MNL:QSM:02/11

IT Policy of NHSRC

Division Name: IT-Admin Division

Division Head: Brig. Sanjay Baweja

Issue Date: 30 August 22

Revision No.: 01

Signature	*Signature*	*Signature*	*Signature*
Prepared By: Mukesh Kumar Executive-IT	**Checked By:** Mr. Kanhaiya Jha IT Manager	**Reviewed By:** Brig. Sanjay Baweja PAO, NHSRC	**Approved By:** **Executive Director,** **Maj Gen (Prof) Atul Kotwal, SM, VSM**

Information Technology Policy of NHSRC)

(Policy, Plan and Procedure)

Table of Contents

Information Technology Management Framework
(Policy, Implementation Plan and Procedure)

Overview:

National Health Systems Resource Centre (NHSRC) has been set up under the National Rural Health Mission (NRHM) of Government of India to serve as an apex body for technical assistance. IT Section is the part of Administration division of NHSRC which is responsible for developing IT framework, policy, assessing requirement for the organization along with provision of implementation support & monitoring of information management.

Framework of Information Management:

Information technology management policy of NHSRC address the governance, operational management, support services requirement for different division of NHSRC as follows:

Objective

Key objective and deliverables of the IT policy are:

- Ensuring safety- To ensure a safe, protective, and healthy environment to the individuals engaged with NHSRC by maintaining integrity.
- Creating awareness with procedure- To keep aware of procedures to be followed for various tasks which needs to perform by referring this policy with their own.
- To commensurate the standards- To promote Individuals to use standard procedure by confidentiality in audit.

Target Audience

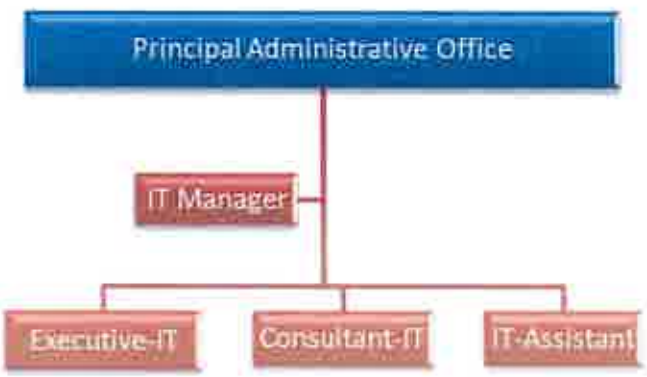
All NHSRC personnel and guests.

Management of policy

Key responsible person for management of Information process is:

- Draft prepared by Executive-IT and IT Manager.
- Reviewed by Principal Administrative Officer-NHSRC and
- Final approving authority of the IT policy is Executive Director-NHSRC.

Organogram:



Roles and Responsibilities of Members IT Team:

IT-Manager

Roles:

- Developing and implementing IT policy and best practice guides for the organization.
- To handle the dependencies between projects.
- Liaising/coordination with NIC or other vendors as required.
- Supervision of LAN and EPBAX at NHSRC.

Responsibilities:

- Manage information technology and applications systems.
- Design, develop, implement, and coordinate systems, policies, and procedures.
- Overseeing and determining timeframes for major IT projects including system updates, upgrades, migrations, and outages.
- File Management and Movement.
- AMC and Contact Management.
- Responsible for timely Insurance & Guaranty / Warranty status and recordkeeping.
- Issuance of IT Clearance Certificate.
- Monitor and optimize infrastructure performance and manages backups.
- Identify and deliver cost saving and service improvement initiatives.

Executive- IT

Roles:

- To provide IT support to NHSRC in running smooth communication network so that there will be no delay. Developing IT policy and IT Standards for functioning of IT Section.

Responsibilities:

- All IT Equipment (Server/Desktop/Laptop/Printer) and Networks- Hardware/software installation, configuration, maintenance, Monitoring and backup.
- Maintenance of service Complaint Records of IT equipment as well user's complaint record.
- Updation, monitoring, reporting of all websites developed and maintained by NHSRC.
- File Management- noting/drafting of IT related files along with track/maintaining of file movement register.
- Updation and maintenance of IT stock register.
- Procurement of IT related assets if required in compliance with Government financial Rule (GFR-2017).
- Contract Management- Preparation and execution (opening/preparation of comparative/letter of intent /award of contract) of Tender/EOI/Bid document for all IT related services/items.
- Monitoring and maintenance of satisfactory report, payment processing after service period or as per contract.
- Asset management- track of all IT related equipment, its servicing, maintenance of issuance and receiving register.

- Email- upon joining of any new user, mail ID creation, user joining to respective groups (Google/Exchange), configuration of outlook in user's computer/s.
- Intranet- upon joining of any user, creation of user in local Domain, joining of user's laptop in NHSRC's domain with all respective applicable policy, creation of respective folders, assigning respective permission and mapping network drive to respective user's laptop.
- Extension: Assigning of respective extension number along with maintenance of extension record.
- Monitoring and maintenance of Biometric machine/CCTV/EPABX.

Consultant-IT

Roles:

- Support IT Manager in Developing and implementing IT policy and best practice guides for the organization.
- Manage the LAN, TCP/IP and troubleshooting, conversant with windows server administration.
- To handle the dependencies between projects.
- Liaising / coordination with NIC or other vendors as required.
- Manage EPBAX at NHSRC.

