राष्ट्रीय हथकरघा विकास निगम लिमिटेड,

(भारत सरकार का उपक्रम, वस्त्र मंत्रालय)

वेगमैन्स बिजनेस पार्क, चतुर्थ तल, टावर-1, प्लाट नं.3, के.पी.-III, सूरजपुर-कासना मेन रोड,

ग्रेटर नोएडा – 201306

का.आ.सं:एनएचडीसी/एचआरएम/का.आ./23-24/179 दिनांक: 19/02/2024

कार्यालय - आदेश

Consequent upon the issuance of Comprehensive Guidelines on **"Policy on Use of IT Resources of Government of India"** by Ministry of Communications and Information Technology and **Laptop Policy - 2023** of National Handloom Development Corporation Ltd. and to streamline the working of the Corporation for better/optimal utilization of IT Resources, the following shall be applicable with immediate effect:-

i. IT Resources that are more than five to seven years old and can no longer be updated with the latest operating system and patches, shall be taken out of the system;

ii. Desktops of those employees, who have already been provided Laptop/tabs, will not be repaired/replaced further;

iii. All those employees, who have already been provided Laptops and are covered under new Laptop Policy, can purchase accessories as per their entitlement (Para 2.1.6 of Laptop Policy). The codal life of accessories will also be co-terminus with that of the Laptop.

2. MeitY's Guidelines vide F.No. 2(22)/2013-EG-II in October, 2014 are enclosed herewith for strict compliance.

This issues with the approval of Competent Authority.

(गौरव त्रिपाठी)
सहायक प्रबन्धक(मा.सं.)

प्रतिलिपि :

1. प्रबन्ध निदेशक कार्यालय
2. महाप्रबन्धक
3. उप महाप्रबन्धक (वि. एवं ले.)
4. समस्त क्षेत्रीय कार्यालय
5. सूचनापट्ट / मानव संसाधन विभाग

F. No. 2(22)/2013-EG-II
Ministry of Communication & Information Technology
Department of Electronics & Information Technology

सत्यमेव जयते

Policy on Use of IT Resources of Government of India

October 2014
Version 1.0

Department of Electronics and Information Technology
Ministry of Communications and Information Technology
Government of India
New Delhi – 110003

Contents

1. Introduction

1.1. Government provides IT resources to its employees to enhance their efficiency and productivity. These resources are meant as tools to access and process information related to their areas of work. These resources help Government officials to remain well informed and carry out their functions in an efficient and effective manner.

1.2. For the purpose of this policy, the term 'IT Resources' includes desktop devices, portable and mobile devices, networks including wireless networks, Internet connectivity, external storage devices and peripherals like printers and scanners and the software associated therewith.

1.3. Misuse of these resources can result in unwanted risk and liabilities for the Government. It is, therefore, expected that these resources are used primarily for Government related purposes and in a lawful and ethical way.

2. Scope

This policy governs the usage of IT Resources from an end user's [1] perspective.This policy is applicable to all employees of GoI and employees of those State/UT Governments that use the IT Resources of GoI and also those State/UT Governments that choose to adopt this policy in future

3. Objective

The objective of this policy is to ensure proper access to and usage of Government's IT resources and prevent their misuse by the users. Use of resources provided by Government of India implies the user's agreement to be governed by this policy.

4. Roles and Responsibilities

The following roles are required in each organization [2] using the Central / State / UT Government IT resources. The official identified for the task shall be responsible for the management of the IT resources deployed for the use of entire user base under their respective domain.

4.1. Competent Authority [3] as identified by each organization.

4.2. Designated Nodal Officer [4] as identified by each organization.

4.3. Implementing Agency [5]: The overall responsibility for Information Security will be that of the respective organization. In the interest of security of the network services, it is recommended that the organizations should use the GoI network services provided by NIC, in which case NIC would be the Implementing Agency for security of network services on behalf of the concerned organization. In organizations not using NIC network services, the respective organization will be the Implementing Agency.

