एन एम डी सी
NMDC

SECURITY AUDIT, EVENT LOG AND AUDIT TRAIL 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

SECURITY AUDIT, EVENT LOG AND AUDIT TRAIL POLICY

VERSION CONTROL

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

एन एम डी सी
NMDC

SECURITY AUDIT, EVENT LOG AND AUDIT TRAIL POLICY

OBJECTIVE

In order to safeguard information and computing resources from various business and environmental threats, systems and procedures must be developed and implemented to monitor the activities related to the use of NMDC Information System resources, to ensure that the information on these systems is not disclosed to unauthorized individuals, and that the integrity of the data is maintained. NMDC should therefore have a policy for conducting security audits, maintaining the event logs and audit trails, preventing and detecting any unwanted tampering and use of its IT resources. This policy will also provide the authority for members of NMDC's Information Security team to conduct a security audit on any system at NMDC. In addition this document aims to provide a guideline for what to audit.

These security audits may be conducted to:

a) Ensure integrity, confidentiality and availability of information and resources
b) Investigate possible security incidents
c) Ensure conformance to NMDC security policies
d) Monitor user or system activity where appropriate

SCOPE

This policy applies to all the NMDC staff and any persons using the information technology resources of NMDC. This includes contractors, consultants, third-party associates and any temporary employees of NMDC.

RESPONSIBILITY

The Security Officer-IT is the executive owner of this policy. He shall be responsible for implementing the policy and subsequent procedures in the organization. All the users of NMDC's IT Resources, including the IT Department, are responsible for executing the procedures. Security Manager shall monitor the implementation and execution of these procedures.

POLICY RULES

General

Security audit:

Regular Information Security Audit of NMDC resources shall be conducted as per the time interval designated by the Information Security Manager.

IT security audit should be done as per best practice guidelines like ISACA, ITIL, BS15000, ISO 27001 etc.

When requested, and for the purpose of performing an audit, any access needed will be provided to members of NMDC's Information Security team (team comprising of IT staff assigned responsibilities of Information Security) or third party security auditor. This access may include:

Commented [BA1]: Department to decide on who will conduct audits

a) User level and/or system level access to any computing or communications device
b) Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on NMDC equipment or premises
c) Access to work areas (offices, cubicles, storage areas, etc.)
d) Access to interactively monitor and log traffic on NMDC networks.

एन एम डी सी
NMDC

SECURITY AUDIT, EVENT LOG AND AUDIT TRAIL POLICY

Event log and audit trail:

All such records, event logs and audit trails shall be maintained, as are required for:

a) Monitoring the appropriate usage of NMDC's IT resources
b) Detecting unwanted and malicious activity with the IT resources
c) Associating particular events with users and reporting on the effectiveness and compliance with security policies.

It will be the responsibility of users of NMDC's IT resources, to report any violations or breaches and any other Information Security related events that are noticed by them.

Procedures – Security audit

Prior approval

The authorizations for conducting a security audit have to be taken from the respective application owner by the member of the Information Security Team conducting the audit (Refer Annexure 1). This shall be followed by an approval from the concerned Security Officer. The access at the database and Operating System level has to be approved by the concerned Security Officer, for conducting the security audit. In case the security audit is being conducted by a third party, approval has to be taken from the Security Manager for the same.

User responsibility

All users of the application shall co-operate with the concerned application being audited for security by providing necessary information to the Security Auditor.

Security auditor's responsibility

The Security Auditor shall not disclose any such information gathered during the security audit, as is liable to cause harm to the business of NMDC. All the documents collected during such audit along with the report shall be handed over to the concerned Security Officer.

Application security audit

The security of any functional application in NMDC shall include but not limit to the following areas to be audited:

a) No. of administrator level accounts and their access logs
b) Access controls for each user – frame/field/transaction level
c) Check successful/unsuccessful logins and logouts
d) Successful/unsuccessful use of privileged commands in the application, if any
e) Successful/unsuccessful use of application and session initiation
f) Successful/unsuccessful modifications of access controls

Operating Systems audit

The Operating System Security audit is the most critical part of the security audit, since access to the OS, remotely or locally, can lead to access to any information resources residing on the particular server. The OS level shall include but not limit to the procedures described below.

एन एम डी सी
NMDC

SECURITY AUDIT, EVENT LOG AND AUDIT TRAIL POLICY

1. Licensing

The personnel conducting the security audit shall check the license agreement of the installed OS for adequacy. All operating systems used on application servers must have an adequate service agreement with vendors, the maintenance of which is the responsibility of the respective Security Administrators.

