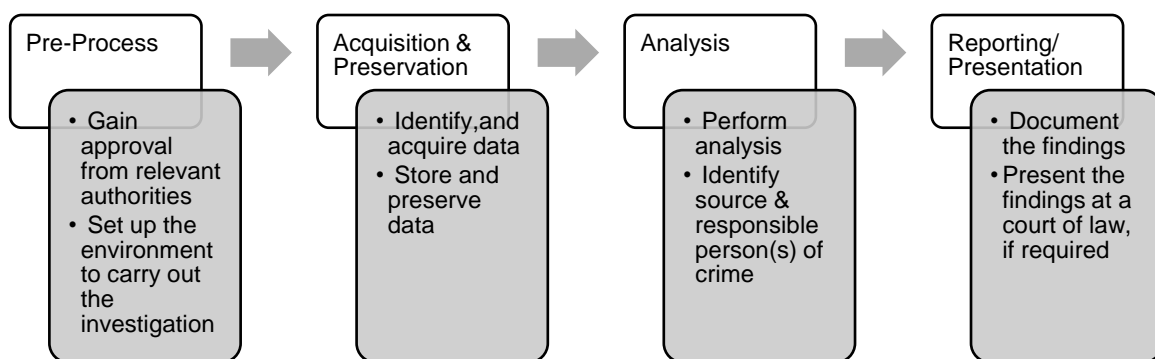



Figure 3. Phases of Forensic Investigation

	Ncell	Classification: Internal
	Information Security Incident Management Procedure	Owner: CIO/Head of IT
		Effective Date: 05-10-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

10. Escalation Matrix

The following escalation matrix should be adhered to:

Escalation Level	Level Description
Level 1	Unit Head
Level 2	Section Manager
Level 3	Head of IT & CTO

11. Governance and Compliance

- Exception management process shall be followed to raise the exception for this procedure.
- Internal and external compliance review shall be conducted as per the organization internal and external audit requirements.

12. Associated Documents

- Information Security Policy

Priority / Incident Type	First Escalation Level (After resolution time)	Second Level Escalation (After resolution time)	Third Level Escalation (After resolution time)
P1 – Critical	2 hours	3 hours	4 hours
P2 – High	2 hours	4 hours	6 hours
P3 – Medium	After 24 hours	After 48 hours	After 72 hours
P4 – Low	After 2 days	After 4 days	After 6 days