Government of Odisha

Cyber Security Policy

Odisha Computer Application Centre (OCAC)

(Technical Directorate of E&IT Department, Govt. of Odisha)
OCAC Building, Plot No.-N-1/7D, Acharya Vihar, RRL Post Office,
Tel No: - 0674-2567280/2567064/2567295/2588283

Document Control

Document Title	Cyber Security Policy - Odisha 2021
Document ID	CS- POL-001
Date of Release	
Document version	Version 4.0
Document reviewer	Chirag Barot
Document Owner	Odisha Computer Application Centre (OCAC) Government of Odisha
Security Classification	Confidential

Document Version Control

Version	Author	Date	Change Description
1.0	Deloitte	January 27, 2021	First Draft
2.0	Deloitte	March 04, 2021	Second Draft
3.0	Deloitte	July 13, 2021	Third Draft
4.0	Deloitte	Aug 16,2021	Fourth Draft

Distribution List

The following persons hold copies of the document: all amendments and updates to the document must be distributed to the distribution list.

Sr.	Name	Designation	Department
1.	Mrs. Madhumita Rath	GM (Admin), OCAC	OCAC
2.	Mr. Saroj Kumar Tripathy	Joint GM (Technical) & Nodal officer	OCAC
3.	Mr. Digvijaysinh Chudasama	Partner	Deloitte

4.	Mr. Vishal Gupta	Associate Director	Deloitte
5.	Ms. Ruhaakhtar Husseni	Manager	Deloitte
6.	Mr. Prabhupad Mohapatra	Deputy Manager	Deloitte
7.	Mr. Siddharth Pujari	Assistant Manager	Deloitte

Contents

Acronyms

Sr. No.	Abbreviations	Description/ Definitions
1.	AMC	Annual Maintenance Contract
2.	BCM	Business Continuity Management
3.	BCP	Business Continuity Plan
4.	CCTV	Closed Circuity Television
5.	CD	Compact Disk
6.	CISO	Chief Information Security Officer
7.	COBIT	Control Objectives for Information and Related Technologies
8.	COTS	Commercial Off-The-Shelf
9.	CS	Cyber Security
10.	CSeC	Cyber Security Committee
11.	CSF	Cyber Security Framework
12.	DC	Data Center
13.	DMZ	Demilitarized Zone
14.	DRP	Disaster Recovery Plan
15.	DVD	Digital Video Disk
16.	ERT	Emergency Response Team
17.	GoO	Government of Odisha
18.	HR	Human Resource
19.	ICT	Information and Communication Technology
20.	ID	Identifier
21.	IP	Internet Protocol
22.	IPR	Intellectual Property Right
23.	IS	Information Security
24.	ISM	Information Security Manager
25.	ISP	Information and Cyber Security Policy
26.	IT	Information Technology

Sr. No.	Abbreviations	Description/ Definitions
27.	LAN	Local Area Network
28.	LEA	Legal Enhancement Agency
29.	NIST	National Institute of Standards and Technology
30.	PII	Personal Identifiable Information
31.	PRO	Recovery Point Objective
32.	RCA	Root Cause Analysis
33.	RTO	Recovery Time Objective
34.	SCMC	State Crisis Management Committee
35.	SFTP	Secure File Transfer Protocol
36.	SPI	Sensitive Personal Information
37.	SLA	Service Level Agreement
38.	SOP	Standard Operating Procedure
39.	SPOC	Single Point of Contact
40.	SSL	Secure Socket Layer
41.	TPA	Third Party Assessment
42.	UOS	Uninterrupted Power Supply
43.	VLAN	Virtual Local Area Network
44.	VPN	Virtual Private Network
45.	WAN	Wide Area Network

1. Introduction

Today world is a complex environment consisting of increasing interdependency and this is in large part due to the evolution of information and communications technology.

There are many benefits to this interdependence, but there are also disadvantages, taking into consideration the fact that public institutions and departments have become almost entirely reliant on IT systems to carry out important functions.

The economic security of the state depends on the reliable functioning of critical infrastructure. Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the State's security, economy, and public safety and health at risk. Similar to financial and reputational risk, cybersecurity risk affects a department's bottom line.

The Odisha state government has been a key driver for increased adoption of IT-based products and IT enabled services in Public like Government to Government (G to G) services, Government to Citizen (G to C) Services, Business (Investor facilitation & tracking), Education (e-Learning, virtual classrooms, etc.) and financial services (mobile banking/ payment gateways), etc. Such initiatives have enabled increased IT adoption in the state through sectoral reforms and adopt Digital India program which have led to creation of large-scale IT infrastructure with corporate / private participation.

The scope of cybersecurity is expanding and enhancing digital security. Safety becomes an issue with the intersection of technology and the physical world including Internet of Things [IoT]). The policy addresses the digital risks and digital adversaries that will continue to challenge government eco-system. It serves as an umbrella for defining and guiding the actions related to security of cyberspace

The policy provides an overview of what it takes to effectively protect ICT infrastructure, information, information systems & networks, its supporting environment, infrastructure and applications and gives an insight into the Government's approach and strategy for protection of cyber space in the state. It also outlines some pointers to enable collaborative working of all key players in public & private to safeguard state's information and information systems. This policy, therefore, aims to create a cyber-security framework, which leads to specific actions and programs to enhance the security posture of state's cyber space.

