National Cyber Security Policy -2013

Preamble

1. Cyberspace[1] is a complex environment consisting of interactions between people, software and services, supported by worldwide distribution of information and communication technology (ICT) devices and networks.

2. Owing to the numerous benefits brought about by technological advancements, the cyberspace today is a common pool used by citizens, businesses, critical information infrastructure, military and governments in a manner that makes it difficult to draw clear boundaries among these different groups. The cyberspace is expected to be more complex in the foreseeable future, with many fold increase in networks and devices connected to it.

3. Information Technology (IT) is one of the critical sectors that rides on and resides in cyberspace. It has emerged as one of the most significant growth catalysts for the Indian economy. In addition to fuelling India's economy, this sector is also positively influencing the lives of its people through direct and indirect contribution to the various socio-economic parameters such as employment, standard of living and diversity among others. The sector has played a significant role in transforming India's image to that of a global player in providing world-class technology solutions and IT business services. The government has been a key driver for increased adoption of IT-based products and IT enabled services in Public services (Government to citizen services, citizen identification, public distribution systems), Healthcare (telemedicine, remote consultation, mobile clinics), Education (e-Learning, virtual classrooms, etc) and Financial services (mobile banking / payment gateways), etc. Such initiatives have enabled increased IT adoption in the country through sectoral reforms and National programmes which have led to creation of large scale IT infrastructure with corporate / private participation.

4. In the light of the growth of IT sector in the country, ambitious plans for rapid social transformation & inclusive growth and India's prominent role in the IT global market, providing right kind of focus for creating secure computing environment and adequate trust & confidence in electronic transactions, software, services, devices and networks, has become one of the compelling priorities for the country. Such a focus enables creation of a suitable cyber security eco-system in the country, in tune with globally networked environment.

[1] ISO / IEC 27032-2012

5. Cyberspace is vulnerable to a wide variety of incidents, whether intentional or accidental, manmade or natural, and the data exchanged in the cyberspace can be exploited for nefarious purposes by both nation- states and non-state actors. Cyber attacks that target the infrastructure or underlying economic well-being of a nation state can effectively reduce available state resources and undermine confidence in their supporting structures. A cyber related incident of national significance may take any form; an organized cyber attack, an uncontrolled exploit such as computer virus or worms or any malicious software code, a national disaster with significant cyber consequences or other related incidents capable of causing extensive damage to the information infrastructure or key assets. Large-scale cyber incidents may overwhelm the government, public and private sector resources and services by disrupting functioning of critical information systems. Complications from disruptions of such a magnitude may threaten lives, economy and national security. Rapid identification, information exchange, investigation and coordinated response and remediation can mitigate the damage caused by malicious cyberspace activity. Some of the examples of cyber threats to individuals, businesses and government are identity theft, phishing, social engineering, hactivism, cyber terrorism, compound threats targeting mobile devices and smart phone, compromised digital certificates, advanced persistent threats, denial of service, bot nets, supply chain attacks, data leakage, etc. The protection of information infrastructure and preservation of the confidentiality, integrity and availability of information in cyberspace is the essence of a secure cyber space.

6. There are various ongoing activities and programs of the Government to address the cyber security challenges which have significantly contributed to the creation of a platform that is now capable of supporting and sustaining the efforts in securing the cyber space. Due to the dynamic nature of cyberspace, there is now a need for these actions to be unified under a **National Cyber Security Policy**, with an integrated vision and a set of sustained & coordinated strategies for implementation.

7. The cyber security policy is an evolving task and it caters to the whole spectrum of ICT users and providers including home users and small, medium and large enterprises and Government & non-Government entities. It serves as an umbrella framework for defining and guiding the actions related to security of cyberspace. It also enables the individual sectors and organizations in designing appropriate cyber security policies to suit their needs. The policy provides an overview of what it takes to effectively protect information, information systems & networks and also gives an insight into the Government's approach and strategy for protection of cyber space in the country. It also outlines some pointers to enable collaborative working of all key players in public & private to safeguard country's information and information systems. This policy, therefore, aims to create a cyber security framework, which leads to specific actions and programmes to enhance the security posture of country's cyber space.

I. Vision

To build a secure and resilient cyberspace for citizens, businesses and Government

II. Mission

To protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation.

III. Objectives

1) To create a secure cyber ecosystem in the country, generate adequate trust & confidence in IT systems and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy.

2) To create an assurance framework for design of security policies and for promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (product, process, technology & people).

3) To strengthen the Regulatory framework for ensuring a Secure Cyberspace ecosystem.