Responsibilities:

- Maintain the program documentation that includes all plans, deadline & briefs.
- Any assignment, which may be given/ assigned to him/her from time to time by Executive Director/ Principal Administrative Officer/IT manager.

Policy Review and Amendments:

- Policy should be reviewed by IT Section.
- Review Period should not be more than five years.
- Record of Amendments Should be kept likewise tabulated below:

Date	Version	Issues	Reason	New Number
28 Nov. 23	V-1.0	***Social media and BYOD***	Amendment	V-2.0

Applicability & Compliance:

- All NHSRC personnel will comply this policy.
- All Non-Compliance activity will be treated as per NHSRC Policy.
- Action will be taken by head of the organization.
- NHSRC follows the regulation of autonomous bodies as per GOI.

Introduction:

The NHSRC IT Policy and procedure manual provides the policies & procedures for selection and use of information technology within the institution which must be followed by all personnel.
It also provides guidelines to administer these policies & the correct procedure to follow.

NHSRC will keep all IT policies current and relevant. Therefore, from time to time it will be necessary to modify and amend some sections of the policies and procedures, or to add new procedures. Any suggestions, recommendations or feedback on the policies and procedures specified in this manual are welcome. These policies and procedures apply to all NHSRC Personnel.

1. Communication Policy (External)

1. Internet Usage Policy

Objective

The Internet Usage Policy provides guidelines for acceptable use of the organization's Internet network so as to devote Internet usage to enhance work productivity and efficiency and ensure safety and security of the Internet network, organizational data and the employees.

General Guidelines

- ✓ Internet is a paid resource and therefore shall be used only for office work.
- ✓ The organization reserves the right to monitor, examine, block or delete any/all incoming or outgoing internet connections on the organization's network.
- ✓ The organization has systems in place to monitor and record all Internet usage on the organization's network including each website visit, and each email sent or received. The IT Section can choose to analyse Internet usage and publicize the data at any time to assure Internet usage is as per the IT Policy.
- ✓ The organization has installed an Internet Firewall to assure safety and security of the organizational network. Any individual who attempts to disable, defeat, circumvent or bypass the Firewall will be subject to strict disciplinary action.

Internet Login Guidelines

- ✓ All individuals will be assigned a dynamic local IP address for internet & intranet use and will be responsible for the internet usage through this local dynamic IP (captured with Mac Address).
- ✓ Wireless network is also provided by the organization (subject to unavailability of LAN Connection).
- ✓ For wireless network, password for new personnel must be requested by the individuals or respective division.
- ✓ Sharing the Username and Password with another personnel, visitor or guest user is prohibited.
    - A visitor or guest user who wants to use the office Internet will be given a Guest Username and Password.

- Any password security breach must be notified to the IT Section immediately.
- Username and password allotted to an individual will be deleted upon resignation/termination/retirement from the organization.

Password Guidelines

The following password guidelines can be followed to ensure maximum password safety.

Select a Good Password:

- ✓ Choose a password which does not contain easily identifiable words (e.g. your username, name, phone number, house location etc.).
- ✓ Use 8 or more characters.
- ✓ Use at least one numeric and one special character apart from letters.
- ✓ Combine multiple unrelated words to make a password.

Keep your Password Safe:

- ✓ Do not share your password with anyone.
- ✓ Make sure no one is observing you while you enter your password.
- ✓ As far as possible, do not write down your password. If want to write it down, do not display it in a publicly visible area.
- ✓ Change your password periodically (every 3 months is recommended).
- ✓ Do not reuse old passwords. If that is difficult, do not repeat the last 5 passwords.

Other Security Measures:

- ✓ Ensure your computer is reasonably secure in your absence.
- ✓ Lock your monitor screen, log out or turn off your computer when not at desk.

Online Content Usage Guidelines:

- ✓ Employees are solely responsible for the content accessed and downloaded using Internet facility in the office. If they accidentally connect to a website containing material prohibited by the organization, they should disconnect from that site immediately.
- ✓ During office hours, employees are expected to spend limited time to access news, social media and other websites online, unless explicitly required for office work.
- ✓ Employees are not allowed to use Internet for non-official purposes using the Internet facility in office.
- ✓ Employees should schedule bandwidth-intensive tasks like large file transfers, video downloads, mass e-mailing etc. for off-peak times.

Use of social media:

Scope

- This applies to all staff employed, or third parties engaged by, or on behalf of NHSRC in relation to the use of social media for organization.

Social media is defined as any type of interactive online media that allows parties to communicate instantly with each other or to share data in a public or internal forum. This constantly changing area includes (but is not limited to):

- Online social forums such as Twitter; Facebook; Google+, LinkedIn, Instagram and Snapchat.
- Blogs, videos and image-sharing websites such as YouTube and Flickr
- Messaging technologies such as WhatsApp, Telegram, Skype for Organization

These procedures should be followed in relation to any social media used to promote good practice; protect organization and its staff and to promote the effective and innovative use of social media as part of official activities.

Staff: responsibilities -

- ✓ Should not use social media websites to criticize NHSRC, or any staff members, or third parties.
- ✓ Should not use social media websites to abuse, harass staff members, or any other third parties.
- ✓ All staff must remember not to post any comment, or image that would bring the organization into disrepute, or give cause for a third party to consider taking legal action.
- ✓ Must not place information pertaining to, or upload image(s) of staff to any web site without the prior consent being obtained from the staff in question.