2. Background

The Government of Odisha has been a key driver in the use of ICT extensively for delivery of public services. The OdishaOne portal Program being currently implemented by the Government is based on a whole-of-government approach, whereby most of the e-Governance systems are interconnected and integrated and provides a wide range of services online.

Industries Department of the Government of Odisha has developed an online Single Window portal, GO SWIFT i.e. Government of Odisha – Single Window for Investor Facilitation & Tracking, to promote a conducive business environment through transparency and time-bound clearances

The government has been driving the 'Mo Sarkar' and '5T' projects for the past two years, which is all about changing the business process of the government and helping it to become transparent and efficient through technology.

In this context, it is all the more necessary for Odisha to fortify its cyber security mechanisms and create a robust security ecosystem in the State.

3. Vision and Mission

The vision of the Odisha Cyber Security Policy is to create a robust cyber ecosystem, wherein the citizens and department users transact online securely and take steps to protect their identity, privacy and finances online, the departments conduct their operations without any disruption or damage and the Government ensures that its data and ICT systems are secure.

The Policy outlines the specific steps and mission initiatives to be taken by the Government and all other stakeholders to realize the vision stated above.

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

4. CERT-O

In the wake of lack of adequate expertise in Government/Government Agencies, there emerged a need for setting up of a permanent mechanism which would act as nodal agency for monitoring various cyber security related matters for Government of Odisha/Government Organisations. The state government had therefore felt the necessity for setting up of Computer Emergency Response Team-Odisha (CERT-Odisha or CERT-O) in line with CERT India (CERT-IN) to cater to crisis situations in Cyber Security matters of Government of Odisha.

4.1. Objectives of CERT – O

- To initiate proactive measures to increase awareness and understanding of Information security and computer security issues throughout the community of network users and service providers by disseminating security related information.
- To act as a nodal agency to conduct security audits or assessments of government and constituent IT infrastructure in the state, evolving security policy for the state.
- To act as a central point for monitoring, identifying vulnerabilities and suggesting remedial measures for correcting vulnerabilities in computer and communication systems (websites & e-governance applications) belonging to government and 'certify' any e-governance or e-commerce site in the state
- To conduct education, training, research and development.
- To collect and maintain a repository of all System / Website administrators of Odisha Government Websites/Web applications
- To build capacity among the technical personnel to identify and fight security threats.
- To assist CSeC and State Crisis Management Committee (SCMC) by priority with relevant information for their decision-making process.
- To carry out direction of CSeC and State Crisis Management Committee (SCMC) to fight cyber-attacks.
- To govern and monitor the Odisha Cyber Security Operation Centre (CSOC).
- To include government organizations and departments under the monitoring umbrella of Odisha CSOC.
- To create a suitably qualified and empowered personnel who can further enhance knowledge and expertise in this area to advance the mission.
- To formulate state's crisis management plan as appropriate from time to time and implement the same in coordination with CERT-In & with direction of Cyber Security Committee (CSeC) and State Crisis Management Committee (SCMC).

5. Purpose

Cybersecurity is a team effort and every individual or department has to be a part of the cyber security stance by the State. The Government will take the lead to spearhead initiatives to enhance Odisha State's cybersecurity stance, and we will need everyone's cooperation to reap long term benefits for the cyber ecosystem. We aim to build a Smart State – one that will be enabled by trustworthy infrastructure and technology.

- To create a safe cyber society in Odisha State, by generating adequate trust and confidence in IT/ICT/Information process systems in Odisha cyberspace and thereby enhance adoption of secured IT and ICT infrastructure in all sectors.

- To create a Cyber Security Policy Framework for designing of security policies and promote actions for compliance to national and international standards for strengthen the regulatory framework for ensuring safe cyber ecosystem.

- To develop suitable indigenous security technologies by proof of concept, pilot developments and encouraging growth for synchronizing with the emerging global digital economy / network society
- To enable visibility of the integrity of IT/ICT trusted products and services by establishing secured infrastructure for ensuring the security /confidentiality of data and to protect privacy of information and communication infrastructure to ensure public safety and National Security
- To encourage wider usage of IT/ICT infrastructure by all entities including Government for trusted communication, transactions and authentication
- To establish and create Odisha State Security Operation Centre (KS- SOC) for obtaining strategic information regarding incidents, threats towards Odisha State IT/ICT infrastructure for creating incident response, crisis management through effective predictive, preventive, protective, response and recovery actions and support to protect resilience of State IT/ICT and other critical infrastructures
- To support capacity building activities by enabling Education, Training and Awareness activities for creating skilled manpower and spreading cyber security awareness among public
- To encourage the adoption of information security best practices by all entities and Stakeholders in the Government, public & private sector and citizens that is consistent with industry standards
- To enable effective prevention, investigation and prosecution of cyber-crime and enhancement of law enforcement capabilities through appropriate support to establish capacity building activities for Legal Enforcement Agencies
- To enhance global cooperation by promoting shared understanding and leveraging relationships by creating culture of cyber security and privacy enabling responsible

user behavior and actions through an effective communication and promotion strategy for safer cyberspace of Odisha

6. Scope

- This policy applies to all employees of Odisha Government i.e. remote workers, permanent, and part-time employees, contractors, volunteers, suppliers, interns, and/or any individuals with access to the state department's / agencies' electronic systems, information, software, and/or hardware.