4) To enhance and create National and Sectoral level 24 x 7 mechanisms for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective, response and recovery actions.

5) To enhance the protection and resilience of Nation's critical information infrastructure by operating a 24x7 National Critical Information Infrastructure Protection Centre (NCIIPC) and mandating security practices related to the design, acquisition, development, use and operation of information resources.

6) To develop suitable indigenous security technologies through frontier technology research, solution oriented research, proof of concept, pilot development, transition, diffusion and commercialisation leading to widespread deployment of secure ICT products / processes in general and specifically for addressing National Security requirements.

7) To improve visibility of the integrity of ICT products and services by establishing infrastructure for testing & validation of security of such products.

8) To create a workforce of 500,000 professionals skilled in cyber security in the next 5 years through capacity building, skill development and training.

9) To provide fiscal benefits to businesses for adoption of standard security practices and processes.

10) To enable protection of information while in process, handling, storage & transit so as to safeguard privacy of citizen's data and for reducing economic losses due to cyber crime or data theft.

11) To enable effective prevention, investigation and prosecution of cyber crime and enhancement of law enforcement capabilities through appropriate legislative intervention.

12) To create a culture of cyber security and privacy enabling responsible user behaviour & actions through an effective communication and promotion strategy.

13) To develop effective public private partnerships and collaborative engagements through technical and operational cooperation and contribution for enhancing the security of cyberspace.

14) To enhance global cooperation by promoting shared understanding and leveraging relationships for furthering the cause of security of cyberspace.

IV. Strategies

A. Creating a secure cyber ecosystem

1) To designate a National nodal agency to coordinate all matters related to cyber security in the country, with clearly defined roles & responsibilities.

2) To encourage all organizations, private and public to designate a member of senior management, as Chief Information Security Officer (CISO), responsible for cyber security efforts and initiatives.

3) To encourage all organizations to develop information security policies duly integrated with their business plans and implement such policies as per international best practices. Such policies should include establishing standards and mechanisms for secure information flow (while in process, handling, storage & transit), crisis management plan, proactive security posture assessment and forensically enabled information infrastructure.

4) To ensure that all organizations earmark a specific budget for implementing cyber security initiatives and for meeting emergency response arising out of cyber incidents.

5) To provide fiscal schemes and incentives to encourage entities to install, strengthen and upgrade information infrastructure with respect to cyber security.

6) To prevent occurrence and recurrence of cyber incidents by way of incentives for technology development, cyber security compliance and proactive actions.

7) To establish a mechanism for sharing information and for identifying and responding to cyber security incidents and for cooperation in restoration efforts.

8) To encourage entities to adopt guidelines for procurement of trustworthy ICT products and provide for procurement of indigenously manufactured ICT products that have security implications.

B. Creating an assurance framework

1) To promote adoption of global best practices in information security and compliance and thereby enhance cyber security posture.

2) To create infrastructure for conformity assessment and certification of compliance to cyber security best practices, standards and guidelines (Eg. ISO 27001 ISMS certification, IS system audits, Penetration testing / Vulnerability assessment, application security testing, web security testing).

3) To enable implementation of global security best practices in formal risk assessment and risk management processes, business continuity management and cyber crisis management plan by all entities within Government and in critical sectors, to reduce the risk of disruption and improve the security posture.

4) To identify and classify information infrastructure facilities and assets at entity level with respect to risk perception for undertaking commensurate security protection measures.

5) To encourage secure application / software development processes based on global best practices.

6) To create conformity assessment framework for periodic verification of compliance to best practices, standards and guidelines on cyber security.

7) To encourage all entities to periodically test and evaluate the adequacy and effectiveness of technical and operational security control measures implemented in IT systems and in networks.

C. Encouraging Open Standards

1) To encourage use of open standards to facilitate interoperability and data exchange among different products or services.

2) To promote a consortium of Government and private sector to enhance the availability of tested and certified IT products based on open standards.

D. Strengthening the Regulatory framework

1) To develop a dynamic legal framework and its periodic review to address the cyber security challenges arising out of technological developments in cyber space (such as cloud computing, mobile computing, encrypted services and social media) and its harmonization with international frameworks including those related to Internet governance.

2) To mandate periodic audit and evaluation of the adequacy and effectiveness of security of information infrastructure as may be appropriate, with respect to regulatory framework.

3) To enable, educate and facilitate awareness of the regulatory framework.

E. Creating mechanisms for security threat early warning, vulnerability management and response to security threats

1) To create National level systems, processes, structures and mechanisms to generate necessary situational scenario of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities.

