DRAFT

Assam Cyber Security Policy 2019

Information Technology Department, Government of Assam

Table of Contents

1. Purpose

The purpose of this policy is to provide the Government of Assam with the necessary ICT direction, support and ICT security framework requirements to protect the digital information and ICT infrastructure. The protection extends to data and ICT systems of all the Departments and its constituents' organizations, based on their administrative, business and specific legal requirements.

This policy shall meet the minimum cyber security requirements in order to protect the confidentiality, integrity and availability of state-owned electronic information by Departments and its constituent organizations. It shall provide the Departments and its constituent organizations with the assurance and the "acceptable" level of asset protection from external and internal threats.

2. Short Title and Commencement

i. This policy may be called the "Assam Cyber Security Policy 2019".
ii. This shall extend to the whole of the State of Assam.
iii. This shall come into force on the date of its publication in the Official Gazette.

3. Definitions

i. **"Act"** means the Information Technology Act 2000 and subsequent amendments as enacted from time to time **by Government of India.**
ii. **"Agency"** means any organization that is involved in business interest with the State Government or is handling any government related data.
iii. **"Antivirus"** means software designed to detect and destroy computer viruses.
iv. **"BYOD**" Bring Your own device refers to the policy of permitting employees to bring their personally owned mobile devices (laptops, tablets, and smart phones) to their workplaces, and to use those devices to access privileged

company applications & information.

v. **“CERT-In”** means Computer Emergency Response Team-India.

vi. **“CII”** means Critical Information Infrastructure (CII) and defined as a computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety as defined in the Section 70 of the IT Act, 2000.

vii. “**Cloud Computing**” means the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer.

viii. **“Cyber Security”** means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.

ix. **“Department”** means the Administrative Department under the Government of Assam as specified in the Assam Rules of Executive Business, 1968.

x. **“GoI”** means Government of India

xi. **“Government”** means Government of Assam.

xii. **“Incident”** means a security event that changes or affects the everyday operations of a network or information technology service, indicating that a security policy may have been violated or a security safeguard may have failed.

xiii. **“Information Security”** means a practice of protecting information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

xiv. **“IoT”** means Internet of Things.

xv. **“ISMS”** means Information Security Management System.

xvi. **“IT Audit”** means a process of collecting and evaluating evidence to determine whether a computer system has been designed to maintain data integrity, safeguard assets, allows organizational goals to be achieved effectively, and uses resources efficiently.

xvii. **“IT Department”** means the Information Technology Department, Government of Assam.

xviii. **“NCIIPC”** means National Critical Information Infrastructure Protection Centre**,** is an organisation of Government of India created under Sec 70A of the Information Technology Act, 2000 (amended 2008), through a gazette notification on 16th Jan 2014.

xix. **“Official Gazette”** means the official gazette of the Government.

xx. **“Organisations” means** the Departments and its constituent’s agencies and institutes of Government of Assam

xxi. **“Policy”** means a statement of intent, and is implemented as a procedure or protocol.

xxii. **“State”** means the State of Assam.

All other words and expressions used but not defined in this policy, but defined in the Information Technology Act, 2000 (and amendment 2008) or National Cyber Security Policy 2013 and/or guidelines and / or rules and regulations made thereunder shall have the same meaning as respectively assigned to them in such Acts and /or policy and / or guidelines and / or rules and regulations, as the case may be.

4. Vision

To ensure, promote and sustain a safe and resilient cyberspace in the State to promote well-being of the citizens, business, Government and sustainability of its infrastructure in cyber security sector.

5. Mission

To identify, analyze, protect and build capabilities to prevent and respond to cyber threats posed on State's information and Information Infrastructure in Cyber Space through a combination of institutional structures, people, processes, technology and cooperation.

6. Objective

This Policy shall serve as best practices in information security for all the Departments and its constituent’s organizations of Government of Assam. This policy shall include all aspects of management, direction and support for information security in accordance with Government business, legislation, regulations and IT Act 2000 (and amendment 2008) requirements.