- All information assets which include, but are not limited to software assets, physical assets, paper assets, service assets, people assets and assets that are physically or electronically stored, processed and/or transmitted by any of the aforesaid types of assets.

7. Policy Owner

Government of Odisha shall appoint a suitably qualified and experienced senior level officer exclusively as CISO, who will be responsible of articulating and enforcing this policy to protect their information assets.

7.1. Policy Review, update and maintenance

The CISO is responsible for the review, updating and maintenance of Cyber Security policy. For any changes, review would be mandatory and the board shall be informed.

The review will include, but will not be limited to:

- Feedback from end users i.e. Government of Odisha Employees.
- Change in government processes.
- Improvement in the allocation of resources and responsibilities.
- Legal / Regulatory requirements.

8. Exceptions

There may be instances where there is a justifiable need to perform actions that are in conflict with Cyber Security Policy. Whenever for technical or operational reasons, it is not possible to comply with this policy, a time bound waiver must be requested, and this waiver needs to be approved by CISO. All approved exceptions should be reviewed at least annually or as and when required.

9. Strategies

The Cyber security Policy holds several strategies that are intended to provide a holistic and complete solution for cyber security threat. The strategies can be further divided into multiple guidelines.

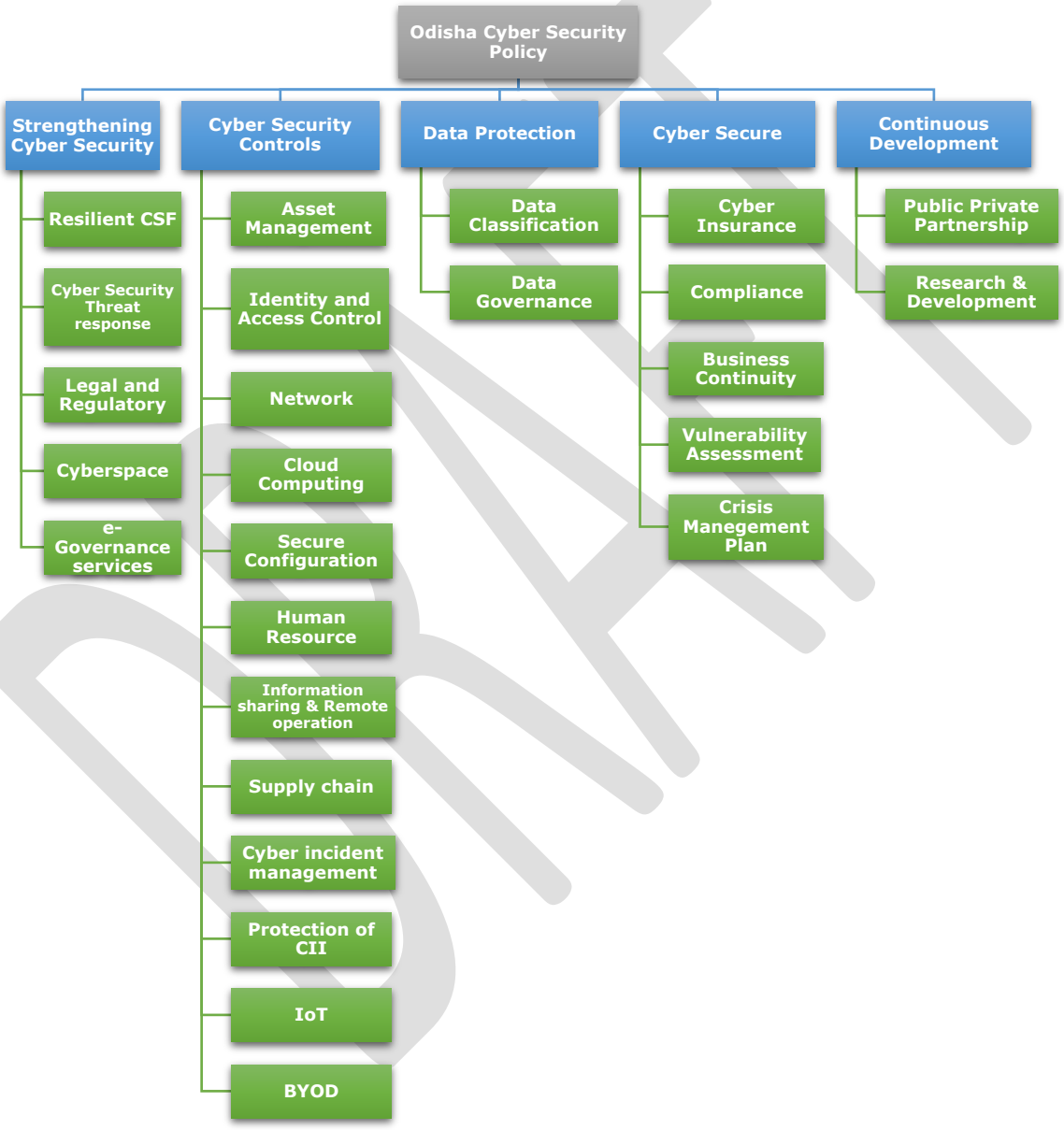

Figure 2: Cyber Security Policy Strategies

9.1. Strengthening Cyber Security

9.1.1. Resilient Cyber Security Framework

- To promote adoption of leading practices in information security and compliance and thereby enhance cyber security posture.
- To create infrastructure for conformity assessment and certification of compliance to cyber security leading practices, standards and guidelines (E.g. ISO 27001 ISMS controls, NIST Cyber Security guidelines, IS system audits, Penetration testing / Vulnerability assessment, application security testing, web security testing).
- To enable implementation of information security leading 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 of State.
- To identify and classify information infrastructure facilities and assets at entity level with respect to risk perception for undertaking commensurate security protection measures.
- To encourage secure application / software development processes based on global leading practices.
- To create conformity assessment framework for periodic verification of compliance to leading practices, standards and guidelines on cyber security.
- 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.