2) To operate a 24x7 National Level Computer Emergency Response Team (CERT-In) to function as a Nodal Agency for coordination of all efforts for cyber security emergency response and crisis management. CERT-In will function as an umbrella organization in enabling creation and operationalization of sectoral CERTs as well as facilitating communication and coordination actions in dealing with cyber crisis situations.

3) To operationalise 24x7 sectoral CERTs for all coordination and communication actions within the respective sectors for effective incidence response & resolution and cyber crisis management.

4) To implement Cyber Crisis Management Plan for dealing with cyber related incidents impacting critical national processes or endangering public safety and security of the Nation, by way of well coordinated, multi disciplinary approach at the National, Sectoral as well as entity levels.

5) To conduct and facilitate regular cyber security drills & exercises at National, sectoral and entity levels to enable assessment of the security posture and level of emergency preparedness in resisting and dealing with cyber security incidents.

F. Securing E-Governance services

1) To mandate implementation of global security best practices, business continuity management and cyber crisis management plan for all e-Governance initiatives in the country, to reduce the risk of disruption and improve the security posture.

2) To encourage wider usage of Public Key Infrastructure (PKI) within Government for trusted communication and transactions.

3) To engage information security professionals / organisations to assist e-Governance initiatives and ensure conformance to security best practices.

G. Protection and resilience of Critical Information Infrastructure

1) To develop a plan for protection of Critical Information Infrastructure and its integration with business plan at the entity level and implement such plan. The plans shall include establishing mechanisms for secure information flow (while in process, handling, storage & transit), guidelines and standards, crisis management plan, proactive security posture assessment and forensically enabled information infrastructure.

2) To Operate a 24x7 National Critical Information Infrastructure Protection Centre (NCIIPC) to function as the nodal agency for critical information infrastructure protection in the country.

3) To facilitate identification, prioritisation, assessment, remediation and protection of critical infrastructure and key resources based on the plan for protection of critical information infrastructure.

4) To mandate implementation of global security best practices, business continuity management and cyber crisis management plan by all critical sector entities, to reduce the risk of disruption and improve the security posture.

5) To encourage and mandate as appropriate, the use of validated and certified IT products.

6) To mandate security audit of critical information infrastructure on a periodic basis.

7) To mandate certification for all security roles right from CISO / CSO to those involved in operation of critical information infrastructure.

8) To mandate secure application / software development process (from design through retirement) based on global best practices.

H. Promotion of Research & Development in cyber security

1) To undertake Research & Development programs for addressing all aspects of development aimed at short term, medium term and long term goals. The Research & Development programs shall address all aspects including development of trustworthy systems, their testing, deployment and maintenance throughout the life cycle and include R&D on cutting edge security technologies.

2) To encourage Research & Development to produce cost-effective, tailor-made indigenous security solutions meeting a wider range of cyber security challenges and target for export markets.

3) To facilitate transition, diffusion and commercialisation of the outputs of Research & Development into commercial products and services for use in public and private sectors.

4) To set up Centres of Excellence in areas of strategic importance for the point of security of cyber space.

5) To collaborate in joint Research & Development projects with industry and academia in frontline technologies and solution oriented research.

I. Reducing supply chain risks

1) To create and maintain testing infrastructure and facilities for IT security product evaluation and compliance verification as per global standards and practices.

2) To build trusted relationships with product / system vendors and service providers for improving end-to-end supply chain security visibility.

3) To create awareness of the threats, vulnerabilities and consequences of breach of security among entities for managing supply chain risks related to IT (products, systems or services) procurement.

J. Human Resource Development

1) To foster education and training programs both in formal and informal sectors to support the Nation's cyber security needs and build capacity.

2) To establish cyber security training infrastructure across the country by way of public private partnership arrangements.

3) To establish cyber security concept labs for awareness and skill development in key areas.

4) To establish institutional mechanisms for capacity building for Law Enforcement Agencies.

K. Creating Cyber Security Awareness

1) To promote and launch a comprehensive national awareness program on security of cyberspace.

2) To sustain security literacy awareness and publicity campaign through electronic media to help citizens to be aware of the challenges of cyber security.

3) To conduct, support and enable cyber security workshops / seminars and certifications.

L. Developing effective Public Private Partnerships

1) To facilitate collaboration and cooperation among stakeholder entities including private sector, in the area of cyber security in general and protection of critical information infrastructure in particular for actions related to cyber threats, vulnerabilities, breaches, potential protective measures, and adoption of best practices.

