एन एम डी सी

NMDC

INTERNET POLICY

DRAFT

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

INTERNET POLICY

VERSION CONTROL

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

DRAFT

एन एम डी सी
NMDC

INTERNET POLICY

OBJECTIVE

The objective of this policy is to define acceptable usage of internet services provided by NMDC. This policy is designed to protect the organizational resources against intrusion by malware that may be brought into the network by users as they use the internet. It is also designed to prevent unauthorized and unprotected connections to the internet which may allow a host of unsafe content to enter the organizational network and compromise data integrity and system security across the entire network.

SCOPE

This policy applies to everyone using Internet services in the company. It includes all Users, IT personnel, contractors, trainees, etc., working for NMDC.

RESPONSIBILITY

System Administrator and the IT users are responsible for implementing and executing the procedures mentioned in this document. IT Security Nodal Officer will monitor the execution of the procedures.

POLICY RULES

IT system management policy

1. Internet access shall be provided through wired and wireless access points.
2. Internet access is being provided for official business use only.
3. Internet access shall be available from 8 AM to 10 PM. Software updates, downloads are to be scheduled during night hours so that there is no inconvenience to the users during day time.
4. All internet traffic shall be routed through a firewall where corporate internet browsing policies are applied to block unwanted sites not relevant to official use.
5. Social media and entertainment sites may be allowed after office hours (6:00 PM – 8:00 AM).
6. Only standard ports shall be allowed / opened in firewall.
7. Any change in firewall rules are to be done only after the approval of Head-C&IT.
8. UTM Appliance / Firewall shall be configured in such a way that logs of at least 6 months are available. Efforts are to be made to download or take backup of the log.
9. C&IT reserves the right to block any user or device from internet access if there has been a breach or there is a security threat to the network.
10. All internet traffic must be routed through organization's approved proxy services only. Setting up such proxy server shall need clearance by the C&IT department.
11. C&IT Department shall not modify any firewall policies for allowing any user to access blocked websites. User can access such websites beyond office hours or through internet access via non NMDC network in case of BYOD devices.

User related policy

1. All internet usage is for business purposes only and requires users to avoid going to malicious websites which could compromise security.

DRAFT

एन एम डी सी
NMDC

INTERNET POLICY

2. Users' internet activity may be logged and monitored: The C&IT department shall monitor all internet usages from time-to-time. All internet activities will be logged for further review. This is to ensure all internet users adhere to the policy.
3. The users are allowed to connect to the internet as provided by C&IT department and has an approval for all connections to the internet or other private network. In case specific approval has been obtained to connect to a private network or the internet it shall have an approval from C&IT department and respective head of the function.
4. Users are not permitted to setup any type of proxy servers on the network.
5. The users should use NMDC provided internet facilities and should not access internet by connecting a modem, broadband or wireless media or any other such device. (non BYOD devices)
6. Prohibited and inappropriate use of internet: Use or attempt to initiate such activities using NMDC's computing facilities or equipment leading to abusive, unethical or 'inappropriate' use of the Internet are considered grounds for disciplinary, legal and / or punitive actions. The company has a discretion to block such internet activities that are deemed unsuitable and/or unacceptable. Examples of prohibited internet use include, but are not limited to, the following:
   a) Uploading/saving/sending NMDC's confidential and/or sensitive material to the public or any locations that are considered not appropriate or insecure
   b) Spoofing the identity of another user on the internet
   c) Introducing material considered indecent, offensive or is related to the production, use, storage or transmission of sexually explicit or offensive items on NMDC's network or systems using internet
   d) Conducting illegal activities, including gambling.
   e) Accessing or downloading pornographic/offensive and other improper materials
   f) Using software files, images or other information downloaded from the internet that has not been released for free public use.
   g) Uploading or downloading commercial software in violation of its copyright
   h) Making or posting indecent remarks
   i) Downloading any software or electronic files without reasonable updated virus protection measures in place.
   j) Using foul/obscene/offensive language/material
   k) Harassing, insulting others
   l) Violating laws (copyright and others)
   m) Hacking, damaging computers
   n) Misrepresenting yourself/facts or others
   o) Stock trading
7. Users shall refrain from clicking on offers and ads displayed on webpages as they may be fraudulent and affect NMDC's network.
8. It is a general policy that Internet access is provided via proper level of security and control to provide non-repudiation, authentication and encryption, to ensure confidentiality, integrity, and availability of the resident information.
9. Sensitive information resident on personally owned computers connected to the internet is generally more susceptible access by unauthorized personnel to cyber-attacks, and/or compromise. Such sensitive information must never be sent unencrypted via the internet.

DRAFT

INTERNET POLICY

10. The internet is globally accessed (i.e., there are no physical or traditional territorial boundaries). Transmissions through ISPs or servers can magnify these risks.
11. Sensitive business related information must not be posted on any public Internet website, discussed in a publicly available chat room or any other public forum on the internet.
12. Internet and email use should be consistent with the NMDC's code of conduct, and Information Technology Act 2000 (and amendments to it).

DRAFT