एन एम डी सी
NMDC

INCIDENT HANDLING POLICY

Author		**Document name**		**Date of first issue**	
Owner	C & IT Department	**Document ref. no.**		**Date of latest re-issue**	
Version	1.1	**Page**	1 of 10	**Date of next review**	
Issue Status	Under Review/ Live	**Security classification**	Internal use only	**Reviewer**	

एन एम डी सी
NMDC

INCIDENT HANDLING POLICY

VERSION CONTROL

Revision no.	Date of issue	Prepared by	Reviewed by	Approved by	Issued by	Remarks

एन एम डी सी
NMDC

INCIDENT HANDLING POLICY

OBJECTIVE

The purpose of this policy is to minimize the damage from the incidents and malfunctions happening in NMDC`s IT environment and also to monitor and learn from such incidents. NMDC will detect and report incidents relating to exceptional situations in day-to-day administration of IT and information security related areas in a timely manner.

SCOPE

This policy applies to all NMDC staff as well as to the third parties (contractors/trainees/clients and other users), and all NMDC information resources.

RESPONSIBILITY

Commented [BA1]: A CERT is not necessarily needed. The existing team can be assigned roles to handle the incidents.

The responsibility of implementing and monitoring the policy and procedures mentioned in this document is of Security Officer (IT and Communications). The Security Manager must also review the IT systems for incident management and security related issues.

Security manager is responsible for ensuring that incident response procedures are established, maintained, and documented as outlined above. He is the focal point during security incidents and is the Incident Handling Team (IHT) Lead.

Security Officer is responsible for providing a chain of custody and security expertise to company management including investigating and reporting security incidents.

Security Administrators of their respective areas are responsible for responding to incident response notification and investigating and reporting security incidents pertaining to their system expertise. System Administrators are part of the IHT.

Security Executives as a support for the security administrators for the Incident management and recovery.

All individuals authorized to access the IT resource are responsible for observing prudent security precautions and reporting any suspicious situations to the Security team.

POLICY RULES

Defining 'incident'

Commented [BA2]: The portal for incidents should enable users to select the category while reporting incident.
A comprehensive categorization will reduce dependency on employee to identify incidents

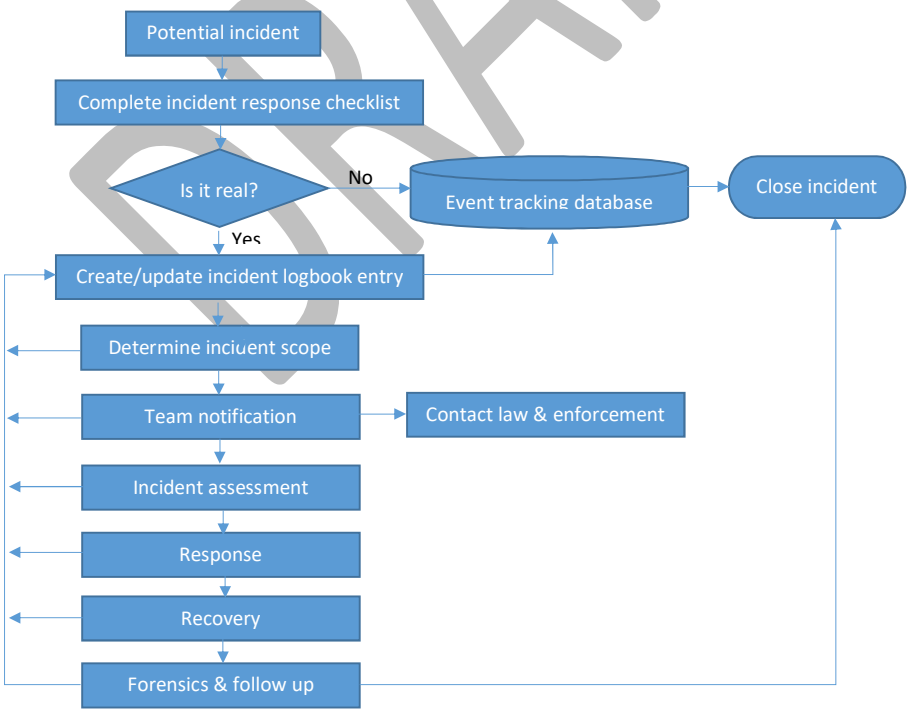
1. 'Incident' is a term related to exceptional situations or a situation that warrants intervention of senior management. An incident is detected in day-to-day operations and management of the IT function. This may be result of unusual circumstances as well as the violations of existing policies and procedures of NMDC.
2. Security Incident may relate to any of the following, but not limited to
    a) Disruption of NMDC services
    b) Unauthorized modification of information/data
    c) Sensitive information lost
    d) Violation of NMDC policies

