संख्या-1151/78-1-2021-70आई0टी0/2017

प्रेषक,

अरविन्द कुमार,
अपर मुख्य सचिव,
उ0प्र0 शासन।

सेवा में,

समस्त अपर मुख्य सचिव/प्रमुख सचिव/सचिव,
उ0प्र0 शासन।

आई0टी0 एवं इलेक्ट्रानिक्स अनु0-1 लखनऊ: दिनांक 23 जुलाई, 2021

विषयः- उत्तर प्रदेश साइबर सिक्योरिटी गाइडलाइन्स/दिशा-निर्देशों को अपनाये जाने के सम्बन्ध में।

महोदय/महोदया,

अवगत कराना है कि देश में साइबर सुरक्षा के दृष्टिगत इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय, भारत सरकार द्वारा नेशनल साइबर सिक्योरिटी पॉलिसी-2013 (संलग्नक-1) जारी की गयी है, जिसको क्रियाशील करने के उद्देश्य से राज्यों द्वारा यथावश्यक दिशा-निर्देश निर्गत किये जाने की अपेक्षा है।

2- आप अवगत हैं कि ई-गवर्नेन्स के क्षेत्र में भारत सरकार एवं राज्य सरकार के संयुक्त प्रयासों के परिणामस्वरूप प्रदेश में Critical Infromation Infrastructure (CII) स्थापित किया गया है, जिसमें मुख्यतः उत्तर प्रदेश स्टेट डाटा सेन्टर (यू0पी0एस0डी0सी0), उत्तर प्रदेश स्टेट वाईड एरिया नेटवर्क (यूपीस्वान), कॉमन सर्विस सेन्टर (सी0एस0सी0), मिशन मोड प्रोजेक्ट्स (एम0एम0पी0), ई-डिस्ट्रिक्ट, ई-पंचायत, कृषि, खाद्य एवं रसद, भूलेख, ई-प्रोक्योरमेन्ट, ई-ऑफिस, मुख्यमंत्री हेल्पलाईन (1076) इत्यादि सम्मिलित हैं।

3- साइबर स्पेस में बढ़ रही इन्टरनेट की मॉग के फलस्वरूप साइबर क्राइम की सम्भावनायें भी काफी बढ़ गयी हैं, जिसके लिये साइबर सिक्योरिटी मानकों जैसे-सिस्टम सिक्योरिटी, नेटवर्क सिक्योरिटी, एप्लीकेशन, डाटा एवं इन्फॉर्मेशन सिक्योरिटी का अनुपालन किया जाना अत्यन्त आवश्यक है। इस सम्बन्ध में उत्तर प्रदेश साइबर सिक्योरिटी गाइडलाइन्स (संलग्नक-2) तैयार की गई है, जिसके अनुरूप समस्त विभागों के स्तर से कार्यवाही की जानी अपेक्षित है। साइबर सिक्योरिटी के सभी मानकों को अपनाने के बाद विभागीय Legacy डाटा चोरी होने, डिलीट होने, अनावश्यक बदलाव होने या किसी भी डिवाइस को नुकसान होने से बचाया जा सकता है।

4- साइबर सिक्योरिटी मानकों को लागू कर विभाग Unauthourized Access से सुरक्षित रह सकते हैं, जिससे किसी भी प्रकार के डाटा लॉस की सम्भावना नहीं रहेगी। इनके लागू होने से विभाग अपने नेटवर्क को भी सुरक्षित रख सकते हैं, जिससे इन्टरनेट के उपयोग से किसी प्रकार के नुकसान की सम्भावना न हो।

5- साइबर सिक्योरिटी में नेटवर्क की अलग-अलग परतों में अलग-अलग सुरक्षा प्रदान की जाती है। उक्त के दृष्टिगत ऑनलाइन साइबर अपराधों को रोकने के लिये साइबर सुरक्षायें जैसे- Network and Gateway Security, Data Loss Prevention(DLP), Application Security, Email Security, Antivirus Security, Network Access Control लागू होना अत्यन्त आवश्यक है।

6- ज्ञातव्य है कि दुनिया में जितने भी साइबर हमले हो रहे हैं, वह सब अलग-अलग प्रकार से किये जाते हैं तथा बदलती टेक्नोलॉजी के साथ साइबर हमलों के भी नये प्रकार जैसे- Malware Attack (Virus, Trojan, Spyware, Ransomware, Adware, Botnet, Worm), SQL Injection, Phishing, Man-in-the-middle attack, Denial of Service attack, Zero Day सामने आ रहे है।