i. To protect the State Government digital information as well as data within its custody or safeguarding its confidentiality, integrity and availability.
ii. Identification and notification of Critical Information Infrastructure of the State Government for protection with the support of NCIIP.
iii. To establish safeguards to protect the information technology systems and resources from theft, abuse, misuse and any form of damage.
iv. To establish responsibility and accountability for information security in State departments and agencies.
v. To ensure that the Departments and its constituents' organizations are able to continue its administrative and ease of doing business activities in the event of significant information security incidents.
vi. Securing e-governance by implementing global best practices, and wider use of Public Key Infrastructure.
vii. Protection and resilience of critical information infrastructure.
viii. To setup incident response plan and Cyber Attack Crisis Management Plan to support government, business and citizen.
ix. To automate incident response across people, processes and technology
x. To ensure the security of Mobility, Cloud Computing and Bring Your Own Device (BYOD).
xi. To setup identity governance and access control management.
xii. To Protect data in motion & at rest and address compliance requirements of National and International.
xiii. To ensure the security of IoT installation and its computing environment.
xiv. To establish Cyber Café registration and Monitoring Cell.
xv. To established Social Media Regulations and Compliance.
xvi. To promote research and adoption of emerging technologies like artificial intelligence, machine learning, block chain etc. for ensuring cyber security in the State.
xvii. To established best practices for secure e-Waste management of every department of Govt. of Assam.

xviii. To introduce course curriculum in the education system (Schools & Colleges of State Government) the on cyber security.

xix. To provide training and capacity building of the employees on cyber security on regular basis to allow them to minimize the occurrence and severity of information security incidents.

xx. To impart trainings to officers from Law Enforcement, Forensic and judiciary etc.

xxi. To encourage CSR funding by the corporate houses for awareness program of citizen in the State.

xxii. To provide suitable coverage of IT Act 2000 (and amendment 2008), National Cyber Security Policy 2013 and International Standards ISO 27001, 17799 etc.

xxiii. To setup Cyber Security Helpline for the people to report the Cyber incidents.

xxiv. To Promote Cyber ecosystem management with emphasis on its Safety and Security.

7. Cyber Security Threats, Challenges and Mitigation

A. Cyber Security Threats

Today’s cybercrime landscape is diverse. Cyber threats typically consist of one or more of the following types of attacks:

i. Malware – Malicious software to disrupt computers.

ii. Viruses, Worms, Trojan Horse, Ransomware etc.

iii. Theft of Intellectual Property or Data.

iv. Hacktivist – Cyber protests that are socially or politically motivated.

v. Mobile Devices and applications and their associated Cyber Attacks.

vi. Social Engineering – Entice Users to click on malicious links.

vii. Spear Phishing – Deceptive Communications (e-mails, texts, tweets etc.).

viii. Domain Name System (DNS) Attacks.

ix. Network Security threat– internet traffic Hijacking.

x. Denial of Service (DoS) – blocking access to websites.

xi. Advance persistence threats.

One of the major challenges of the cyber threat is to identify the sources of attacks and its intention. The most common sources are:

a. **Cyber Criminals:** Seeking commercial gain from hacking banks and financial institutes as well as fishing scams and computer ransomware.

b. **Cyber Terrorists:** Mission to penetrate and attack critical assets and national infrastructure for aims to relating to political power and branding.

c. **Cyber Espionage:** Using stealthy malware to penetrate both corporate, military data servers in order to obtain plans and intelligence.

d. **Cyber Hacktivists:** Groups such as "Anonymous" with political agenda that hack sites and servers to virally communicate the messages for specific campaigns.

The State Government needs proper mechanism for Cyber Threat Identification and Mitigation.

B. Cyber Security Challenges

The aim of Digital India Programme is to digitally empowering Indian citizens by boosting connectivity, expanding ICT access, and improving electronic delivery of services. However, as the State makes progress on these goals, new threats in cyberspace poses new security challenges, as outlined below:

i. Cyberspace has inherent vulnerabilities that is hard to identify

ii. Innumerable entry points to internet.

iii. Increased use of mobile and web technologies

iv. It is generally observed that new forms of cyber-attacks outpace the defense mechanisms.

v. Nation states, non-state actors, and individuals are equipped to wage cyber-attacks.

vi. Internet technology makes it relatively easy for miscreants to conduct cyber attacks.

vii. Proliferation of Internet of Things (IoT) and lack of proper security in devices.

viii. Protection of personal data.

ix. Detection of financial frauds.

x. Fraud protection and criminal detection.

xi. Lack of awareness on Cyber security.

xii. Lack of Cyber Security specialists.

xiii. Use of pirated and unlicensed software and systems.