2) To create models for collaborations and engagement with all relevant stakeholders.

3) To create a think tank for cyber security policy inputs, discussion and deliberations.

M. Information sharing and cooperation

1) To develop bilateral and multi-lateral relationships in the area of cyber security with other countries.

2) To enhance National and global cooperation among security agencies, CERTs, Defence agencies and forces, Law Enforcement Agencies and the judicial systems.

3) To create mechanisms for dialogue related to technical and operational aspects with industry in order to facilitate efforts in recovery and resilience of systems including critical information infrastructure.

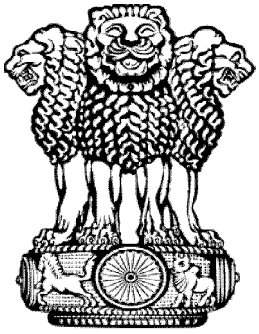
N. Prioritized approach for implementation

To adopt a prioritized approach to implement the policy so as to address the most critical areas in the first instance.

V. Operationalisation of the Policy

This policy shall be operationalised by way of detailed guidelines and plans of action at various levels such as national, sectoral, state, ministry, department and enterprise, as may be appropriate, to address the challenging requirements of security of the cyberspace.

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



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

SECURITY POLICY FOR USER

1. **Purpose:** The policy aims at providing secure and acceptable use of client systems.

2. **Scope:** This policy is applicable to the employees in the Ministry / Department / Subordinate office of Government of India for handling of unclassified information.

3. **Exception Management:** For any exception / deviation, the user shall take approval from the Chief Information Security Officer (CISO).

4. **Policy**

4.1 Acceptable Use of Client Systems

4.1.1 User shall be responsible for the activities carried out on the client system, using the accounts assigned to him / her.

4.1.2 User's network access shall be subjected to monitoring / filtering for malicious / unauthorized activities.

4.1.3 For any administrative activities on the client system, user shall adhere to Security Policy for System Administrator.

4.1.4 User shall use account with limited privileges on client system and shall not use administrator privileges. (refer: Limited User Account Creation Procedure)

4.1.5 Backup of important files shall be taken by the user at regular intervals. (refer: Data Backup and Restoration Procedure)

4.1.6 System / media containing official information shall be physically secured. (refer: Security Guidelines for User)

4.1.7 User shall not leave system unattended. The user shall lock out his / her system before leaving the system. Additionally, system idle timeout shall be configured on the client system. (refer: System Idle Timeout Configuration Procedure)

4.1.8 Maintenance or rectification of faults in the client system shall be carried out under close supervision of the user.

4.1.9 User shall check that the system time is as per IST. Any variation shall be reported to the System Administrator / Network Security Administrator.

4.1.10 User shall not engage in any of the following activities:

4.1.10.1 Circumventing security measures

4.1.10.2 Unauthorized access to Systems / Data / Programs

4.1.10.3 Harassing other users by accessing or modifying their data / resources on the system

4.1.10.4 Creating, accessing, executing, downloading, distributing, storing or displaying any form of anti-national, offensive, defamatory, discriminatory, malicious or pornographic material

4.1.10.5 Making copies of software / data for unauthorized use

4.1.10.6 Impersonation

4.1.10.7 Phishing

4.1.10.8 Social engineering

4.1.10.9 Unauthorized use of software license

4.1.10.10 Providing official e-mail address on Internet mail groups / bulletin boards for personal use

4.1.10.11 Any activity that is in violation of Central Civil Services (Conduct) rules

4.1.11 User shall report security incident to the System Administrator / Network Security Administrator. (refer: Security Incident Management Process)

4.1.12 User shall ensure that unauthorized Peer to Peer file sharing software is not installed.

4.1.13 User shall ensure that the system is configured as follows:

4.1.13.1 User shall not share client system with anyone, by default. However, if necessary for any specific reason (such as client system used in shift-duty), following shall be ensured:

4.1.13.1.1 Explicit approval of competent / designated authority is taken for each client system and every user accessing it.

4.1.13.1.2 Every user on the shared client system has a separate account.

4.1.13.1.3 File / Folder access permission is limited to meet functional requirement of the user.

4.1.13.2 User shall not share hard disk or folders with anyone, by default. However, if necessary, only the required folders shall be shared with specific user. (refer: Hard Disk / Folder Sharing Procedure)

4.1.13.3 Client System has Client System Security (CSS) implemented as per Client System Security Guidelines.

4.1.13.4 By default all interfaces on the client system are disabled and only those interfaces which are required are enabled. For configuration user shall contact the System Administrator.