INCIDENT HANDLING POLICY

e) Unauthorized access to information
f) Identity thefts.
g) Loss/theft of NMDC's assets
h) Misuse of information and computing resources
i) Incidents related to Physical Security such as but not limited to laptop theft, unauthorized entry into premises, assault, etc.
j) Suspected/Successful hacking attempts
k) Virus incidents regarding e-mail, Internet, CD, diskette and others
l) Failure / crash of IT equipment
m) Power problems and loss of data
n) Natural calamity or disaster
o) Hardware, Software, and Operational errors that results in erroneous data

3. Any incident impacting security should be reported as per the Security incident reporting procedure.
4. User should be made aware of procedures for reporting a Security incident.
5. Users and contractors should not probe the systems for its weaknesses and suspected areas of weakness should be reported.
6. Users and contractors should not test the security mechanisms/products deployed at NMDC.
7. Whenever the computing resources are observed functioning in an unusual manner, which relates to any security incident, operations team should disconnect the resource from the network and any evidence such as log files should be preserved.

Incident response flowchart



एन एम डी सी
NMDC

INCIDENT HANDLING POLICY

Detailed procedure

1. Detection and initial reporting

An incident may be detected by anybody in the company. The concerned employee must immediately bring it to the notice of the Incident handling team. The concerned Security Executives should complete the Incident Response (IR) checklist and additionally inform Security Officer depending on the nature and criticality of incident. (Refer Annexure 1 – Incident checklist).

The person who discovers the incident shall inform immediately to any of the following (based on increasing order of severity):

a) Helpdesk
b) Security Executives
c) Security Administrator
d) Security Officer
e) Security Manager

Is it real

It is the responsibility of security executive and administrator to determine the exact problem. To assist in identifying whether there really is an incident, security executive/administrator may take help of Security Officer/Manager. Audit information is also extremely useful, especially in determining whether there is a network attack. It is extremely important to obtain a system snapshot as soon as one suspects that something is wrong. Many incidents cause a dynamic chain of events to occur, and an initial system snapshot may do more good in identifying the problem and any source of attack than most other actions that can be taken at this stage. (Refer Annexure 2 – Symptoms)

Prioritization of duties in the event of incident

It is also important to prioritize the actions to be taken during an incident well in advance of the time an incident occurs. Sometimes an incident may be so complex that it is impossible to do everything at once to respond to it; priorities are essential. In case of an incident the activities executed would be prioritized as under:

a) Priority one—Protect human life and people's safety.
b) Priority two—Protect classified and/or sensitive data. Prevent exploitation of classified and/or sensitive systems, networks or sites. Inform the other security officers in other offices about the incidents that have occurred.
c) Priority three—Protect other data, including proprietary, scientific, managerial and other data. Prevent exploitations of other systems, networks or sites and inform already affected systems, networks or sites about successful penetrations.
d) Priority four—Prevent damage to systems (e.g., loss or alteration of system files, damage to disk drives, etc.).
e) Priority five—Minimize disruption of computing resources (including processes). If required with the approval of Security Officer, shut a system down or disconnect from a network than to risk damage to data or systems. However, the damage and scope of an incident may be so extensive that service agreements may have to be over-ridden.

2. Update incident logbook

If it is determined that the incident is real, the details of the incident are recorded in the Incident logbook. Recording system events, telephone conversations, time stamps, etc., can lead to a more rapid and systematic identification of the problem, and is the basis for subsequent stages of incident handling (i.e. response, recovery, law enforcement involvement).

All the logs listed below (in case of hacking or computer related incident) should be attached with the logbook. At a minimum, you should record:

a) All system events (audit records).
b) All actions you take (time tagged).
c) All phone conversations (including the person with whom you talked, the date and time, and the content of the conversation).

Event tracking database: The Event Tracking Database is to be used to track and document all reported potential incidents (whether real or not). This database will have all the historic information of any type of security event. The Event Tracking and Notification Checklists for each event are stored here. Additionally, all information concerning an incident that is entered into the Logbook needs to be eventually entered into the event-tracking database.

3. Determine incident scope

Upon completing the incident response checklist and determining the event is real, the security executive\administrator will determine whether or not escalation is warranted. If the event can be resolved in the course of the phone call, completing the IR Checklist should close the event. If the event requires further action, it should be classified for proper handling. The scope and impact of the problem also needs to be assessed by the IHT. It is important to correctly identify the boundaries of the incident in order to effectively deal with it. The impact of an incident will determine its priority in allocating resources to deal with the event. Some of the areas where assessment has to be performed are:

a) Single site or multi-site incident?
b) How many IT resources/components effected by this incident?
c) Is sensitive information involved?
d) What is the entry point of the incident (network, phone line, local terminal, etc.)?
e) What is the potential damage of the incident?
f) What is the estimated time to close out the incident?
g) What resources could be required to handle the incident?