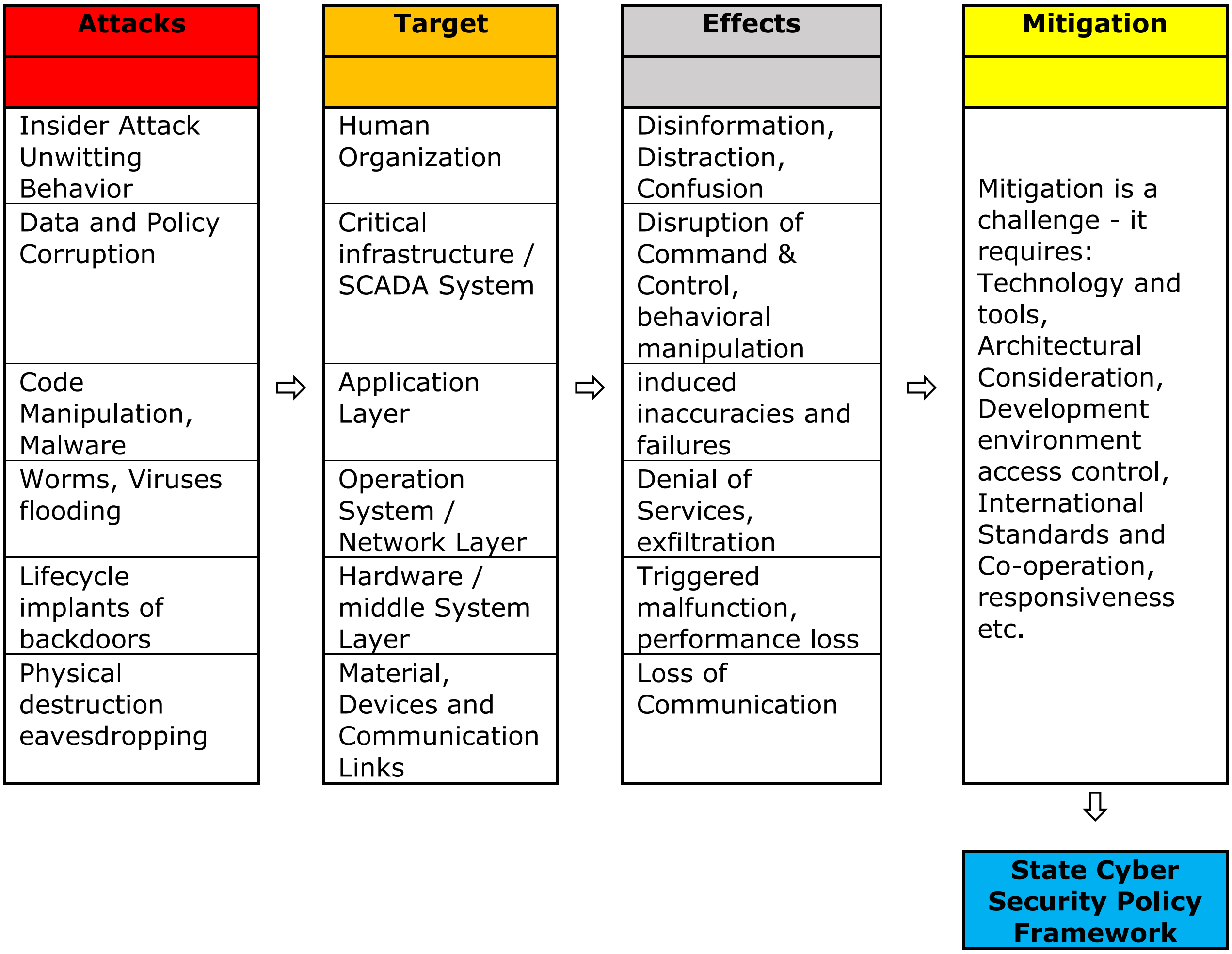
xiv. Increased use of Cyberspace by terrorists.

xv. Lack of e-Waste disposal mechanism.

xvi. Lack of dedicated cyber security funding by government.

C. Cyber Threat Mitigation

An attack vector is a path or means by which a source can gain access to a computer or network server in order to deliver a payload or malicious outcome. Attack vectors enable source to exploit system vulnerabilities, including the human element. Departments / organisations shall explore different attack vectors based on their system vulnerabilities including human factor while planning / preparing information security requirement under this policy and apply the various controls for mitigation.