4.4. The Nodal Agency [6] for managing all IT Resources except network services shall be the respective organization.

5. Access to the Network

5.1. Access to Internet and Intranet

a. A user shall register the client system and obtain one time approval from the competent authority before connecting the client system to the Government network.

b. It is strongly recommended that sensitive offices shall maintain two independent networks, i.e. Internet [7] and Intranet [8]. Both the networks shall not have any physical connection/devices between them. Users in such deployments shall have two access devices, i.e. desktops. One shall be connected to the internet and the other to the intranet. End point compliance [9] shall be implemented on both the networks to prevent unauthorised access to data.

c. Users shall not undertake any activity through any website or applications to bypass filtering of the network or perform any other unlawful acts which may harm the network's performance or security

5.2 Access to Government Wireless Networks

For connecting to a Government wireless [10] network, user shall ensure the following:

a. A user shall register the access device and obtain one time approval from the competent authority before connecting the access device to the Government wireless network.

b. Wireless client systems and wireless devices shall not be allowed to connect to the Government wireless access points without due authentication.

c. To ensure information security, it is recommended that users should not connect their devices to unsecured wireless networks.

5.3 Filtering and blocking of sites:

a. IA may block content over the Internet which is in contravention of the relevant provisions of the IT Act 2000 and other applicable laws or which may pose a security threat to the network.

b. IA may also block content which, in the opinion of the organization concerned, is inappropriate or may adversely affect the productivity of the users.

6. Monitoring and Privacy:

6.1 IA shall have the right to audit networks and systems at regular intervals, from the point of compliance to this policy.

6.2 IA/Nodal Agency, for security related reasons or for compliance with applicable laws, may access, review, copy or delete any kind of electronic communication or files stored on Government provided devices under intimation to the user. This includes items such as files, e-mails, and Internet history etc.

6.3 IA may monitor user's online activities on Government network, subject to such Standard Operating Procedures as the organization may lay down in this regard.

7. E-mail Access from the Government Network

7.1. Users shall refrain from using private e-mail servers from Government network.

7.2. E-mail service authorized by the Government and implemented by the IA shall only be used for all official correspondence. For personal correspondence, users may use the name-based e-mail id assigned to them on the Government authorized e-mail Service.

7.3. More details in this regard are provided in the "E-mail Policy of Government of India".

8. Access to Social Media Sites from Government Network

8.1 Use of social networking sites by Government organizations is governed by "Framework and Guidelines for use of Social Media [11] for Government Organizations" available at http://deity.gov.in.

8.2 User shall comply with all the applicable provisions under the IT Act 2000, while posting any data pertaining to the Government on social networking sites.

8.3 User shall adhere to the "Terms of Use" of the relevant social media platform/website, as well as copyright, privacy, defamation, contempt of court, discrimination, harassment and other applicable laws.

8.4 User shall report any suspicious incident as soon as possible to the competent authority.

8.5 User shall always use high security settings on social networking sites.

8.6 User shall not post any material that is offensive, threatening, obscene, infringes copyright, defamatory, hateful, harassing, bullying, discriminatory, racist, sexist, or is otherwise unlawful.

8.7 User shall not disclose or use any confidential information obtained in their capacity as an employee/contractor [12] of the organization.

8.8 User shall not make any comment or post any material that might otherwise cause damage to the organization's reputation.

9. Use of IT Devices Issued by Government of India

IT devices issued by the Government to a user shall be primarily used for Government related purposes and in a lawful and ethical way and shall be governed by the practices defined in the document **"Guidelines for Use of IT Devices on Government Network"** available at http://www.deity.gov.in/content/policiesguidelines/ under the caption "Policy on Use of IT Resources". The aforesaid document covers best practices related to use of desktop devices, portable devices, external storage media and peripherals devices such as printers and scanners.

10. Responsibility of User Organizations

10.1. Policy Compliance

a. All user organizations shall implement appropriate controls to ensure compliance with this policy by their users. Implementing Agency shall provide necessary support in this regard.

b. A periodic reporting mechanism to ensure the compliance of this policy shall be established by the competent authority of the organization.

c. Nodal Officer of the user organization shall ensure resolution of all incidents related to the security aspects of

this policy by their users. Implementing Agency shall provide the requisite support in this regard.

d. Competent Authority of the user organization shall ensure that training and awareness programs on use of IT resources are organized at regular intervals. Implementing Agency shall provide the required support in this regard.

e. User organization shall not install any network/security device on the network without consultation with the IA.