4. Team notification

Security officer is responsible for informing the concerned members of the IHT. Response can occur through phone consultation. If on-site response is required, team members are activated through the pager or phone system. Any subject matter experts necessary due to involved technologies or the event type should be contacted to determine availability.

Here are the lists of personnel that should be notified during an IR at NMDC:

a) NMDC`s IHT Members (Technical, Administrative, Response Teams, Investigative, Legal, Vendors, Service providers)
b) Wider community (Users, Customers, if required).
c) Other sites that might be affected (if required).
d) Vendor List

Explicit notification

First of all, any notification to either local or off-site personnel must be explicit. This requires that any statement (be it an electronic mail message, phone call, or fax) provides information about the incident that is clear, concise, and fully qualified.

Legal department

A member identified from NMDC`s legal department will be notified incident is in progress. The member will protect the legal and financial interests of NMDC assets, systems and resources. If required the member of legal council may establish contacts with personnel from investigative agencies such as the CBI and local law enforcement.

5. Incident assessment

The objective of this phase is to perform a high level risk assessment of the incident. The risk assessment will be completed on a high within hours of arriving on site, and no actions should be taken which limit later recovery options.

a) Gather background information: Perform the initial risk assessment by examining the network maps. Identify if:
   i. The compromised machine is critical.
   ii. Any critical machines "trust" the compromised machine.
   iii. Any critical machines on the same subnet as the compromised machine.
   iv. Any critical machines trust a machine on the same subnet as the compromised machine
   v. Any sensitive information travel by the compromised machine

b) Monitor: Monitoring will begin as soon as the Incident Handling Team arrives and continues until recovery is complete. In case of a computer hacking some of the steps to be followed are
   i. Determine if there are any active connections to or from the compromised machine.
   ii. Use a packet sniffer to check for any packets entering or leaving the machine.
   iii. If active connections are noted, look for clues in the traffic types and source/destination addresses.
   iv. If any of the addresses noted are client addresses but appear suspicious, place packet sniffers at those locations as well.
   v. If critical information is being transferred,
   vi. If monitoring detects active hacker activity, observe and record all activity. Observing the hacker first hand is the most effective way of determining hacker actions. Postpone any further actions that will alert the hacker.

c) Examine network logs: Logs from the network devices (router etc.) will/may be used to know about hacker activity. Examine and store logs from firewalls, IDS, routers, or similar network devices. Any traffic that matches the attacker profile will be stored. This includes traffic with a

source/destination address of the compromised machine or suspected hacker. It also includes traffic of the type that matches the suspected compromise method.

6. Formulate response options

The complete IHT would be responsible for formulating the response options. When formulating options, carefully consider the consequences of each action. The security manager is overall in charge of the actions to be taken. In case of a dispute his verdict would be final. The response to an event will fall into the general categories of monitoring, investigating, isolating, containing, and eradicating.

7. Recovery

At this point the method and extent of compromise have been determined and the damage has been accessed. The goal of this stage is to recover compromised machines to a secure, operational state as efficiently as possible. In case of an intrusion the machines access information will be changed immediately. Any machines that share accounts with the compromised machine will also be considered compromised. All compromised machines will be recovered on the basis of their criticality. Some of the steps that would be performed in case of intrusion are:

a) Password Change (host wide, system wide, or enterprise wide).
b) Plug vulnerabilities. Done for machines not directly compromised. The network log may be used to identify the vulnerability used by the intruder. Securing a host involves turning off unused services, applying operating system and application patches, strong passwords, and competent administration. If the method of compromise was due to insecure user practices or poor administration, user education and policy creation should be part of the recovery.

All the steps and recovery options decided in the previous stage will be implemented. The actual recovery will take place offline where possible. If the machine is critical to operations, a temporary replacement while the host is rebuilt and secured. If several machines need to be rebuilt, then it would be performed simultaneously.

8. Forensics & follow-up

The most critical element of the follow-up stage is performing a post-intrusion forensics analysis. The forensics report will cover

a) What happened, and at what times
b) What was the staff involved with the incident perform
c) A formal chronology of events (including time stamps) important for legal reasons.
d) Monetary estimate of the amount of damage the incident caused in terms of any loss of software and files
e) Hardware damage, and manpower costs to restore altered files, reconfigure affected systems, and so forth.
f) Actions taken by the staff and IHT team
g) Methodology and tools used for forensics study
h) Copy of all the logs
i) Recommendations for enhancing security and rectifying bugs

INCIDENT HANDLING POLICY

A follow-up report is valuable because it provides a reference to be used in case of other similar incidents. Similarly, it is also important to act quickly. This estimate may become the basis for subsequent prosecution activity by the CBI and other legal agencies.