Attacks	Target	Effects	Mitigation
Insider Attack Unwitting Behavior	Human Organization	Disinformation, Distraction, Confusion	Mitigation is a challenge - it requires: Technology and tools, Architectural Consideration, Development environment access control, International Standards and Co-operation, responsiveness etc.
Data and Policy Corruption	Critical infrastructure / SCADA System	Disruption of Command & Control, behavioral manipulation	
Code Manipulation, Malware	Application Layer	induced inaccuracies and failures	
Worms, Viruses flooding	Operation System / Network Layer	Denial of Services, exfiltration	
Lifecycle implants of backdoors	Hardware / middle System Layer	Triggered malfunction, performance loss	
Physical destruction eavesdropping	Material, Devices and Communication Links	Loss of Communication	

8. Indicative Security Design

Security Design must be inline with future technology with continual improvement of the suitability, adequacy and effectiveness of security management. Defense in Depth approach shall be followed to cybersecurity solution design, in which a series of defensive mechanisms are layered in order to protect valuable data and information. If one mechanism fails, another layer steps up immediately to thwart an attack. The following feature shall be maintained while designing information security solution by the user departments.

i. **Smart:** Security innovation must deliver more capable solutions to keep pace with threats.

ii. **Open:** Platforms and security standards must be open and interoperability to promote collaboration and accelerate adoption.

iii. **Trust:** Technology and security providers must be trustworthy in the creation and operation of their products.

iv. **Strong:** Products and services must be hardened to resist compromise and make security transparent to users.

v. **Ubiquitous:** Security must protect data wherever it exists or is used, for all parties and devices across the compute landscape.

vi. **Adaptive security:** Provides real-time security monitoring that scrutinizes the anomalies, malicious activities and vulnerabilities. If a threat is detected, the platform automatically implements security measures that counter the threat in a number of ways. This includes the following methods:

   a. **Prediction:** Predicts the most likely attacks, targets and methods. Predictive measures to identify attackers, their objectives and methods prior to materialization of visible attacks.

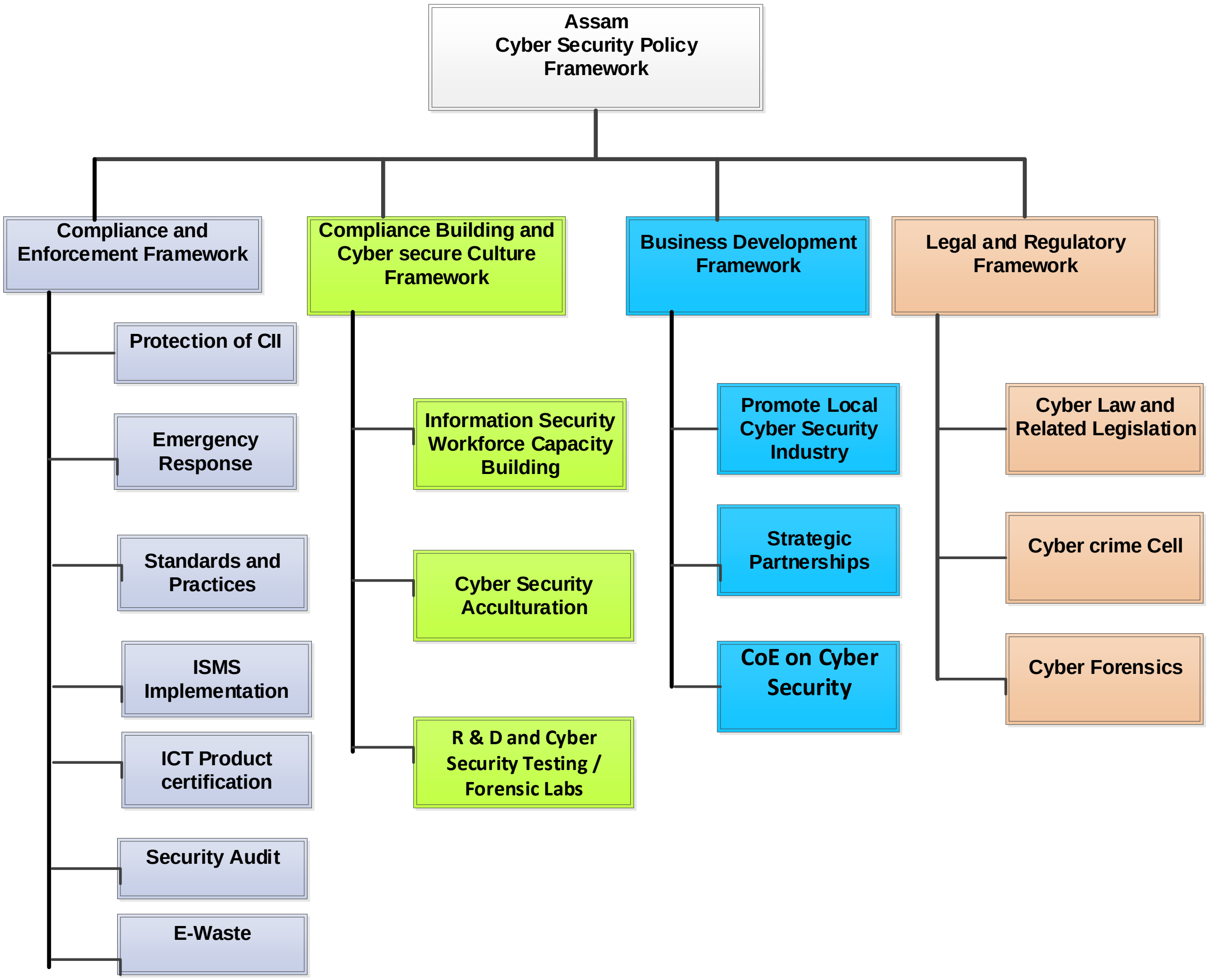
b. **Prevention:** Prevent or deter attacks so no loss is experienced. Secure the computing environment with current tools, patches, updates and other preventive methods in a timely manner. Educating and reinforcing good user behaviors.