7- विभागीय डाटा एवं नेटवर्क की सुरक्षा के लिये भारत सरकार द्वारा जारी दिशा-निर्देशों के अनुपालन में समस्त विभागों द्वारा अपने यहाँ Chief Information Security Officer (CISO) नामित किया जाना आवश्यक है, जिनके द्वारा विभागीय Critical Infromation Infrastructure (CII) का चिन्हिकरण किया जायेगा। विभागीय वेबसाइट्स/पोर्टल्स, कम्प्यूटर, मोबाइल, एण्ड प्वाइन्ट एवं नेटवर्क पर कोई Adverse Cyber Security Event होने अथवा किसी अन्य माध्यम से Vulnerability/Flaws की सूचना प्राप्त होने की स्थिति में नामित विभागीय CISO द्वारा CERT-In, GoI की ई-मेल-incident@cert-in.org.in पर सूचना तत्काल उपलब्ध करायी जानी होगी, साथ ही उसकी प्रति सेन्टर फॉर ई-गवर्नेन्स (सी0ई0जी0) की ई-मेल-ceglko.up@gmail.com एवं यूपीडेस्को की ई-मेल-mdupdesco.up@gmail.com पर भी उपलब्ध करायी जानी होगी।

8- आप अवगत ही हैं कि प्रदेश सरकार द्वारा जनपद लखनऊ में उत्तर प्रदेश स्टेट डाटा सेन्टर स्थापित कर संचालित है, जिसमें वर्तमान में 155+ विभागीय एप्लीकेशन्स/पोर्टल्स क्रियाशील हैं। देश में साइबर सुरक्षा के दृष्टिगत भारत सरकार द्वारा नेशनल साइबर कोर्डिनेशन सेन्टर (एन0सी0सी0सी0) की स्थापना की गयी है। इस प्रोजेक्ट के माध्यम से स्टेट डाटा सेन्टर के सेन्ट्रेलाइज्ड Logs की एक्सेस CERT-In, GoI को उपलब्ध हो जायेगी, जिसका विश्लेषण (AI/ML) कर Cyber Threats/Attacks से सम्बन्धी सूचनाओं को प्राप्त किया जा सकेगा। स्टेट डाटासेन्टर में विभागीय वेबसाइट्स/पोर्टल्स की होस्टिंग से पूर्व सम्बन्धित विभागों के स्तर से एन0आई0सी0, भारत सरकार द्वारा जारी वेबसाइट सिक्योरिटी गाइडलाइन्स NIC-Computer Emergency Response Team (CERT) (संलग्नक-3) का अनुपालन सुनिश्चित किया जाना अपेक्षित है।

9- उक्त के सम्बन्ध में मुझे यह कहने का निदेश हुआ है कि कृपया उक्त दिशा-निर्देशों का अनुपालन अपने विभाग में सुनिश्चित कराने का कष्ट करें।

<u>संलग्नकः यथोक्त।</u>

भवदीय,

(अरविन्द कुमार)
अपर मुख्य सचिव।

संख्या-1151(1)/78-1-2021 तद्दिनांक

उपर्युक्त की प्रतिलिपि निम्नलिखित को सूचनार्थ एवं आवश्यक कार्यवाही हेतु प्रेषित:-

1- स्टाफ आफिसर, मुख्य सचिव, उ0प्र0 शासन।

2- निजी सचिव, अपर मुख्य सचिव, मा0 मुख्यमंत्री उ0प्र0।

3- निजी सचिव, कृषि उत्पादन आयुक्त, उ0प्र0।

4- निजी सचिव, अवस्थापना एवं औद्योगिक विकास आयुक्त, उ0प्र0 शासन।

5- निजी सचिव, अपर मुख्य सचिव, आई0टी0 एवं इलेक्ट्रानिक्स विभाग, उ0प्र0 शासन।

6- निजी सचिव, विशेष सचिव, आई0टी0 एवं इलेक्ट्रानिक्स विभाग, उ0प्र0 शासन।

7- प्रबन्ध निदेशक, यूपीडेस्को/यूपीएलसी/अपट्रान पावरट्रानिक्स लि0/श्रीट्रान इण्डिया लि0, लखनऊ।

8- राज्य समन्वयक, सेन्टर फॉर ई-गवर्नेन्स, उ.प्र., अपट्रान बिल्डिंग, गोमतीनगर, लखनऊ।

9- हेड, एस.ई.एम.टी., उ.प्र.।

10- राज्य सूचना विज्ञान अधिकारी (एस.आई.ओ.), एन.आई.सी., योजना भवन, लखनऊ।

11- गार्ड फाइल।

आज्ञा से,
2३/7

(कुमार विनीत)
विशेष सचिव।

संलग्नक-1

File No: 2(35)/2011-CERT-In

Ministry of Communication and Information Technology
Department of Electronics and Information Technology

NOTIFICATION

Dated: 02July, 2013

Subject: Notification on National Cyber Security Policy-2013 (NCSP–2013)

National Cyber Security Policy– 2013(NCSP–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

[1] ISO / IEC 27032-2012

country. Such a focus enables creation of a suitable cyber security eco-system in the country, in tune with globally networked environment.