9.1.2. Cyber Security Threat Response Strategy and mitigation

- To create State 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.
- To operate a 24x7 Odisha SOC to function as a Nodal Agency for coordination of all efforts for cyber security emergency response and crisis management. CERT-O will function as an umbrella organization in enabling creation and operationalization of departmental SOC as well as facilitating communication and coordination actions in dealing with cyber crisis situations.
- To operationalize 24x7 departmental SOC for all coordination and communication actions within the respective sectors for effective incidence response & resolution and cyber crisis management.
- To implement Cyber Crisis Management Plan for dealing with cyber related incidents impacting critical national resources or endangering public safety and security of the

Nation, by way of well-coordinated, multi-disciplinary approach at the State, departmental as well as entity levels.

- To conduct and facilitate regular cyber security drills & exercises at State, departmental and entity levels to enable assessment of the security posture and level of emergency preparedness in resisting and dealing with cyber security incidents.
- To implement and operate a Security Operation Centre (SOC) for ensuring 24x7 security monitoring facility.

9.1.3.Legal and Regulatory Framework

- To develop a 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.
- 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.
- To enable, educate and facilitate awareness of the regulatory framework.

To tackle the challenges in Cyber Security and handling of cybercrimes, Commissionerate Police in Odisha launched a help desk to redress crimes related to fraud through phone call and cybercrime. In addition, in exercise of powers conferred by Clause (s) of Section-2 of the Cr.P.C., the Govt. of Odisha, Home Department, Bhubaneswar, vide Notification No. 22730/CP dated 09.06.2004 declared the office of the Superintendent of Police, CID, CB, Odisha, Cuttack, as the Cyber Crime Police Station, having its jurisdiction all over Orissa.

Any cyber-crime should be reported by the citizen through the prescribed network. Any policy, guidelines, notification issued by Govt. of Odisha related to cybercrime, shall adhere to the Information Technology Act – 2000.

9.1.4. Cyberspace

- To encourage all departments, state nodal agencies, private and public to designate a member of senior management, as Information Security Officer (ISO), responsible for cyber security efforts and initiatives.
- To encourage all departments / nodal agencies to develop information security policies duly integrated with their business plans and implement such policies as per industry 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.

- To ensure that all departments / nodal agencies earmark a specific budget for implementing cyber security initiatives and for meeting emergency response arising out of cyber incidents.
- To provide fiscal schemes and incentives to encourage entities to install, strengthen and upgrade information infrastructure with respect to cyber security.
- To prevent occurrence and recurrence of cyber incidents by way of incentives for technology development, cyber security compliance and proactive actions.
- To establish a mechanism for sharing information and for identifying and responding to cyber security incidents and for cooperation in restoration efforts.

9.1.5. e-Governance Services

- To mandate implementation of global security leading practices, business continuity management and cyber crisis management plan for all e-Governance initiatives in the State, to reduce the risk of disruption and improve the security posture.
- To encourage wider usage of Public Key Infrastructure (PKI) within Government for trusted communication and transactions.
- To engage information security professionals / agencies to assist e-Governance initiatives and ensure conformance to security leading practices.

9.2. Cyber Security Controls

9.2.1. Asset Management

Asset Management specifies the importance of maintaining records of each information asset including identification of the asset owner and asset classification.

Information assets of Govt. of Odisha shall receive comprehensive protection and shall have an identified owner. It provides direction to ensure that:

- An information asset register documenting the types of information assets of each business function is maintained.
- Information assets of each business function have designated owners.
- Use of department resources shall be limited to organizational purposes and department reserves the right to monitor and report the usage.
- Every department / agency is required to prepare and maintain an up to date inventory of all information assets associated with business function and define classification guidelines.

- A Standard Operating Procedure (SOP) document to be maintained by the respective department / agency regarding the allocation, return and disposal of assets.
- Use of dept. managed resources shall be prohibited for the use of commercial activities other than those related to organizational purposes.
- Computing and Network resources provided by department / agency shall be used only by the authorized employees and Third Parties.
- Should clearly define all associated services and different architectures under the department.
- All assets regarding cloud services should comply with MeitY procedural guidelines. Understanding of the implications pertaining to cloud computing and cross-border movement of data.

9.2.2. Identity and Access Control

Access controls are required for all IT systems in accordance with risk in order to protect information assets against unauthorized logical access.