c. **Detection:** Identify attacks not prevented to allow for rapid and thorough response. Efficient management to efforts to contain, repair, and recover as needed. Returning the environment to normal operations.

d. **Response:** Rapidly address incidents to minimize losses and return to a normal state. Monitor key areas and activities for attacks which evade prevention. Identifies issues, breaches, and attacks.

9. Framework for the Assam Cyber Security Policy

The Cyber Security Policy shall develop the following umbrella framework consisting of four sub- frameworks under this policy, which shall form the core pillars to provide a holistic approach to deal with cyber security in the State. IT Department, Govt. of Assam being nodal department shall develop necessary guidelines for supporting these frameworks. IT Department, Govt. of Assam shall also help the other user departments to prepare department specific guidelines / procedures related to information security under this framework. The modalities for implementation of different frameworks under this policy in time bound, well-coordinated, multi-disciplinary approach through necessary funding.


Assam Cyber Security Policy Framework
Compliance and Enforcement Framework
Protection of CII
Emergency Response
Standards and Practices
ISMS Implementation
ICT Product certification
Security Audit
E-Waste
Compliance Building and Cyber secure Culture Framework
Information Security Workforce Capacity Building
Cyber Security Acculturation
R & D and Cyber Security Testing / Forensic Labs
Business Development Framework
Promote Local Cyber Security Industry
Strategic Partnerships
CoE on Cyber Security
Legal and Regulatory Framework
Cyber Law and Related Legislation
Cyber crime Cell
Cyber Forensics

The four pillars that hold up the State cyber security policy framework are described as under:

i. Compliance and Enforcement Framework

a. Protection of CII of the State Government.

b. Emergency Response System for cyber Security incidents in the State.

c. Standards and Practices adopted at National and International Level.

d. Information Security Management System (ISMS) Implementation.

e. ICT Product certification for use in the Government.

f. Security Audit for systems and software

g. Secure disposal of e-Waste

ii. Compliance Building and Cyber secure Culture Framework

a. Information Security Workforce Capacity Building.

b. Cyber Security Acculturation focusing on building capacity in information security and raising awareness to the various stakeholders on the importance of securing information and practicing safe usage of ICT in the State.
c. Introduction of cyber security related courses for students at various levels and develop a pool of skilled manpower.
d. Capacity building on Research and Development, setting up Cyber Security Testing and Forensic Labs.

iii. Business Development Framework

a. Promote Local Cyber Security Industry and Start up initiatives.
b. Strategic Partnerships with National and International agencies of repute.
c. Center of Excellence on Cyber Security partnering with national and international agencies.

iv. Legal and Regulatory Framework

a. Cyber Law and Related Legislation enacted by the Government of India.
b. Cyber Crime Cell for investigation of cyber fraud and other crimes.
c. Cyber Forensics for evidence gathering to expedite the investigations.

10. Legal and Regulatory Guidelines

The rapid advancement in internet technology and absence of any internet boundaries has led to exponential increase in Cyber Crimes and its anonymity thus posing a major challenge in cyber-crime investigation. To tide over these new challenges in Cyber Security and for handling of the emerging Cyber Crimes, Assam Police has made a road map to establish, a unique initiative, called “Assam Police CyberDome” Centre for Cyber Security handling of Cyber Crimes. Any act, policy, guidelines, notification issued by the Home / Police Department, Govt. of Assam related to cybercrime, shall adhere to the “Legal and Regulatory Framework” of Assam State cyber security policy framework.