2. OS access controls

The security auditor shall verify that:

a) The access to sensitive OS commands on the server is restricted to only the users who require access to the particular platform, as per NMDC policy, for their job functions.
b) Users are not given a login ID on the local machine domain but are given on the domain controller wherever a domain controller is available. In case the domain controller is not available then local log in to the desktop can be given. In both cases all users will be given only one login ID with the associated group 'Users'.
c) The access to important program and data files is restricted only to the concerned personnel.
d) Where technically feasible, the OS has been configured to time-out online terminals/desktops/laptops after the set minutes of inactivity.

3. Technical review of OS changes

The security auditor shall verify if the latest patches and upgrades to the OS have been applied to take lnerabilities being exposed in the OS and for maintaining integrity of the data, thereof, on the server.

4. Privilege management

The privilege levels in each operating system differs in the way they are managed. The security auditor shall verify that:

a) The system level privileges are allocated only to system administrators of the particular system.
b) Privileges are allocated to individuals on a "need-to-know" basis and on an "event-by-event" basis (i.e. the minimum requirement for their functional role only when needed).
c) The record of all privileges is maintained. All privileges are granted only after going through the proper authorization process as per NMDC policy.
d) Users assigned high privileges for special purposes use a different user identity for normal business use (e.g. "System Administrator" login is not to be used for running the application).

5. Frequency

A regular OS security audit needs to be performed across the NMDC. For all the critical servers (LDAP, Firewall, IDS, Financial Application servers, etc.) audit would be performed every three months and for other servers every six months. The frequency may be changed in case of any intrusion detected subjected to the approval of Information Security Manager.

Network security audit

1. WAN connectivity

The security auditor shall verify that:

a) Access control have been defined on all the interfaces of the router so as to allow minimum number of services to other networks.
b) Password encryption service will have to be enabled on all the routers so that it does not display the password in clear text.
c) Telnet access to the switches will be restricted to only the administrator of the switches.
d) Whether the data traveling over the WAN link is encrypted or not.

2. LAN connectivity

LAN security audit shall consist of:

a) Checking the authentication mechanism for users to access the LAN resources
b) Check if dial-up connectivity using modems is being used from any computer on the network.
c) Check for all the points applicable to WAN connectivity

3. Network access

Security audit of network access shall comprise of the following verifications:

a) If all the host Operating Systems are configured to validate each user prior to allowing network access
b) If the company network is being used only for valid business purpose
c) If the access to network resources to all the users has been provided on the basis of valid business need. Unnecessary shares should not be created on individual hard drives by users and this should be verified during the audit
d) If the firewall has been hardened against penetration
e) If all the traffic from inside the network to the outside travels through the firewall and that the firewall is a dedicated host. If it is not a dedicated host, check for the services running on the firewall.
f) If all the default passwords of the networking equipment (routers, switches, etc.) have been changed or if such accounts have been disabled.
g) If any banners are being displayed on any external network connections without user authentication.

4. Frequency

A periodic audit would be performed for the networks of NMDC. The Information Security Officer would perform LAN audit at each location every three months and WAN audit every six months. The frequency may be changed in case of any intrusion detected subjected to the approval of Information security manager.

Additional procedures

The security audit shall consist of, apart from the procedures defined above, the following:

a) Review of roles & responsibilities and their segregation as per the security organization structure
b) Verification of physical security to the data centers
c) Licensing of the third party software being used at NMDC
d) Review of backup and recovery procedures
e) Review of any access to 3rd parties to the NMDC IT resources

f) Review of incident management and response mechanisms
g) Overall compliance to the IT Security Policies & Procedures
h) Review of Disaster Recovery Plan
i) Review of legal compliance to various IT Acts and Data Privacy Acts
j) Review of compliance for any IT Certifications- Systrust, BS 7799/ISO27001, etc.
k) Review of ecommerce initiatives and websites.

Procedures – Event log and audit trail

Reporting of Security Violations

1. Employee reporting requirements

All the employees of NMDC are responsible for maintaining a familiarity with the Information Technology Security Policies, Procedures, Standards and Guidelines and are responsible for reporting any suspected activities, security breaches or violations.

2. Recipients of reports

Employees who suspect a security breach or violation must communicate their concerns to their immediate supervisor. This individual must then evaluate the reported exceptions and refer all violations to the concerned Security Administrator.

3. Immediate reporting

IT resource misuse or suspected attempts to defeat IT resource safeguards, or attempts to gain unauthorized access to a resource should be reported immediately. All NMDC employees must cooperate with the Information Security Officer or security audit personnel on requests for information about usage of IT resources.