4.2 Virus and Malicious Code (adware, spyware, malware)

4.2.1 User shall ensure that client system is configured with the authorized anti-virus software. *(refer: Anti-Virus Management Procedure)*

4.2.2 User shall ensure that anti-virus software and the virus pattern files are up-to-date. (refer: Anti-Virus Management Procedure)

4.2.3 User shall ensure that anti-virus scan is configured to run at regular intervals. (refer: Anti-Virus Management Procedure)

4.2.4 In case a virus does not get cleaned, incident shall be reported to the System Administrator / Network Security Administrator. (refer: Security Incident Management Process)

4.3 Hardware, Operating System and Application Software

4.3.1 User shall use only the software / hardware which are authorized by the Department.

4.3.2 The following activities shall be carried out by the System Administrator. However, the User shall ensure the following:

4.3.2.1 Operating System and other software is installed using authorized source / Original Equipment Manufacturer (OEM) media with valid license.

4.3.2.2 While installing the Operating System and other software packages, only the required utilities are installed / enabled. (refer: Operating System Hardening Guidelines).

4.3.2.3 Latest available service packs, patches and drivers are installed. (refer: Patch Installation Procedure and Patch Verification Procedure)

4.3.2.4 Booting from removable media is disabled. (refer: Removable Media Boot-up Disable Procedure)

4.3.2.5 Auto-run on all removable drives is disabled. (refer: Auto-Run Disable Procedure)

4.3.3 User shall allow the installation of service packs and patches provided by the patch server. (refer: Patch Installation Procedure and Patch Verification Procedure)

4.4 E-mail Use

4.4.1 Only the E-mail account provided by the Department shall be used for official communication.

4.4.2 Official E-mail shall not be forwarded to personal E-mail account.

4.4.3 E-mail password shall not be shared even for official purpose.

4.4.4 User shall not attempt any unauthorized use of E-mail services, such as:

4.4.4.1 Distribution of messages anonymously

4.4.4.2 Misusing other user's E-mail address

4.4.4.3 Using a false identity

4.4.4.4 Sending messages to harass or intimidate others

4.4.5 Password used for online forms / services / registrations / subscriptions shall not be the same as the password of official E-mail account.

4.5 Password Security

4.5.1 Selection of password shall be done as per the Password Management Guidelines.

4.5.2 The following activities shall be carried out by the System Administrator. However, the User shall ensure the following:

4.5.2.1 Passwords are enabled on BIOS, System login and Screensaver levels. *(refer: Password Enabling Procedure)*

4.5.2.2 Auto-logon feature on the client system is disabled. (refer: Auto-Logon Disable Procedure)

4.5.2.3 User account is locked after a predefined number of failed login attempts.

4.5.3 User shall not share or reveal passwords.

4.5.4 Passwords shall be changed at regular intervals as per the Password Management Guidelines.

4.5.5 If a password is suspected to have been disclosed / compromised, it shall be changed immediately and a security incident shall be reported to the System Administrator / Network Security Administrator (refer: Security Incident Management Process).

4.6 Portable Storage Media

4.6.1 User shall use officially issued portable storage media only.

4.6.2 User shall return the portable storage media, if it is no longer a functional requirement or in case of damage / malfunctioning.

4.6.3 User shall ensure that portable storage media used is free from virus.

4.6.4 User shall ensure that the execution of software from portable storage media is not done.

4.7 Network Access Policy applicable for the user

4.7.1 User shall take prior approval from the competent authority to connect the client system to the network.

4.7.2 A client system authorized to connect to one network shall not connect to any other network.

4.7.3 For wireless connectivity, user shall ensure the following:

4.7.3.1 By default, the wireless interfaces are disabled.

4.7.3.2 Client system does not connect to wireless networks / devices without approval from the competent authority.

4.7.3.3 If permitted, the wireless interface of the client system is enabled to connect to authorize wireless network only.

4.8 Client System Log

4.8.1 User having administrative privilege shall not disable / delete the audit trails / logs on the client system.

5.Review: This Security Policy shall be reviewed at the time of any change in the IT environment or once every year, whichever is earlier. The review shall be carried out for assessing the following:

5.1 Impact on the risk profile due to, but not limited to, the changes in the deployed technology / network security architecture, regulatory and / or legal requirements**.**

5.2 The effectiveness of the security controls specified in the policy. As a result of the review, the existing policy may be updated or modified.

6.Enforcement: Violation of this policy shall amount to misconduct under CCS Conduct rules.