11. Government of India's Acts and Policies

This Cyber Security Policy shall also enforce the various IT security policies/guidelines defined for Government of India. Some of them have been mentioned below:

i. IT Act 2000 (and amendment 2008)
ii. National Cyber Security Policy 2013
iii. Aadhar Act 2016
iv. Framework & Guidelines for Use of Social Media for Government Organisations of MeitY, GoI.
v. National Data Sharing and Accessibility Policy (NDSAP-2012)
vi. Policy on Open Standards for e-Governance.
vii. Policy on Open Application Programming Interfaces (APIs) for Government of India.
viii. E-mail Services and usage policy, Govt. of India
ix. Security Policy for Access Control.
x. Virus and Malicious Code (adware, spyware, malware) prevention & usage of Antivirus Policy.
xi. Information System/IT Audit Policy or any other relevant notifications issued by GoI from time to time.
xii. E-waste (Management), Rules, 2016

12. Protection of Personal Data

Processing / sharing personal data while protecting privacy requires organizations / agencies to develop and implement solutions that complies with applicable privacy laws, regulations, and policies. In this regards, IT Act 2000 (amendment 2008), Aadhar Act and any other notifications and guidelines enacted by Govt. of India be strictly followed under this policy.

13. Cyber Security of Social Media

Social Media in recent times has become synonymous with Social Networking sites such as Facebook or MicroBlogging sites such as Twitter etc. However, very broadly social media can be defined as any web or mobile based platform that enables an individual or agency to communicate interactively and enables exchange of user generated content. Because of social media’s widespread popularity, it is often used for nefarious purposes that include cyberbullying, harassment, stalking, spread rumors, fake content, share unflattering or illegal images of individuals etc.

This policy recognises the “Framework & Guidelines for use of Social Media for Government Organisations” approved by the GoI, shall be followed by the Government of Assam creating a subset of guidelines specific to State under this policy. Any refinement in the context of social media security, regulation and enforcement, the State shall be defined and incorporated in consultation with Personnel and Home Department, Government of Assam.

14. Recent Initiatives by GoI

The following are the recent initiative taken by the Government of India

i. **Cyber Surakshit Bharat Initiative:** It was launched in 2018 with an aim to spread awareness about cybercrime and building capacity for safety measures for Chief Information Security Officers (CISOs) and frontline IT staff across all government departments.

ii. **National Cyber security Coordination Centre (NCCC):** In 2017, the NCCC was developed. Its mandate is to scan internet traffic and communication metadata coming into the country to detect real-time cyber threats.

iii. **Cyber Swachhta Kendra:** In 2017, this platform was introduced for internet users to clean their computers and devices by wiping out viruses and malware.

iv. **Education and Awareness Project (ISEA):** – a project to raise awareness and to provide research, education and training in the field of Information Security.

v. **International cooperation:** Looking forward to becoming a secure cyber ecosystem, India has joined hands with several developed countries like the United States, Singapore, Japan, etc. These agreements will help India to challenge even more sophisticated cyber threats.

The above mentioned initiatives shall be incorporated in this policy as an information security measures and any such initiatives in future also shall also be mandatorily followed by this policy.

15. Emergency Response Team for Cyber Security Incidents

Following steps shall be taken up for creating emergency response mechanism -

i. To setup a State Level Computer Emergency Response Team in collaboration with National level Computer Emergency Response Team (CERT-In) and NCIIPC, shall act as a Nodal Agency for State cyber security emergency response, cyber crisis management and cyber disaster management. The agency shall provide cyber security related actionable advisory to the Apex committee and also provide advisories to all the stakeholders. The agency shall also conduct penetration testing and security audit or assessment of government IT infrastructure of the State and initiate proactive measures.

ii. To create State level systems, processes, structures and mechanisms to combat cyber threats and enable timely information sharing amongst the stockholders.

iii. To develop a cyber grievance mechanism as a single point of contact for the state to report incident of cyber crime, cyber fraud, cyber harassment or bullying and other cyber security attacks faced by all stakeholders including citizens.