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 tenn 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.

(J.Satyanarayana)
Secretary, DeitY
Tel: 24364041

New Delhi, Dated: 2 July 2013

Copy to:
1. All Concerned Ministries/ Departments of Government of India
2. Cabinet Secretariat
3. PMO
4. Planning Commission
5. Comptroller and Auditor General of India
6. JS & FA, Department of Electronics and Information Technology
7. Internal Distribution

(J.Satyanarayana)
Secretary, DeitY
Tel: 24364041

संलग्नक-2

Uttar Pradesh Cyber Security Guidelines

Definition: -

Cyber Space – Cyber space 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.

Cyber Security – The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.

Periodic Security Audit

Periodic cyber security audit will help in identifying various vulnerabilities to be eradicated by department. Cyber criminals can launch attacks against your critical data from both within and outside your organization. An audit will provide you a good idea about the possible paths of attacks.

GIGW Compliance

The "Guidelines for Indian Government Websites" developed by National Informatics Centre (NIC) have been framed with an objective to make the Indian Government Websites conform to the essential pre-requisites of UUU trilogy i.e. Usable, User-Centric and Universally Accessible. These are mandatory to be followed throughout the lifecycle of a Government website, web portal/application right from its conceptualization to design, development, maintenance and management. GIGW guidelines ensure transparency, accessibility, effectiveness and easy access to benefit citizens.

HTTPS on websites

HTTPS (Hypertext Transfer Protocol Secure) is an internet communication protocol that protects the integrity and confidentiality of data between the user's computer and the departmental site. The HTTPS will provide Encryption, Data Integrity & Authentication.

W3C Compliance

W3C stands for "World Wide Web Consortium" which "develop Web standards" in order to lead the Web to its full potential".W3C compliance basically means that the HTML and CSS code that a website is built with is fully compliant with the standards set by the World Wide Web Consortium.

Regular Patching

Patch Management should be a key part of cyber security strategy. New vulnerabilities are discovered all the time and unless patches are applied, hackers will exploit these vulnerabilities to gain access to network. Patching is estimated to prevent up to 85% of all-cyber-attacks so it's vital your department to apply these patches as soon they become available.

Use data encryption

Data encryption prevents any unauthorized person from gaining access to data. Department can encrypt data to transform it into another form that only the person with the decryption key can access the message. Data encryption is currently one of the most popular data protection techniques used by various Organizations. The aim of encrypting data is to protect the confidentiality of digital data.

Back up important data

Important data can be lost as a result of a security breach. The department will ensure that important information is backed up frequently on the cloud or a local storage device.

Enable firewall protection

It is recommended that all organization set up a firewall to provide a barrier between their data and cybercriminals. In addition to the standard external firewall, many Organizations are starting to install internal firewalls to provide additional protection.

Keep software/Hardware up-to-date

Always update to the latest version of software to protect from new or existing security vulnerabilities.

- Turn on automatic system updates for devices
- Make sure desktop web browser uses automatic security updates
- Keep web browser plugins like Flash, Java, etc. updated

Outdated computer hardware may not support the most recent software security upgrades. Additionally, old hardware makes it slower to respond to cyber-attacks if they happen. Make sure to use computer hardware that's more up-to-date.

Strong, Complex passwords with multi-factor authentication

Strong, complex passwords can help stop cyber thieves from accessing Department /Organization information. Creating unique, complex passwords is essential. Organization may also require multi-factor authentication for all users.
Mobile Alerts must be enabled for unauthorized access to user profile and password change

Use a secure file sharing solution

The files you share are only as secure as the tools you use to share them with. Adopt a secure file sharing solution to encrypt your files while they're in transit and at rest to prevent unauthorized access and keep your files safe.

Use anti-virus and anti-malware

As long as you're connected to the web, it's impossible to have complete and total protection from malware. However, you can significantly reduce your vulnerability by ensuring you have an anti-virus and at least one anti-malware installed on your computers.

Use a VPN to privatize your connections

For a more secure and privatized network, use a virtual private network (VPN). It'll encrypt your connection and protect your private information, even from your internet service provider.

Remove adware from your machines

Adware collects information about you to serve you more targeted ads. It's best to rid your computer of all forms of adware to maintain your privacy. Use adware cleaner to clean adware and unwanted programs from your computer.