Inappropriate Use

The following activities are prohibited on organization's Internet network. This list can be modified/updated anytime by the IT Section as deemed fit. Any disciplinary action considered appropriate by the IT Section (including legal action or termination) can be taken against an employee involved in the activities mentioned below:

- Playing online games, downloading and/or watching games, videos or entertainment software or engaging in any online activity which compromises the network speed and consumes unnecessary Internet bandwidth.
- Downloading images, videos and documents unless required to official work Accessing, displaying, uploading, downloading, storing, recording or distributing any kind of pornographic or sexually explicit material unless explicitly required for office work.
- Accessing pirated software, tools or data using the official network or systems.
- Uploading or distributing software, documents or any other material owned by the organization online without the explicit permission of the IT Section.
- Engaging in any criminal or illegal activity or violating law.
- Invading privacy of coworkers.
- Using the Internet for personal financial gain or for conducting personal business.
- Deliberately engaging in an online activity which hampers the safety & security of the data, equipment and people involved.
- Carrying out any objectionable, frivolous or illegal activity on the Internet that shall damage the organization's reputation.

2. Email & Chat Policy

Objective

This policy provides information about acceptable usage, ownership, confidentiality and security while using electronic messaging systems and chat platforms provided or approved by the organization. The policy applies to all electronic messages sent or received via the above-mentioned messaging systems and chat platforms by all personnel of the organization.

General Guidelines

- ✓ The organization reserves the right to approve or disapprove which electronic messaging systems and chat platforms would be used for official purposes. It is strictly advised to use the pre-approved messaging systems and platforms for office use only.
- ✓ An individual who, upon joining the organization, is provided with an official email address should use it for official purposes only.
- ✓ Any email security breach must be notified to the IT Section immediately.
- ✓ Upon termination, resignation or retirement from the organization, the organization will deny all access to electronic messaging platforms owned/provided by the organization.
- ✓ All messages composed and/or sent using the pre-approved messaging systems and platforms need to comply with the company policies of acceptable communication.
- ✓ Electronic mails and messages should be sent after careful consideration since they are inadequate in conveying the mood and context of the situation or sender and might be interpreted wrongly.
- ✓ All email signatures must have name and designation of individuals.

Ownership

- ✓ The official electronic messaging system used by the organization is the property of the organization and not the employee. All emails, chats and electronic messages stored, composed, sent and received by any individual in the official electronic messaging systems are the property of the organization.
- ✓ The organization reserves the right to intercept, monitor, read and disclose any messages stored, composed, sent or received using the official electronic messaging systems.
- ✓ The organization reserves the right to alter, modify, re-route or block messages as deemed appropriate.
- ✓ IT Section can change the email system password and monitor email usage of any individual for security purposes.

Confidentiality

- ✓ Proprietary, confidential and sensitive information about the organization or its personnel should not be exchanged via electronic messaging systems unless pre-approved by the reporting advisor (s) and/or the IT Section.
- ✓ Caution and proper judgment should be used to decide whether to deliver a message in person, on phone or via email/electronic messaging systems.

- ✓ Before composing or sending any message, it should be noted that electronic messages can be used as evidence in a court of law.
- ✓ Unauthorized copying and distributing of copyrighted content of the organization is prohibited.

Email Security:

Anti-virus:

- ✓ Anti-virus software pre-approved by the IT Team, should be installed in the laptop/desktop provided to new personnel after joining the organization.
- ✓ All individual in the organization are expected to make sure they have anti- virus software installed in their laptops/desktops (personal or official) used for office work.
- ✓ Organization will bear responsibility for providing, installing, updating and maintaining records for one anti-virus per individual at a time for the official laptop provided by the organization. The individual is responsible for installing good quality anti-virus software in their personal laptop/desktop used for office work
- ✓ Employees are prohibited from disabling the anti-virus software on organization-provided laptops/desktops.
- ✓ Employees should make sure their anti-virus is regularly updated and not out of date.

Safe Email Usage:

Following precautions must be taken to maintain email security:

- ✓ Do not to open emails and/or attachments from unknown or suspicious sources unless anticipated by you.
- ✓ In case of doubts about emails/ attachments from known senders, confirm from them about the legitimacy of the email/attachment.
- ✓ Use Email spam filters to filter out spam emails.

Inappropriate Use

- ✓ Official Email platforms or electronic messaging systems including but not limited to chat platforms and instant messaging systems should not be used to send messages containing pornographic, defamatory, derogatory, sexual, racist, harassing or offensive material.
- ✓ Official Email platforms or electronic messaging systems should not be used for personal work, personal gain or the promotion or publication of one's religious, social or political views.
- ✓ Spam/ bulk/junk messages should not be forwarded or sent to anyone from the official email ID unless for an officially approved purpose.

3. Phone Usage Policy (Local/STD/ISD)

- ✓ Landline phone systems are installed in the organization's workstations to communicate internally with others and to make external calls (long distance i.e. STD), reception staff may be informed.
- ✓ The landline phones should be strictly used to conduct official work only. As far as possible, no personal calls should be made using landline phones owned by the organization.
- ✓ Long distance calls should be made after careful consideration since they incur significant costs to the organization.
- ✓ The IT Section is responsible for maintaining telephone connections in offices. For any problems related to telephones, IT Section should be contacted.
- ✓ NHSRC Personnel should remember to follow telephone etiquette and be courteous while representing themselves and the organization using the organization's phone services.