Requirement of Access Control

Management of Access Control:

- Managers shall be accountable for the access rights of the users under their supervision.
- Users shall be granted with least privilege required for a particular role or function.
- Additional restrictions shall be implemented for Special Privilege Accounts.
- All accesses shall be reviewed on periodic basis and appropriate actions shall be taken.
- Additional authentication methods (like two factor authentication) shall be used when allowing users to connect remotely.
- Access to operating system shall to be controlled by a secure logon procedure.
- The use of utility programs that might be capable of overriding the system and application controls shall be restricted and tightly controlled.
- Restrictions on connection times shall be used to provide additional security for high-risk applications.
- Inactive sessions shall be terminated after a defined period of inactivity.

Access to network and network services:

- Computer networks shall be segregated to isolate critical GoO IT assets and those exposed to higher risks (Internet facing).
- Sensitive systems shall have a dedicated (isolated) computing environment.

- Any category / website that poses a security risk shall be blocked explicitly after due diligence.
- Access to non-business related website shall be prohibited such as pornography, terrorism, hacking.

User Access Management

User registration and de-registration:

- A formal documented procedure shall be in place for granting and revoking access to all IT systems.
- All usernames should to be uniquely identifiable and the principles of non-repudiation have to be met.

User access provisioning

- All user access requests shall be authorized by the user's reporting manager. The level of access to be granted, or role profile to be assigned to a user, shall be approved by the business system owner or their approved deputies / Project Manager / reporting official.
- It is the responsibility of the approver(s) to ensure the person has a legitimate business need for the level of access requested, after doing due diligence.

Management of privilege access rights:

- Creation and allocation of privileged user accounts / IDs on the information systems shall be authorized.
- The privilege associated with each system (e.g. Operating Systems, Databases, and Applications) and their corresponding users are identified.
- Privileges are allocated to individuals on a 'need-to-have' basis in strict adherence to the authorization process for privilege access.
- A record of all privilege accounts used on the information systems is maintained; changes made to privileged accounts are recorded.

Management of secret authentication information:

- Temporary passwords shall be provided only after confirming the user identity and the password should expire upon first use.
- Default vendor passwords requires to be altered following installation of systems or software. Such altered passwords shall be known only on need to know basis to privilege users.

Review of user access rights:

- Accounts that access executive or confidential data shall be reviewed semi-annually, using a documented business process. Review process shall verify that an on-going process is in place to ensure that employees who have left GoO no longer have active accounts and those unnecessary entitlements have been removed when roles have changed.

Removal or adjustment of access rights:

- Access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.
- Email Access rights of employees shall be removed upon termination of their employment, contract or agreement.

9.2.3. Network Security

The establish and maintain a secured connectivity within and outside every department / agency, State should ensure that every agency and departments under its governance follow the minimum requirements:

- Investigate any unauthorized access of computer networks, systems or devices.
- State would collaborate with academic or administrative departments and law enforcement when appropriate.
- All assets connected to internet or any network should have adequate security installed and must be configured and maintained in such a manner as to prohibit unauthorized access or misuse.
- Every activity and usage through the internet / internal network should be monitored and judged appropriately for suspicious activity and transactions.
- Implement mechanism to monitor and restrict network packet sniffing or snooping.
- To develop authorization mechanism at every ingress and egress points in the network architecture.
- Develop guidelines for addition or deletion of any network asset, gateways, etc. to the existing network and architecture.
- Should ensure that written Service Level Agreement (SLA) are in place with external Internet Service Providers (ISP) and relevant monitoring system is in place for compliance.

9.2.4. Cloud computing

Cloud computing recently has displayed lot of potential to public and government bodies in terms of scalability, elasticity, high performance together with less administration. Policy should be developed to understand, manage and control the risks mainly affecting confidentiality, security and resiliency related to cloud computing. The following points should be considered while hardening the guidelines for cloud computing:

- Should clearly define all associated services and different architectures to be implemented.
- Cloud service provider should comply with cloud security and certification as per MeitY procedural guidelines.

- Clear understanding of the implications pertaining to cloud computing and cross-border movement of data.
- State or designated agency must assess the impact on business processes before shifting to cloud services to avoid any technical barriers.
- State or designated agency should be fully aware about where its information actually resides at any given point in time.
- State or designated agency should have the capability/assurance to find and access its data and information at any point of time.
- Should ensure that written Service Level Agreement (SLA) are in place with Cloud Service Providers and relevant monitoring system is in place for compliance.
- State or designated agencies should consider the risks associated with any possible compromise to government data or information through any third-party having access to data or information.
- Should be aware and document the responsibility for the security of the information even while residing with a cloud service provider.

9.2.5.Internet of Things (IoT)

The IoT is diverse from traditional computers and computing devices, makes it more vulnerable to security challenges in different ways. As the expansion of the IoT market continues, so do the number of potential risks that threaten the performance and safety of devices and the integrity of IoT data. Poorly secured IoT devices and services can serve as entry points for cyber-attacks, compromising sensitive data and threatening the safety of individual users.

In addition to securing IoT devices, department / designated agency also needs to ensure that their IoT networks are secure. Access control mechanisms and strong user authentication can help to ensure that only authorized users are able to gain access to the IoT framework.

Prior to hardening the IoT devices, State or its designated agency should ensure the following:

- Detection: Understanding exactly which IoT devices and components are connected to a given network or system.
- Authentication: Verifying the identity and origin of IoT devices to detect and prevent spoofing.
- Updating: Continually maintaining, updating, and upgrading IoT security capabilities to stay ahead of hackers and cybercriminals.