10.2. Policy Dissemination

a. Competent Authority of the user organization should ensure proper dissemination of this policy.

b. Competent Authority may use newsletters, banners, bulletin boards etc. to facilitate increased awareness about this policy amongst their users.

c. Orientation programs for new recruits shall include a session on this policy.

11. Security Incident Management Process

11.1 A security incident is defined as any adverse event that can impact the availability, integrity, confidentiality and authority of Government data.

11.2 IA reserves the right to deactivate/remove any device from the network if it is deemed as a threat and can lead to a compromise of a system under intimation to the competent authority of that organization.

11.3 Any security incident [13] noticed must immediately be brought to the notice of the Indian Computer Emergency Response Team (ICERT) and the IA.

12. Scrutiny/Release of logs

12.1 Notwithstanding anything in the above clause, the disclosure of logs relating to or contained in any IT Resource, to Law Enforcement agencies and other organizations by the IA shall be done as per the IT Act 2000 and other applicable laws.

12.2 IA shall neither accept nor act on the request from any other organization, save as provided in this clause, for scrutiny or release of logs.

13. Intellectual Property

Material accessible through the IA's network and resources may be subject to protection under privacy, publicity, or other personal rights and intellectual property rights, including but not limited to, copyrights and laws protecting patents, trademarks, trade secrets or other proprietary information. Users shall not use the Government network and resources in any manner that would infringe, dilute, misappropriate, or otherwise violate any such rights.

14. Enforcement

14.1 This policy is applicable to all employees of Central and State Governments as specified in clause 2 of this document. It is mandatory for all users to adhere to the provisions of this policy.

14.2 Each organization shall be responsible for ensuring compliance with the provisions of this policy. The Implementing Agency would provide necessary technical assistance to the organizations in this regard.

15. Deactivation

15.1. In case of any threat to security of the Government systems or network from the resources being used by a user, the resources being used may be deactivated immediately by the IA.

15.2. Subsequent to such deactivation, the concerned user and the competent authority of that organization shall be informed.

16. Audit of NIC Network Infrastructure

The security audit of NIC network infrastructure shall be conducted periodically by an organization approved by Deity.

17. Review

Future changes in this Policy, as deemed necessary, shall be made by DeitY with approval of the Minister of Communication & IT after due inter-ministerial consultations.

GLOSSARY

S no.	Term	Definition
1	**Users**	Refers to Government/State/UT employees/contractual employees who are accessing the Government services
2	**Organization**	Ministry/Department/Statutory Body/Autonomous body under Central and State Governments
3	**Competent Authority**	Officer responsible for taking and approving all decisions relating to this policy in his Organization
4.	**Nodal Officer**	Officer responsible for all matters relating to this policy who will coordinate on behalf of the Organization
5	**Implementing Agency (IA)**	A Body which will be responsible for ensuring compliance with this policy with reference to network services including power to take precautionary and penal actions as specified in this policy.
6	**Nodal Agency**	Respective organization responsible for ensuring compliance with this policy with respect to use of It resources except network services.
7	**Internet**	Internet is a network of the interlinked computer networking worldwide, which is accessible to the general public. These interconnected computers work by transmitting data through a special type of packet switching which is known as the IP or the internet protocol
8	**Intranet**	An intranet is a private network that is contained within an organization. For the purpose of this policy, computers connected to an intranet are not allowed to connect to internet.
9	**End point compliance**	End point compliance is an approach to network protection that requires each computing device on a network to comply with certain standards before network access is granted. Endpoints can include desktops, laptops, smart phones, tablets etc
10	**Wireless**	Any type of computer network that uses wireless data connections for connecting network nodes. For the purpose of this policy, all the GoI wireless networks will be deployed in a secure manner.

11	**Social Media**	Applies to social networking sites, blogs, electronic newsletters, online forums, social networking sites, and other services that permit users to share information with others in a contemporaneous manner.
12	**Contractor/contractual employees**	An employee who works under contract for GoI. A contract employee is hired for a specific job or assignment. A contract employee does not become a regular addition to the GoI staff and is not considered a permanent employee of GoI
13	**Security Incident**	Any adverse event which occurs on any part of the government data and results in security threat/breach of the data