4. Provision of violation information to SO

The respective Security Administrator from the IT Department is responsible for summarizing and reporting security violations.

Network security monitoring

1. Purpose of monitoring

Systems should be monitored to ensure conformity to logical access policies and procedures. This is necessary to determine the effectiveness of measures adopted and to ensure conformity to logical access policies and procedures.

2. Audit trail rules

Audit trails recording exceptions and other security-related events must be generated by the Security Administrators and kept for at least six months to assist in future investigations and access control monitoring. A record of successful system access, in addition to rejected attempts, should be created. At a minimum, audit trails must include the following:

a) User ID's
b) Dates and times for logon and logoff
c) Terminal identity or location if possible

SECURITY AUDIT, EVENT LOG AND AUDIT TRAIL POLICY

3. Monitoring of system use

The systems use must be monitored to ensure that users are only performing processes that have been explicitly authorized. The level of monitoring required for individual systems should be determined by a separate risk assessment. Areas that must be monitored are:

a) Access failures
b) Review of logon patterns for indications of abnormal use or revived user Ids
c) Allocation and use of accounts with a privileged access capability
d) Tracking of selected transactions
e) The use of sensitive resources
f) Dial-up activity
g) Firewall activity
h) O/S and application access attempts

4. Role of Security Administrators/IT support team

For applications that have been determined to contain confidential / essential information, and where the system or application software permits, the concerned Security Administrators must produce security log reports, investigate access violations and resolve the violations periodically, as determined by Security Manager

5. Monitoring of Firewall Audit Reports

Auditing and logging should be enabled on the firewall to provide information about the activities to and through the firewall. Because a large volume of data passes through the firewall, significant amount of hard drive space may be required to take the best advantage. This should be made available at all times.

The Security Administrator responsible for the Firewall, must review the internet connection audit reports created on the firewall for any unusual/suspicious activities. The period between reviews should not exceed two days. Alarms must be configured to alert the Information Security Group about any suspected activities, security breaches or violations and any other related events generated by the firewall. The events to be monitored include, but not limited to:

a) A session being initiated from the external world
b) Spoofing activities
c) Suspicious activities taking place internally and from external sources
d) A new server/host attaching to the network locally and remotely
e) Well known hacker signatures
f) Password guessing attempts
g) Attempts to use privileges that have not been authorized
h) Modifications to production application software
i) Modification to system software

Use of Intrusion Detection Systems (IDS)

1. Use of Intrusion Detection/Prevention Systems

एन एम डी सी
NMDC

SECURITY AUDIT, EVENT LOG AND AUDIT TRAIL POLICY

The intrusion detection systems must be employed to perform real-time analysis of network traffic patterns to detect attempted attacks wherever technically feasible. Without intrusion detection software/hardware, it becomes more difficult to detect attempts to breach security, as well as certain types of sophisticated attacks, thus increasing the likelihood of undetected compromise of system integrity and confidentiality.

Intrusion Prevention Systems is a terminology used conventionally for certain advanced Host based IDS that can wrap the OS kernel with an agent that intercepts system calls and evaluates them against a database of defined attacks such as certain buffer overflows and privilege escalation. Such systems should be deployed on the critical servers.

2. Real-time intrusion detection on public access systems

Publicly accessible systems (e.g. external web sites) should utilize system-monitoring tools that provide real-time alerts whenever suspicious user activity is detected.

3. Host based and network based IDS

The Host based IDS must be placed on or close to systems where critical data is residing. Network based IDS must be located on a network segment which is critical and needs to be monitored continuously.

Compliance monitoring

1. Compliance review program

The Security Administrators must periodically review NMDC's security environment for compliance with published Information Technology Security Policies and Procedures. This must include an assessment of user practices, operations, and systems configurations.

2. Compliance monitoring

The Security Officer must continuously monitor the practices of the IT users and third parties present at NMDC to ensure that a high level of compliance is maintained with published Information Technology Security Policies and Procedures, Standards and Guidelines.

ANNEXURE

ANNEXURE 1: REQUISITION FOR SECURITY AUDIT

Business category: (e.g. IT/ Admin/ Production etc.)		
Name of the Functional/Departmental Head		Designation:
Unit:		Department:
Telephone Number Extension	Alternate Phone Extension	City
Type of Security Audit Requested (Tick the appropriate option) 1. Application 2. Operating system 3. Network 4. Complete		
Requestor's Name		Designation:
Signature of the Security Officer		Designation:

एन एम डी सी
NMDC

SECURITY AUDIT, EVENT LOG AND AUDIT TRAIL POLICY

Authorized by (Departmental/Functional Head) and remarks:	