Scan external storage devices for viruses

External storage devices are just as prone to malware as internal storage devices. If you connect an infected external device to your computer, the malware can spread. Always scan external devices for malware before accessing them.

Avoid pop-ups, unknown emails, and links

Beware of phishing. Phishers try to trick you into clicking on a link that may result in a security breach. Phishers prey on employees in hopes they will open pop-up windows or other malicious links that could have viruses and malware embedded in them. That's why it's important to be cautious of links and attachments in emails from senders you don't recognize.

High-Quality Security Training for Employees

90% of all successful cyber-attacks are a result of information unknowingly provided by employees. As networks become harder to breach, hackers are increasingly targeting staff as they provide the easiest way to infiltrate a network.Effective security awareness training is essential in training employees on how to identify and respond appropriately to the growing range of cyber security threats. All employees, at every level of the organisation should receive this training to ensure they are armed with the skills required to identify an attack.

Chief Information Security Officer (CISO) in every department

Appoint a Chief Information Security Officer (CISO), responsible for cyber security efforts and initiatives. The CISO is the ultimate protector. Itroles and responsibilities include protecting people, assets, infrastructure and technology. It serves a critical role assessing risk and acting in the best interest of the department in an effort to eliminate threats.

संलग्नक - 3

NIC CERT

Observe - Detect - Respond

NIC- Computer Emergency Response Team (CERT)

Website Security Guidelines

Document Control

Document Title	Website Security Guidelines
Document Type	Guideline
Document Identifier	WSG
Version	1.0
Date of Release	November 2017
Document Owner	NIC-CERT
Document Author	HARIHARAN M
Document Reviewed By	Nagendra Kumar, HoD, NIC-CERT
Document Approved By	R.S Mani, HoG, NIC-CERT

Document Change History

Version No.	Revision Date	Nature of Change	Date of Approval

Website Security Guidelines

This Guideline is applicable to all NIC Employees, temporary/contractual staffs, Vendors, Third Party Personnel, Central and State Government Employees and other stakeholders who are involved in Website/Application – Development, administration, management.

1. Ensure that the Website is Security Audited and an Audit Clearance certificate is issued by a CERT-IN empaneled vendor before hosting in production environment. The Security Audit should be done every six months or as and when any changes are done to the source code.
2. Use SSL Certificate Site wide on all websites. The SSL Certificate should use at least 2048 bit SHA 256 encryption or higher.
3. Ensure that the SSL Certificate is valid and keep track of the certificate expiry date and take necessary action to renew/replace the certificate before expiry.
4. Disable support for SSL 2.0, SSL3.0, TLS 1.0 at the server level. Use TLS 1.2
5. Disable weak ciphers like DES, 3DES, RC4. Use Strong Ciphers like AES, GCM.
6. Any "non-https" requests received on the website/applications, should be forcefully re-directed to "https".
7. Ensure that all Websites and Applications and their respective CMS (Content Management System), 3rd party plugins, codes...etc., are updated to the latest versions.
8. All Passwords, connection strings, tokens, keys...etc., should be encrypted with salted hash. There should not be any plain passwords stored in config files or source code or in database.
9. All exceptions should be handled appropriately. Custom error pages should be displayed for any errors/exceptions. At no point of time, a portion of source code should be displayed on the page in case of an error or exception.
10. HTTP Response Headers should be obscured.
11. Directory traversal should be disabled. In case of any specific attempt by a user to access a portion of the code by typing the url path (ex: www.xxx.gov.in/js/custom.js) then the same should be redirected to a custom error page.
12. HttpOnly Cookies should be enabled, to restrict access to cookies.

13. All default user names and IIS/apache pages (like admin, default.aspx, index.aspx...etc) should be renamed. The access url for admin panel/CMS, should also be renamed.
14. The Web Server processes should not be running under Administrator or Root user Account. A dedicated User account with limited privileges should be used for the Web Server Processes.
15. All websites/Applications, should be checked by their respective developers on a daily basis and in case of any security compromise, then the same should be reported to NIC-CERT immediately.
16. Write + Execute Permission - both should not be given to upload directory
17. Ensure Input Validation is done properly, while accepting input from the user through the website.
18. Ensure that the Computer/system, from where CMS/site updates are being done is installed with the latest OS + Antivirus Updates and Patches. No unauthorized software/cracks, should be installed on the machine.
19. Restrict the web application to run Stored Procedures, so that SQL Injection attempts are averted.
20. If your website/application is integrated with any 3rd party Applications or using any APIs for external communication, then ensure that all such communications are done through encrypted channel.