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

16. Role of Stakeholders

A. **IT Department:** IT Department, Government of Assam shall be the nodal department for administering the policy and has the authority to implement/modify this policy and formulate guidelines, issue notifications and set up monitoring mechanism for the implementation of this Policy. The broad roles and responsibilities of the IT Department shall be as follows:

i. Periodic evaluation of the information security performance and effectiveness of the security management viz-a-viz organization's security objectives by monitoring and measurements, feedback mechanism, management reviews, result of risk assessment and status of risk treatment plan.

ii. Identify and notify CII of the States and undertake measures to protect the notified CII with the support of National Critical Information Infrastructure Protection Center of Government of India and respective departments. Therefore, State Information Sharing Network for CII shall be established

iii. Institutionalize a collaborative mechanism amongst the State level and Central level Government agencies working in the cyber security domains.

iv. Mentoring other departments regarding implementation of ISMS and its various controls.

v. Review of information security of ICT projects undertaken by the departments and ensure that the development shall have safe and secure e-Governance products, applications and services.

vi. Protect sensitive citizen data stored, owned and processed electronically by the departments in the State.

vii. Facilitate the establishment of State level ICT security assessment center for the security audit of all IT hardware, software and mobile applications etc.

viii. Empanel Security audit firms, information audit organizations and competent professionals for supporting all the departments.

ix. Security Audit Adhering to international standards applicable for all Govt. websites, applications before hosting and publishing.

x. Ensure ISPs operating in the state shall deploy cybersecurity plans in line with Govt. of India / State Govt. cybersecurity policy and IT Act 2000 Intermediaries Guidelines (Amendment) Rules 2018.

xi. Identification, development of required courses and certification programme for imparting training to the State Government employees, Students, Business and Citizen.

B. Important Government Departments

Assam Police, Forensic Directorate, Law Department of Govt. of Assam

i. Enforcement of IT Act 2000 (amended 2008), related IPC and other laws.

ii. Capacity building of police department, law fraternity, Judges etc.

iii. Forensic examination of the cyber security breaches from legal perspective.

iv. Legal meteorology, legislation, research in cyber law, data privacy law, emerging technology laws etc.

C. Citizens: State Government recoginised that in order to create a safe and resilient cyber space in the State, Citizens co-operation and adoptions of best practices on digital and thus their awareness and capacity building is important.

Under this Policy, Citizens shall be encouraged to:

i. Follow cyber hygiene/rules while doing interacting in the cyberspace.

ii. Make them aware about their responsibility in use of digital devices in the cyber space.

iii. Make them aware of the everchanging threat landscape and adopt safety measures.

iv. Learn to identify and report threats in a safe and timely manner to the notified agency/agencies of the State Government.

IT Department shall work out the detail guidelines for awareness and communication for educating the citizens of the State in consultation with various stakeholders.

D. Private Sector: Private sectors working with the Government in particular shall be encouraged to assume following basic responsibility.

i. Be accountable for the products and services they provide to the State Government departments along with adequate guidance for the users for ensuring cyber security.

ii. Adopt ‘security by design’ and ‘privacy by design’ principles into their standards.

iii. Maintain transparency in their security and data-handling mechanisms and be ready to disclose whenever asked for.

iv. Invest in training and capacity building to meet future cyber security needs of the business partners in the State.

v. State Government shall facilitate all business enterprises to report any cyber incidence /threat to the State Cert.

17. Strategic Partner

State Government shall partner with Institutions of repute for driving various initiatives in Cyber Security. The potential partners include academic and research institutions, private players, other Government organizations etc.:

i. Setting up Center of Excellence on Cyber Security partnering with national and international agencies of repute.

ii. Participate in information sharing, focus on actionable threat, vulnerability, and mitigation information with states, national and international partners.

iii. Tie up with partners to deploy/test new products developed.

iv. Collaborate with the private sector, national and international partners to develop a skilled workforce to meet the demand of the cyber security professionals.

18. Implementation Strategies

To accomplish the objectives, the broad policy actionable items for the Government of Assam include:

i. Constitution of a State Apex Committee under the IT Department for providing strategic direction, guidance and coordinate matters related to information security in the state.

ii. Constitution of Department Level Cyber Security Committee to ensure information security and other related issues.

iii. Constitute a district-level Cyber Security Committee under the chairmanship of Addl. Deputy Commissioner (e-Governance) of the district.

iv. Developing a dynamic risk based cyber security frameworks to address the information security challenges in a holistic manner involving all stakeholders.

v. Identification and Securing Critical Information Infrastructure of the State for Government.

vi. Formulate a mandatory implementation action plan for ISMS and relevant guidelines / documents for each department / organisation across the state. All the departments / organisations shall mandatorily perform internal security audit followed by an external security audit periodically as per security requirement.

vii. Allocate the necessary resources and budget for its cyber security annually.

viii. Promoting research and development in cyber security in the State.

ix. Enhancing National and Global cooperation in combating security threats.

x. Fostering education and training programs in cyber security at various levels in the State.

xi. Establishing public and private partnerships to determine best practices in cyber security.

xii. Establish secure communication devices of network providers and ensure liabilities as intermediators.

xiii. Encourage to use certified ICT system and avoid vulnerable / black-listed system notified by the GoI.

xiv. All ICT Service Providers and System Integrators working with State Government shall deploy cyber security plans in the line of State Cyber security policy.

xv. Strengthening criminal-judicial response in IT and cyber law domain by capacity building of Law Enforcement Agency, Prosecution, Judiciary and Forensic department.

xvi. Establish 'First Court of Adjudication' to handle Legal Affairs / Cybercrime cases in the state as per IT Act 2000 and Adjudicating Officer in the entire judicial process.