The following should be considered while hardening the IoT devices:

- **Secure and centralize the access logs of IoT devices:** Centralize access logs, and train security teams to recognize attack and alert patterns that use IoT endpoints.
- **Use encrypted protocols to secure communications:** Choose devices that employ encryption and use it. Devices that connect to mobile apps or other remote gateways should use encrypted protocols as well as encrypt data storage.

- **Create more effective and secure password policies**: Default passwords should be modified to strong, unique ones, and may utilize single sign-on tools to manage and limit access.
- **Implement restrictive network communications policies and set up virtual LAN:** Isolate sensors and other permissive devices on a separate virtual LAN. Sensors should have unique network design and architecture to avoid entire network compromise in case of any cyber breach or attack.
- **Understand that device firmware should be secure:** Implement devices that have secure firmware and upgrade policies when possible. In addition, educate users on how to secure devices.
- **Improve failover design**: Failover design is especially important for IoT devices that involve user safety, video monitoring, and environmental monitors and alarms. These devices should have manual overrides or special functions for disconnected operations.

9.2.6.Bring Your Own Device (BYOD)

BYOD policies enable employees to use their personal devices in the workplace. While this can improve efficiency by enabling employees to use the devices that they are most comfortable with it also creates potential security risks.

The following guidelines should be opted by State or any designated agency for implementation of cyber security towards BYOD policy:

- Defining who can access and which application through personal devices.
- Governance over the accessibility of data / information, who access the data, from where is the data accessed and through which device.
- Storage of all data / information on secure servers accessible through internal network or virtual private network (VPN).
- Restrict unknown and unauthorized applications from accessing department data or information through personal device.
- Wherever possible implementation of controls and tools for mobile device management and mobile application management.
- Every personal device used under BYOD policy should be encrypted to avoid leakage of data during loss or theft of device.
- BYOD security awareness training to be provided to the employees which should include:
    - Workplace ethics for personal devices utilized under BYOD.
    - Strong password policy and storage of data or information locally.
    - Encryption policy and process for personal devices.
    - Communication with department applications through VPN or other technology.

9.2.7. Secure Configuration

Secure configuration refers to security measures that are implemented when installing assets or devices in order to reduce unnecessary cyber vulnerabilities. It is one of the most common identified vulnerability that can easily be exploited. To establish and maintain the integrity of the devices, the following should be followed:

- No asset or device should be deployed into organization's environments without prior approval of the respective information security officer.
- Any modification or change to production systems, network devices, and firewalls should be approved by the respective information officer before they are implemented to assure they comply with business and security requirements.
- Any installation of asset or device, new or modification to existing asset should be tested in separate environment before it is implemented into production.
- State or its designated agency should develop and implement baseline guidelines to hardening any operating systems which are in the production environment.
- All devices and assets should be hardened to prevent usage of unauthorized external media and data sharing.
- Develop and monitor time stamps for every activity and modification done to the production environment.
- Every application / software to be hosted in the State or designated agency's premises should be tested and certified as Safe to Host and free from any vulnerability.
- All procedures and guidelines should be reviewed by respective management to maintain consistency in the organization.
- All devices should be configured as per functional requirement and all unnecessary ports, protocols, service, etc. should be restricted.
- Remote access and authorization to assets of any organization should be limited and regularly monitored to avoid any incident.
- State or designated agency should implement appropriate encryption technologies and utilize secure channels for transfer of data and information through any communication.

9.2.8. Human Resource

- To foster education and training programs for employees, contractors, third party, citizens etc. to support the State's cyber security needs and build capacity.
- To establish cyber security training infrastructure across the State by way of public private partnership arrangements.
- To establish cyber security concept labs for awareness and skill development in key areas.
- To establish institutional mechanisms for capacity building for Law Enforcement Agencies.
- To promote and launch a comprehensive State awareness program on security of cyberspace.

- To establish online learning management system to enforce compliance eLearning & Certification.
- To modify the curriculum of the schools, colleges, and Universities for enhance the awareness of cyber security among school students, general cyber security skills among college students and advanced knowledge of cyber security among the university students.
- Cybersecurity training covering the domains as; email, malware, password security, external media, internet social networking, bring your own device (BYOD), data privacy, etc.
- To sustain security literacy awareness, sensitization and publicity campaign through electronic and paper media to help citizens to be aware of the challenges of cyber security.

9.2.9. Information Sharing and Remote operation

- Identify where critical or regulated data resides, define data categories.
- To create models for collaborations and engagement with all relevant stakeholders.
- To create a think tank for cyber security policy inputs, discussion and deliberations.
- Sensitization and security awareness training for personnel for data handling, remote access and secure configuration.
- Implementation of secure and encrypted communication channels for access to applications and work dashboards.
- Usage of only authorized asset or software for official activity. To restrict any pirated or unlicensed software or tool.
- Hardening and monitoring of assets utilized for remote working by the respective department or agency to prevent any cyber threat or vulnerability.
- Implement appropriate encryption technologies and secure channels for sharing of information.

9.2.10. Supply Chain

- To create and maintain testing infrastructure and facilities for IT security product evaluation and compliance verification as per leading standards and practices.
- To build trusted relationships with product / system vendors and service providers for improving end-to-end supply chain security visibility.
- 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.

- Should ensure documented Service Level Agreement (SLA) with third party service providers and relevant monitoring for compliance.