4. Data Card Policy

- ✓ Each division to be provided with appropriately proportionate numbered data cards for field/site supporting on returnable basis.
- ✓ All the data cards will be post-paid and managed by IT Section
- ✓ Record of the same will be kept by division for divisional issuance as well as by IT Section for overall issuance.

2. Communication Policy (Internal)

Phone Usage Policy (Internal)

- Landline phone systems are installed in the organization's workstations to communicate internally with others and to make external calls (long distance i.e. STD), reception staff may be informed.
- The landline phones should be strictly used to conduct official work only. As far as possible, no personal calls should be made using landline phones owned by the organization.
- Long distance calls should be made after careful consideration since they incur significant costs to the organization.
- The IT Section is responsible for maintaining telephone connections in offices. For any problems related to telephones, IT Section should be contacted.
- NHSRC Personnel should remember to follow telephone etiquette and be courteous while representing themselves and the organization using the organization's phone services.

Storge Area Network

The Protocol for the use of these servers is as follows: -

- All systems (Laptop/Desktop) used by NHSRC personnel should be in the domain nhsrc.org.
- IP address will be assigned to all the systems through the domain server, other than the Printers.
- Static IP address of same range will be assigned to the Printers.
- Folders will be created at the storage server. The accessibility to the folders will be restricted as per details tabulated below: -

Sl. No.	Folders in Storage Server	Permission
1	One folder for each user in the name of user	Accessible to individual and respective division head
2	One folder for each Division in the name of Division	Accessible to all the members of respective Division

- The above-mentioned folders will be mapped as 'Network Drive' with the systems i.e. Laptop/Desktop.
- The Executive Director, NHSRC would have permissions to access all the folders through remote access of the server. PAO, NHSRC would have permissions to access Admin, HR, and Accounts and IT folders.

3. NHSRC Asset Policy

1. IT Asset Policy (Hardware)

Objective

The Equipment Usage policy informs NHSRC Personnel about equipment purchase, organizational level inventory IT, rules for allocating & transferring equipment to NHSRC Personnel, Sections or projects and best practices for all equipment usage and maintenance.

Equipment/ Service Purchase

- The following equipment is purchased by the organization and provided to individual, Sections or projects for their official use. The list can be modified as and when required.
  - Personal Computing Devices (Desktop, Laptop, Tablet)
  - Computer Peripherals (Printer, Scanner, Photocopier, Fax Machine, Keyboard, Mouse, Web Camera, Speaker, Modem etc.)
  - Networking Equipment & Supplies (Router, Switch, Antenna, Wiring, etc.)
  - Cell phones
  - Biometric Devices

- Physical Servers/Cloud Servers: purchases with valid licence for official uses

- To acquire new equipment for official use, it is imperative to adhere to the procedures and guidelines set forth by the GOI. The IT Section will be responsible for purchasing all approved equipment, unless otherwise notified or authorized.

- Cloud Hosting Servers are obtained from data centres of cloud Service providers (CSPs) that have been empanelled by MeitY, in accordance with the MeitY Procurement Guideline. MeitY has empanelled the Cloud Service offerings of leading CSPs to simplify the process of Cloud procurement for Government Sections. Current Cloud guidelines by MeitY for more information is used as a reference. The IT Section will maintain a small inventory of standard PCs, software and equipment required frequently to minimize delay in fulfilling critical orders.

- Portal services along with software requirement as per programmatic need of different division are outsourced as per Government norms. Monitoring is done by the concerned division. IT Section shall support the user division for smooth functioning.

Inventory IT

- The IT Section is responsible for maintaining an accurate inventory of all technological assets, software and tangible equipment purchased by the organization.

- The following information is to be maintained for above mentioned assets in an Inventory Sheet:
  - Item
  - Brand/ Company Name

- Serial Number
- Basic Configuration (e.g. i5 Laptop, 500 GB SSD, 8 GB RAM etc.)
- Physical Location
- Date of Purchase
- Purchase Cost
- Current Person In-Charge

- Proper information about all technological assets provided to a specific Section, project or centre must be regularly maintained in their respective Inventory Sheets by an assigned coordinator from that Section, project or centre on a regular basis. The information thus maintained must be shared with the Procurement Section as and when requested.
- When an Inventory Sheet is updated or modified, the previous version of the document should be retained. The date of modification should be mentioned in the sheet.
- All technological assets of the organization must be physically tagged with codes for easy identification.
- Periodic inventory audits will be carried out by the IT Section to validate the inventory and make sure all assets are up-to-date and in proper working condition as required for maximum efficiency and productivity.

Equipment Allocation, De-allocation & Relocation

Allocation of Assets:

- New Personnel i.e. Consultant/Sr. Consultant/Advisor may be allocated an existing personal computer (desktop or laptop) for office work on the Day of Joining (if procurement required, after procurement)
- If required, personnel can request their Reporting Advisor(s) for additional equipment or supplies like external keyboard, mouse etc.
- Allocation of additional assets to personnel is at the sole discretion of the Reporting Advisor (s).
- No personnel are allowed to carry official electronic devices out of office without permission from Reporting Advisor (s).