19. Apex Committee for State Cyber Security

The IT Department shall constitute an Apex Committee under the Chairmanship of Chief Secretary, Govt. of Assam within 30 days from Gazette notification of this policy. The Apex committee shall provide policy directions and approve necessary funding to carry out implementation and monitoring of Cyber Security in the State. The constitution of the Committee shall have the following structure.

i. Chief Secretary, Govt. of Assam………………………...**Chairman**
ii. Commissioner & Secretary, IT Department, Govt. of Assam
iii. Commissioner & Secretary, Home & Political Affairs, Govt. of Assam

iv. Commissioner & Secretary, Finance Department, Govt. of Assam

v. Commissioner & Secretary, Land and Revenue Department, Govt. of Assam

vi. Commissioner & Secretary, Power Department, Govt. of Assam

vii. Commissioner & Secretary Transport Department, Govt. of Assam

viii. Commissioner & Secretary, Health & Family Welfare Department, Govt. of Assam.

ix. Commissioner & Secretary Education Department, Govt. of Assam

x. DGP, Assam Police, Govt. of Assam.

xi. IGP, Assam Police Cyberdome, Govt. of Assam.

xii. Chief Executive Officer (CEO), Assam Disaster Management Authority, Govt. of Assam

xiii. The Director, Information Technology, Electronics and Communication, Govt. of Assam

xiv. Managing Director, Assam Electronics Development Corporation Limited (AMTRON)

xv. Managing Director, Smart City Project

xvi. State Informatics Officer, National Informatics Center

xvii. Chief Information Security Officer (CISO), IT Department, Govt. of Assam

The Chairman may nominate domain experts from Industry and Academia as members of the committee. Detailed guidelines shall be prepared by the IT Department regarding the functioning, roles and responsibilities of the Committee.

20. Setting up of Department level Cyber Security committee

Each Department shall constitute a departmental level Cyber Security Committee under the Chairmanship of Senior most Secretary of the Department within forty five days (45) of the notification of this policy with following members-

i. Chief Information Security Officer (CISO) of the department.

ii. Nodal officer or Head of the IT Project of the department.

iii. Financial Advisor to the department.

iv. Technical in-charges (System, Network and Database Administrator etc.)

The department having ICT projects which are notified as CII, shall mandatorily nominate a representative from National Critical Information Infrastructure Protection Centre (NCIIPC), Government of India as a member of the above committee.

Detailed guidelines shall be prepared by the Departmental level Cyber Security committee in consultation with IT Department to define the functioning, roles and responsibilities of the Committee.

21. Setting up district level Cyber Security Committee

Each district shall constitute a district Level Cyber Security Committee under the chairmanship of Addl. Deputy Commissioner (e-Governance) of the district.

Detailed guidelines shall be prepared by the District level Cyber Security committee in consultation with IT Department regarding the functioning, roles and responsibilities of the Committee.

22. Budget Allocation for the Implementation of the Policy

i. All departments implementing and maintaining IT projects shall allocate 10% of their annual IT budget towards compliance with the security requirement to cyber security audit, trainings and capacity building etc.

ii. A separate funding by Government of Assam may also be looked upon for Cyber Security requirements of the State. This may be taken up by the Apex Committee based on requirements.

iii. Govt. of Assam shall encourage CSR funding by the corporate houses for creating awareness about cyber hygiene and crowd sourcing of solution through programmes like bug bounty, hackathons etc.

23. Operative Period of Policy

The Assam Cyber Security Policy, 2019 shall be operative for 5 years from the date of Gazette Notification.

24. Policy Review

This Policy shall be reviewed from time to time, considering the threat landscape of cyber security for the State.

The review shall be carried out for assessing the following:

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

ii. The effectiveness of the security directives specified in the policy, the existing policy may be updated or modified.

25. Conclusion

The Cyber Security is a complex subject which may have National and International implications, where threats landscape changes in various forms in short span of time, as such the policy enables the IT Department and other Stakeholders to adopt action in the best interest of the State and Public interest.