Follow up action

If it is determined that the breach occurred due to a flaw in the systems' hardware or software, the vendor (or supplier) will be notified as soon as possible. The relevant telephone numbers (also electronic mail addresses and fax numbers) would be kept with the Security Officer.

9. Close incident

Once the incident has been closed, ensure that a follow-up analysis has been completed and recommendations have been incorporated to the Incident Response Standard.

ANNEXURE

Commented [BA3]: These formats can be incorporated in incident handling portal.

Annexure 1: Incident Response Checklist

- Time/Date:
- Phone:
- Nature of incident (real or perceived? Type of incident if real e.g. virus, worm, intrusion, abuse, damage etc.):
- Description of incident and how did it occur(whether through email, through firewall, etc):
- When did incident occur?
- How was incident detected?
- When was incident detected?

Damage:

- Compromised computer/Server/network components:
- Hardware/OS/Software involved:
- Virus (if any):
- IP or network address of compromised system:
    - Network type at hacked machine: (Ethernet, token ring, FDDI, other)
    - Critical to network ops or business operation? How?
    - Any critical information here (refer to data classification standard)?
    - Physical location?
    - Physical security?
    - Who is primary user/administrator? Contact info?
    - Current status of computer?
- Where from the attack came from such as IP addresses and other related information about the attacker:

Hacker actions (if any):

- Ongoing activity?
- Source address?

- Malicious/foreign logic introduced?
- Any denial of service?
- Any vandalism?
- Any indication whether insider or outsider?

Customer/Vendor actions:

- Connectivity pulled?
- Audit logs examined?
- Remote access/local access to compromised machine available?
- Any changes in network – such as Firewall, ACL, etc.?
- Who has been notified?
- Other actions?

Other Information from:

- System users
- System administrators of compromised machine
- Network administrators at site
- Details discussed with:
- Anyone within client organization not to discuss information with?
- Other?

Signature of Employee:

Signature of Dept/Functional head:

Signature of head Systems:

Annexure 2: Symptoms

There are certain indications or "symptoms" of an incident which deserve special attention:

1. System crashes
2. New user accounts (e.g. the account RUMPLESTILTSKIN has unexplainably been created), or high activity on an account that has had virtually no activity for months
3. New files (usually with novel or strange file names, such as data.xx or k)
4. Accounting discrepancies (e.g. in a UNIX system you might notice that the accounting file called /usr/admin/lastlog has shrunk, something that should make you very suspicious that there may be an intruder)
5. Changes in file lengths or dates (e.g. a user should be suspicious if he/she observes that the .EXE files in an NT computer have unexplainably grown by over 11800 bytes)
6. Attempts to write to system
7. Data modification or deletion (e.g. files start to disappear)
8. Denial of service (e.g. a system manager and all other users become locked out of a UNIX system, which has been changed to single user mode)
9. Unexplained, poor system performance (e.g. system response time becomes unusually slow)

10. Anomalies (e.g. “GOTCHA” is displayed on a display terminal or there are frequent unexplained “beeps”)
11. Suspicious probes (e.g. there are numerous unsuccessful login attempts from another node)
12. Suspicious browsing (e.g. someone becomes a root user on a UNIX system and accesses file after file in one user’s account, then another’s)

None of these indications is absolute “proof” that an incident is occurring, nor are all of these indications normally observed when an incident occurs. If any of these indications are observed, it is important to suspect that an incident might be occurring, and act accordingly. It is essential at this point to collaborate with other technical and computer security personnel (team notification) to make a decision as a group to assess the incident.

Annexure 3: Action Initiated

- **Action Initiated**
  - Date:
  - Incident ID:
  - Brief description (response plan):
  - Impact of the incident:
  - Action taken:
  - Effectiveness of action taken:
- **Routing:**
  - Security Executive / Administrator responsible for disposal
  - Approved by Security Manager

Annexure 4: Incident Contact List

Information Security Manager:

Name: _____Work Phone: _____

HomePhone:_____Mobile:_____Fax:_____E-mail: _____

Information Security Officer:

Name: _____Work Phone: _____

HomePhone:_____Mobile:_____Fax:_____E-mail: _____

Information Security Administrator:

Name: _____Work Phone: _____

HomePhone:_____Mobile:_____Fax:_____E-mail: _____

Information Security Executive:

Name: _____Work Phone: _____

HomePhone:_____Mobile:_____Fax:_____E-mail: _____

एन एम डी सी

NMDC

INCIDENT HANDLING POLICY

Legal Expert:

Name:_____ Work Phone: _____

Homephone:_____Mobile:_____Fax:_____E-mail:_____