9.2.11. Cyber Incident management and monitoring

The government through CERT-O, a nodal agency for the state to coordinate with institutions, organizations and departments. CERT-O will contribute towards the State's efforts for a safer, stronger network for all citizens and departments by responding to major incidents, analyzing threats, and exchanging critical cyber security information with trusted partners.

- Preparation of advisories with actionable information to the Government, critical infrastructure agencies, private industries and general public.
- Preparation of a crisis management plan regarding incident handling and response for critical infrastructure.
- Development of a cyber grievance reporting channel for the state to report incident of cybercrime, cyber fraud and other cyber security attacks faced by all users and citizens.
- Publication of proactive advisories and manuals to increase awareness regarding information security issues.
- Establish a round the clock security operation facility for emergency response and crisis management.

9.2.12. Protection of Critical Information Infrastructure

- To develop a plan for protection of State Critical Information Infrastructure & Protection Centre functioning as the State Department. Integration of Protection Centre with business plan at the entity level and implementation. 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.
- To facilitate identification, prioritization, assessment, remediation and protection of critical infrastructure and key resources based on the plan for protection of critical information infrastructure, NCIIPC Guidelines for Identification of CII and Evaluating Cyber Security Framework of NCIIPC.
- To mandate implementation of global security leading practices, business continuity management, NCIIPC Guidelines for Protection of CII, and cyber crisis management plan by all critical sector entities, to reduce the risk of disruption and improve the security posture.
- To encourage and mandate as appropriate, the use of validated and certified IT products.
- To mandate security audit of critical information infrastructure on a periodic basis.
- To mandate certification / training for all security roles right from CISO / ISO to those involved in operation of critical information infrastructure.

- To mandate secure application / software development process (from design through retirement) based on industry leading practices.
- To report and share the details of the cyber security incidents pertaining to the Critical Information Infrastructure (CII) of the State.
- To mandate development of SOPs for deployment of any asset into department's environments with prior approval from the respective information security officer.
- Proper implementation of controls for any modification to assets.
- Develop and implement baseline process for hardening of assets which are in the production environment.
- Deployment of application / software in the department infrastructure post relevant testing.

9.3. Data Protection

Departments / nodal agencies, people, billions of connected devices generate, process and consume all sorts of data every day. The range of data is also diverse, from ones and zeros coming from simple IoT devices that signal an on/off event (e.g. a motion detector sensor), to weather, traffic, financial transactions, health, and social media among others.

Data protection allows organizations to think about data classification based on sensitivity and business impact, which then helps the organization assess risks associated with different types of data.

9.3.1. Data Classification

- Identify where critical IP or regulated data resides — This could include hard drives, databases, network files, folders, cloud applications, etc.
- Define data categories – and should be kept simple by avoiding complicated or exhaustive classification schemas.
- Detect the most valuable data and leverage technology, such as data classification and labeling automation tools, to safeguard this sensitive information.
- Train existing and new employees how to handle sensitive data, including providing tools and resources for ongoing security awareness.
- Adhere to local, state, and national data protection legislation and regulations and understand the penalties for non-compliance.
- Build a data classification strategy that empowers users to contribute to and take responsibility for properly handling critical IP or regulated data within an organization.

9.3.2. Data Governance

- To establish the goals of the overall Data Governance program and metrics for determining success.
- To establish Data Governance Committee and assigning roles & responsibilities such as Data Protection officers with respect to nodal agencies.
- To facilitate Identification, Prioritization and Classification of critical data assets pertaining to Government of Odisha; and provide appropriate level of oversight of the data assets based on their value and risk.
- To establish data standards and guidelines, along with the procedures and programs to enforce them.
- To establish Data Lifecycle Management process, that should cover Data Usage, Aging, Distribution, Storage and Archival parameters.
- To define and implement Data Access Policy and procedures to enhance security of the data, including confidentiality and protection from loss.
- To define and implement Data Usage Policy and procedures to ensure that data should not be misused or abused, according to any applicable law or regulation.
- To establish mechanisms to ensure Data Integrity, resulting in greater accuracy, timeliness, and quality of available information.
- To regularly monitor and ensure adherence to the defined policy, applicable laws and regulations related especially to Data Privacy & Data Security.

9.4. Cyber Secure

9.4.1. Cyber Insurance

- To create cyber risk profile for the user departments / agencies, and list of expenses to be covered in the event of a security incident.
- Identifying reliable Insurance providers and facilitate in finalizing standard terms and conditions for the agreement.
- To discuss and finalize Insuring clauses like e-theft loss, e-communication loss, e-threat loss, e-vandalism loss, e-business interruption w.r.t the coverage required.
- To monitor and ensure user departments/ agencies must comply with Insurance policy terms & conditions, to avoid any issues related to future claims.

9.4.2. Cyber Security Compliance

- Technical compliance checking shall be conducted at regular intervals by the Cyber Security Committee or any designated agency either manually or with the assistance of automated tools to assess the level of Information and Cyber risk preparedness.
- All functions shall obtain a security clearance for projects, products, applications, services, etc., having information security impact, from the CISO during their initiation and prior to deployment in production environment.
- Technical compliance checking shall cover penetration testing, vulnerability assessments, architecture review which could be carried out internally or by independent experts specifically contracted for this purpose.
- Cyber Security Committee shall report Information Security metrics to CISO on the periodic basis.
- Any technical compliance check shall only be carried out under the authorization of the Cyber Security Committee.