De-allocation of Assets:

- It is the Reporting Advisor's responsibility to collect all allocated organizational equipment & other assets from the personnel who is leaving the organization.
- Updating the Inventory Sheet is mandatory after receiving back all allocated equipment.
- The received assets must be returned to the IT Section by individual. (Clearance must be taken from the IT Section on their clearance form)

Bring Your Own Device (BYOD)

- ✓ Personal mobile devices for organizational uses involves employees registering their devices with the IT Section.
- ✓ IT Team will then record the device and all applications used by it.
- ✓ Personal mobile devices can only be used for specific organizational purposes such as email access, organization internet access, and communication.
- ✓ Employees who use personal mobile devices agree not to download or transfer any sensitive information to the device and not to use it as the sole repository for NHSRC's information.
- ✓ They must also make every reasonable effort to ensure that NHSRC's information is not compromised through the use of mobile equipment in public places.
- ✓ The device must be password protected and maintained with the latest operating software and security software. Employees must not share the device with others and must notify NHSRC immediately in case of loss or theft. They must not connect USB memory sticks from an untrusted or unknown source to NHSRC's equipment.
- ✓ All employees who have a registered personal mobile device for organizational use acknowledge that the organization owns all intellectual property created on the device, can access all data held on the device, and will regularly back up data held on the device.
- ✓ The organization will delete all data held on the device in case of loss or theft and has the first right to buy the device if the employee wants to sell it.
- ✓ The organization will also delete all data held on the device upon termination of the employee, but the terminated employee can request personal data be reinstated from backup data.
- ✓ The organization has the right to deregister the device.

Equipment Usage, Maintenance and Security

- ✓ It is the responsibility of all individuals to ensure careful, safe and judicious use of the equipment & other assets allocated to and/or being used by them.
- ✓ Proper guidelines or safety information must be obtained from designated staff in the IT Section before operating any equipment for the first time.
- ✓ Any observed malfunction, error, fault or problem while operating any equipment owned by the organization or assigned to you must be immediately informed to the designated staff in IT Section
- ✓ Any repeated occurrences of improper or careless use, wastage of supplies or any such offense compromising the safety or health of the equipment and people using them will be subject to disciplinary action.
- ✓ If officially assigned computing device is malfunctioning or underperforming and needs to be replaced or repaired, then written approval from respective Reporting Advisor is required for the same. The malfunctioning device needs to be submitted to the IT Section for checking, maintenance or repair. The IT Section personnel will give a time estimate for repair/maintenance.
- ✓ The Reporting Advisor can be informed about excessive delay or dissatisfaction about the repair or maintenance performed by the IT Section The issue will then be resolved by the Reporting Head in consultation with the IT Section. The IT Section head can be consulted in terms of serious disputes or unresolved issues.

2. Software Usage Policy

Objective

The Software Usage Policy is defined to provide guidelines for appropriate installation, usage and maintenance of software products installed in organization-owned computers.

General Guidelines:

- ✓ Third-party software (free as well as purchased) required for day-to-day work will be pre- installed onto all systems before handing them over to individuals. IT Section can be contacted to add to/delete from the list of pre-installed software on organizational computers.
- ✓ No other third-party software – free or licensed can be installed onto a computer system owned or provided to an employee by the organization, without prior approval of the IT Section
- ✓ To request installation of software onto a personal computing device, an employee needs to send a written request via the IT Ticket System or IT Support Email.
- ✓ Any software developed & copyrighted by the organization belongs to the organization. Any unauthorized use, storage, duplication or distribution of such software is illegal and subject to strict disciplinary action.

Applicability & Compliance

- ✓ No employee is allowed to install pirated software on official computing systems.
- ✓ Software purchased by the organization or installed on organizational computer systems must be used within the terms of its license agreement.
- ✓ Any duplication, illegal reproduction or unauthorized creation, use and distribution of licensed software within or outside the organization is strictly prohibited. Any such act will be subject to strict disciplinary action.
- ✓ The Procurement Section procedures & guidelines need to be followed to purchase new software (commercial or shareware) for official purposes.
- ✓ All approved software will be purchased through the IT Section, unless informed/permitted otherwise.
- ✓ Any individual who notices misuse or improper use of software within the organization must inform his/her Reporting Manager(s).

Software Registration:

- ✓ Software licensed or purchased by the organization must be registered in the name of the organization with the Job Role or Section in which it will be used and not in the name of an individual.
- ✓ After proper registration, the software may be installed as per the Software Usage Policy of the organization. A copy of all license agreements must be maintained by the IT Section
- ✓ After installation, all original installation media (CDs, DVDs, etc.) must be safely stored in a designated location by the IT Section

4. Information Security Policy

Objective

Information security means protection of the organization's data, applications, networks and computer systems from unauthorized access, alteration and Disposal. The Information Security Policy provides guidelines to protect data integrity based on data classification and secure the organization's information systems.

General Guidelines:

- ✓ Various methods like access control, authentication, monitoring and review should be used to ensure data security in the organization.
- ✓ Security reviews of servers, firewalls, routers and monitoring systems must be conducted on a regular basis. These reviews should include monitoring of access logs and intrusion detection software logs.
- ✓ Appropriate training must be provided to data owners, data users, and network & system administrators to ensure data security.

Data Classification

The organization classifies data into three categories:

High Risk:

It includes information assets which have legal requirements for disclosure and financial penalties imposed for disclosure. E.g. Payroll, personnel, financial, biometric data

Medium Risk:

It includes confidential data which would not impose losses on the organization if disclosed but is also not publicly available. E.g. Agreement documents, unpublished reports, etc.

Low Risk:

It includes information that can be freely disseminated E.g. brochures, published reports, other printed material etc.

- Different protection strategies developed by the IT Section for the above three data categories. Information about the same must be disseminated appropriately to all relevant Sections and staff.
- High risk data must be encrypted when transmitted over insecure channels.
- All data must be backed up on a regular basis as per the rules defined by the IT Section at that time.

Access Control

- ✓ Access to the network, servers and systems in the organization be achieved by individual logins and it require authentication. Authentication includes the use of passwords, biometrics or other recognized forms of authentication.

- ✓ All users of systems which contain high or medium risk data must have a strong password as defined in the IT Policy.
- ✓ Default passwords on all systems must be changed after installation.
- ✓ Where possible and financially feasible, more than one person must have full rights to any organization-owned server storing or transmitting high risk and medium risk data.

Virus Prevention

- ✓ Virus prevention for personal computers and email usage has been described previously.
- ✓ Apart from that, all servers and workstations that connect to the network must be protected with licensed anti-virus software recommended by the vendor. The software must be kept up-to-date.
- ✓ Whenever feasible, system/network administrators must inform users when a virus/ other vulnerability has been detected in the network or systems.

Intrusion Detection

- ✓ Intrusion detection must be implemented on all servers and workstations containing high and medium risk data.
- ✓ Operating system and application software logging process must be enabled on all systems.
- ✓ Server, firewall and critical system logs must be reviewed frequently.

Data Collection

- ✓ Due consent of the division and owner must be taken for any kind of data collection for publishing/ uploading/ streaming.

5. IT Support / Help Desk

IT Support on Official Systems

- NHSRC uses an online Ticket System/IT System to provide IT Support to its personnel. The URL for the same is https://docs.google.com/spreadsheets/d/1- eKsUeIXK6Gul0-0eTFxACJwneH-MJtHi_D-HxYJa8/edit#gid=82309965
- NHSRC personnel may need hardware/software installations or may face technological issues which cannot be resolved on their own. Personnel are expected to get help from the IT Section for such issues via the Ticket System or the IT Support Email ID also.
- Any IT Support work informed or assigned via emails sent on Personnel's private email IDs, chats or any other media except the Ticket System or the IT Support Email ID would be not entertained.
- For the sake of quick understanding, NHSRC Personnel are expected to provide details of their issue or help required in the Ticket raised or Support Email sent.
- For major issues like PC replacement, non-working equipment, installation of application software and more, it is mandatory for all Personnel to inform the IT Section
- For any damage to Computers issued by NHSRC, approval from Reporting Advisor would be required for PC replacements.
- After raising a ticket in the Ticket System, employees should expect a reply from the IT Section within 1 working day. The IT Section may ask the employee to deposit the problematic equipment to the IT Section for checking and will inform the timeline for repair/maintenance/troubleshooting/installations or the required work.
- If there is no response in 1 working day, then the IT Section Designated Staff should be asked for an explanation for the delay. If no response is obtained in 3 working days, a complaint can be raised through an email to the employee's Reporting Advisor/PAO and IT Section Designated Staff.
- Tickets will be resolved on a First-Come-First-Served basis. However, the priority can be changed on request at the sole discretion of the designated team in IT Section

IT Support on Personal Systems

Objective

The main aim of this policy is to maintain standard configurations of PC hardware and software purchased for the use of organization work. The hardware standards will help maintain optimum work productivity, computer health & security and provide timely and effective support in troubleshooting PC problems. The software standards will ensure better system administration, effective tracking of software licenses and efficient technical support.

General Guidelines

- ✓ It is the responsibility of the Individual to establish and maintain standard configurations of hardware and software for PCs
- ✓ The standard, can however, be modified at any point in time as required by the IT Section in consultation with the IT Section.

- ✓ Multiple configurations are maintained as per the different requirements of various Sections and projects in the organization, in consultation with the Section/Project Head.
- ✓ Only in exceptional cases, when none of the standard configurations satisfy the work requirements, can an individual request a non-standard PC configuration. Valid reasons need to be provided for the request and written approval of the Reporting advisor (s) is required for the same.

Network Access

- ✓ All Systems being used in the organization are enabled to connect to the Organization's Local Area Network as well as the Internet.
- ✓ Network security is enabled in all Systems through Firewall, Web Security and Email Security software.
- ✓ Individual are expected to undertake appropriate security measures as enlisted in the IT Policy.

Data Backup Procedure

Data Backup is setup during installation of Operating System in a PC. As an additional security measure, it is advised that individual keeps important official data in some external storage device also.

File Backup System:

- For backing up the data, file server is installed for all personnel. All individuals are expected to keep official data on the file system.
- Individuals' Reporting advisor or the IT Section or IT Manager will have access to that data.
- All personal will login to the file server through ADDC* user ID and password.

Server backup:

- IT Section is expected to maintain an incremental backup of all servers with at least 3 copies of all servers. At any time, backups of all servers must be maintained for one week.
- Replica mode of all running servers will be offline, and it should maintain half- hourly backup.
- The hard disk of every server should be in the Red5 mode.

ADDC - Active Directory Domain Controller

Antivirus Software

- ✓ Approved licensed antivirus software is installed on all PCs owned by the organization.
- ✓ Employees are expected to make sure their Antivirus is updated regularly. The IT Section should be informed if the Antivirus expires/unavailable.
- ✓ Any external storage device like pen drive or hard disk connected to the PC needs to be completely scanned by the Antivirus software before opening it and copying files to/from the device.

PC Support

- ✓ Guidance and tips given by the IT Section designated staff for maintaining the PC should be remembered while using a PC.
- ✓ The IT Section should be contacted via the IT Support Ticket System or IT Support Email id for any assistance with your PC hardware or software.
- ✓ Technical support will not be provided for hardware devices or software which are illegal or not included in the standard hardware/software list developed by the IT Section
- ✓ Software applications evaluated by the IT Section to cause problems with the organization's PCs, will be removed.

6. Data Retention and Disposal Policy

Data Retention:

NHSRC IT Policy must comply with Section of Administrative Reforms' policy on Record Retention Schedule in respect of records which is common to All Ministries/ Sections of GoI with all its amendments.

For Electronic Records** - e-Files/records may be digitized any one of the categories:

Category-I (e-Files/records to preserved permanently on which are of historical importance) – For 10 years, it will be kept in the Section 's severs and thereafter transferred to the server of the National Archives of India.

Category –II (e-Files/records of secondary importance and have a reference value for a limited period) – 10 years on the Section 's server. In exceptional cases, if the record is required to be retained beyond 10 years it will be upgraded to Category-I.

* From the paragraph No.105 of the Central Secretariat Manual of Office Procedure.
** From the paragraph No.92 of the Central Secretariat Manual of e-Office Procedure.

For Website data record:

All outdated Announcements, Tenders, Recruitment notices, News and Press Releases are removed after the expiry date set out from the website and/or placed into the archives section.

Data Disposal

Disposal is defined as physical or technical disposal, sufficient to render the information contained in the document irretrievable by ordinary commercially available means.

Once records have been archived for the applicable period set forth in this policy, the same shall be prepared for disposal, subject to request from the Section and necessary approval as stated in the data.

Disposal matrix given below -

Reason of destruction	Requestor	Approver	Authorizer
Conversion of physical record to electronic at the start, in between or end of the retention period			
Permanent disposal of records at the end of archival period - electronic records			
Permanent Disposal of records at the end of archival period - physical records			

Document Disposal guidelines:

- NHSRC shall enforce approved Disposal practices, appropriate for each type of information archived, whether in physical storage media such as CD-ROMs, DVDs, backup tapes, hard drives, mobile devices, portable drives or in database records or backup files. IT hardware, including servers, desktops and other IT peripherals, network devices, optical media like CDs/ DVDs, magnetic tape media, printer consumables, etc. may be physically damaged or degaussed and handed over to concerned E-waste vendors (As per CPCB Guideline of prevalent rules).

- The details of the documents destroyed by the Section shall be recorded in a register or a report to be maintained by the respective Section, wherein brief particulars of the documents destroyed shall be entered, including but not limited to the following details:
    - Name of Record
    - Form of document
    - Particulars of the document
    - Month and Year in which record was created
    - Date of Disposal
    - Mode of Disposal
    - Requestor and request date
    - Approver and approval date
    - Authorizer and authorization date.

7. IT Audit Procedure

IT audit will be done by auditors engaged for the same with a frequency of at least once in a year with maintaining confidentiality, integrity, and availability for below mentioned items.

Hardware Audit

- The IT Section will conduct periodic audit of all the hardware installed in all NHSRC-owned systems to make sure all compliances are being met as per IT policy.
- Prior notice may be provided by the IT Section before conducting the Hardware Audit.
- During this audit, the IT Section will also make sure that the physically cleaned and all the parts of the systems are working properly.
- The full cooperation of all individuals is required during such audits.

Software Audit

- The IT Section will conduct periodic audit of software installed in NHSRC owned systems to make sure all compliances are being met as per IT policy.
- Prior notice may or may not be provided by the IT Section before conducting the Software Audit.
- During this audit, the IT Section will also make sure the all the applications installed are genuine and up to date, backup is being done, patches are installed and malfunctional software must be un-installed.
- The full cooperation of all individuals is required during such audits.

Security system Audit

- The IT Section will conduct periodic audit of Security Systems in place/installed in all NHSRC owned systems to make sure all compliances are being met as per IT policy
- Prior notice may or may not be provided by the IT Section before conducting the Software Audit.
- During this audit, the IT Section will also make sure the anti-virus is updated, the system is scanned and cleaned, and the computer is free of garbage data, viruses, worms, or other harmful programmatic codes.
- The full cooperation of all individuals is required during such audits.

Web Security Audit

- It is mandatory for all web portals that are developed to have SSL installation and undergo security auditing by a Certi-IN empanelled agency. This is in accordance with the Guidelines for Indian Government Websites (GIGW). For further information, please refer to the guidelines.

Audit Report

- Separate audit report of each system may be generated.
- All the Audit Report should be shared by IT Section to PAO, NHSRC for input and appropriate direction may be taken to fulfil the gaps and short comings.
- This report must be kept with IT Section for reference.

Action Plan

- Based on the Audit report generated, action plan may be developed to closer of gap.

8. Training of Staff on Information management procedure

Training of staff is one of the essential activities to ensure quality & effective management of information generated during the process. It is conducted on regular basis for all staff. The following guidelines need to be followed:

- For all the new joiners, monthly induction session to be planned commensuration with HR Induction program.
- All the IT personnel should be nominated to enhance their individual knowledge and skills by HR section.
- All the IT personnel should get training to use any devices or software/application developed or installed to get idea to operate the same.

Education and awareness programs are carried out throughout the year and are designed to educate users on security best practices and their role in protecting organization systems and data. Advanced levels of training may be required by different divisions for certain specific functions, roles or responsibilities. IT Section facilitate specific training requirement as per user Section

Education and awareness program content covers but is not limited to the following areas:

- Acceptable use of organization's computing and information assets.
- Identifying and reporting phishing (and other forms of social engineering).
- Information security and policy governance essentials.
- Role-based security awareness education.
- Ethics and compliance.
- Workplace safety.
- Records and information management.

9. Procedure for uploading of data in public domain

Websites (NHSRC/MoHFW):

Data Collection:

- With due consent of the division/owner only, any data get uploaded to any Platform.

Data Upload:

- All the data gets uploaded on NHSRC website after due approval of ED NHSRC.
- All the data which requires upload on MoHFW website, it first uploaded on NHSRC Website and link of the content sent to NIC with Mata data form approved by JS.

I-got (diksha.gov.in)

Data Collection:

- With due consent of the division/owner only, any data get uploaded to any Platform.

Data Upload

- All the data on diksha.gov.in website gets uploaded after due approval of ED NHSRC.
- All the upload, after due approval from concern JS, it then forwarded to concern JS for upload on diksha.gov.in.

YouTube Channel

Data Collection:

- With due consent of the division/owner only, any data get uploaded to any Platform.

Data Upload:

- All the data gets uploaded on NHSRC YouTube Channel after due approval of ED NHSRC.
- Developed Content from Division, it needs to be forwarded to Publication Unit for Uploading on NHSRC YouTube Channel.

10. Guidelines for condemnation & disposal of IT Equipment

This policy is based on Section of telecommunication Condemnation Policy.

Applicability

These guidelines will be applicable to all IT equipment's installed in NHSRC. and include the following items:

- Servers
- PCs
- Dumb Terminals
- Printers
- UPS
- Laptop/Note-book/tablet
- Data Communication Equipment LAN switches/routers/data cables.

Note:

- Consumable items related to IT like used printer cartridges etc. are not included in the scope of scrapping on account of the fact of its nature as consumable.
- IT items like pen drives/floppies, which are petty valued and are not capitalized, are not qualified for the detailed scrapping procedure.

Grounds for condemnation:

The IT equipment can be condemned on following grounds:

- Equipment outlived its prescribed life and certified by IT Wing as unfit for its useful contribution. The prescribed life of various IT equipment is as following
  - Servers PC's/dumb terminals/printers- 5 years
  - Laptop/Note-book- 4 years or till the fitness of such device is· certified by NIC of the ministry/Section, whichever is later.
  - UPS excluding battery- 5 years
  - Battery of UPS~ 1 year after warranty period.
  - Printers - 5 years
  - Software do not require any physical scrapping.
  - Data Communication Equipment LAN switches/routers/data cables 5 years.

- Equipment which has become obsolete technology-wise and can't be upgraded and support from vendor either paid or unpaid does not exist and their use may result in security threat/ unauthorized access to data.

- Beyond economical repair: When repair cost is considered too high (exceeding 50% of residual value of equipment taking depreciation into account), and the age of the equipment. Such cases should be dealt on case-to-case basis and should have concurrence of finance. In case of IT equipment's, a depreciation of 20% per year may be taken for calculation of residual value.

- Equipment that has been damaged due to fire or any other unforeseen reason and have been certified as beyond repair by the authorized service agency and agreed upon by the IT Wing of DoT.

Disposal:

IT equipment shall be disposed strictly following the procedure as laid down in GFR 2017 and notification regarding disposal of E-Waste issued by Ministry of environment and forests. Once the equipment has been condemned it should be removed from office use and kept in the area allocated for scrapped equipment. Section will also ensure removal of service and inventory labels from such equipment. AMC, if any, for such equipment's/instruments should be stopped with the effective date of scrapping. All data including operating system must be removed after taking proper backup and preserved by user of the equipment.

Procedure:

- ✓ IT Section will be the nodal section for all the IT equipment procured. It will prepare and maintain assets' register for the same. However, individual section will also be provided with all the basic information.
- ✓ Scrapping proposal will be initiated by the user section which will be compiled by IT wing for further processing for scrapping.
- ✓ Section will constitute a condemnation committee which will review the condemnation notes and recommend about the condemnation of equipment as per approved guidelines. The committee should have at least one member from IT Section and one from the finance wing.
- ✓ All procedure and rules of the government on maintenance of records for condemnation of non- consumable items will be adhered to in these cases.
- ✓ The condemnation report so prepared shall be put up for approval. The condemnation will be done only after approval is obtained from competent authority having such powers to approve condemnation. It is suggested that such Scrapping Committee will meet once in a year during the months of May-June or Nov. - Dec. in order to avoid piling up of unusable IT items.

11. Feed Back System

Scope:

There is always a scope of improvement. Divisional feedback should be taken for improvement of the processes/workflows/risk cover/job description, based on feedback.

Frequency:

Frequency of feedback shall be at least once in a year.

Feedback review:

Review of feedback is for improvement in respective area. Each feedback shall be collated by Admin and then reviewed by ED/PAO/ IT Manager before changes are incorporated.