9.4.3. Business Continuity

To ensure continuity of critical functions, it shall be mandated for every department and agency in the State to design, implement and maintain a business continuity plan. The plan should proactively identify issues (building, equipment, technology, cyber, human resources & third parties) that may affect the continuity of operations and build resilience arrangements to mitigate, respond and recover from a disruptive event.

The BCM plans must be socialized and tested to ensure awareness and effectiveness. Through periodic review, the plans must be assessed and updated to ensure relevance to the operating environment.

An IT Disaster Recovery Plan should be designed and implemented to ensure availability of all critical IT and security infrastructure. The plan should account for the response and recovery procedures to deal with disruptions emanating out of a cyber incident.

9.4.4. Vulnerability Management

- Periodic security assessments shall be conducted across State departments or agencies' systems, servers, network devices and applications to detect vulnerabilities. Alternatively, a web application firewall shall be implemented.
- Conducting VA/PT of internet facing web / mobile / cloud based applications, servers & network components throughout their lifecycle. Such assessments shall only be carried out by professionally qualified teams.
- Ensuring that the vulnerability scanning tools are adopted / implemented and regularly updated with latest security vulnerabilities information.
- Timely information about technical vulnerabilities of information systems being used shall be obtained by internal teams, external teams and sources. Assets exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken to address the associated risk.
- Vulnerabilities and system patches shall be prioritized by the information security team for remediation commensurate with the risk to State's systems, networks and data.
- Vulnerability remediation and patching activity for systems, applications, servers and network devices shall be tracked as per defined timelines.
- Critical patches in test environment shall be evaluated before pushing them onto production systems.

9.4.5. Cyber Crisis Management Plan

Cyber resilience is defined as GoO's ability to anticipate withstand cyber-attacks and the capability to contain recover rapidly and evolve to improved capabilities from any disruptive impact caused due to cyber-attacks. Below are the best practices to be followed to withstand Cyber-attacks.

Cyber Crisis Management Strategy

Cyber Incident handling activities include:

- Incident Detection -Incident reporting includes mechanism of Detection and reporting of security incident.
- Resolution steps – Resolution of a security incident includes response, containment and remediation of incident.
- Recovery- Recovery identifies how to safely put the impacted systems back into production.

Post remediation review -

- Post-remediation review is performed to ensure that the incident has been resolved successfully and its resolution has no security impact on the information asset.

Root cause analysis and corrective action-

- Root cause analysis identifies the underlying reasons of why an incident occurred and preparing corrective action plan to eliminate Root Cause.

Test preparedness to withstand cyber attacks

Exercising and Testing

CISO shall develop various exercises such as crisis simulation exercises, mock drills etc., which assess the adequacy and consistency of Cyber crisis management plan. Testing exercise shall also be performed to measure the GoO defensive and responsive capabilities. These exercises tests are conducted at planned intervals or whenever significant changes occur.

CISO to ensure:

- Resiliency tests are conducted in line with Cyber Crisis Management Plan (CCMP) scope and its objectives.
- Resiliency tests are based on appropriate scenarios that are well planned and clearly defined aims and objectives.
- Resiliency tests outcomes shall minimize the risk of disruption of operations
- Produce post exercise reports that contain outcomes recommendations and actions to implement improvement.

Cyber Security Procedures and Guidelines

GoO shall develop Cyber Security procedures and guidelines in addition to the Cyber Security policy. It shall document detailed procedures and guidelines of how to implement the policy

The key objectives are:

- To ensure that Cyber Security Policy is interpreted correctly and uniformly across the GoO including foreign offices
- To provide guidelines for implementation of the policy & standards.
- To create awareness about policy standards and assist in their compliance.

9.5. Continuous development in Cyber Security

9.5.1. Effective Public and Private Partnership

- 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.
- To develop bilateral and multi-lateral relationships in the area of cyber security with other States and other security agencies (like CERT-In, NCIIPC) of Central Government.
- 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.

9.5.2. Research and Development in Cyber Security

- To collaborate in joint Research & Development projects with industry and academia in frontline technologies and solution oriented research.
- 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.
- 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.
- To facilitate transition, diffusion and commercialization of the outputs of Research & Development into commercial products and services for use in public and private sectors.
- To set up Centre of Excellence in areas of strategic importance for the point of security of cyber space.

10. Cyber Security Committee (CSeC)

The committee responsible for addressing cybersecurity within state, may be referred to as the "Cyber Security Committee".

To best address the Govt. of Odisha cybersecurity concerns, the cybersecurity committee must assess the state's risk profile and that entails a detailed examination or audit of a state's digital vulnerabilities, existing defenses, and areas of improvement.

- A cybersecurity committee is tasked with overseeing the development and implementation of state's cybersecurity policy, laying out the standards to which employees must adhere to mitigate the state's vulnerabilities.
- Cybersecurity committees always be responsible for overseeing the development of procedures for a variety of "worst case scenarios".
- A lot of risk and responsibility is weighted on the shoulders of a cybersecurity committee. Committee members always have a combination of expert knowledge and cybersecurity experience.
- The committee's strong decision-making competence gives them their best shot at taking on the enormous challenge of implementing strong cybersecurity defenses.

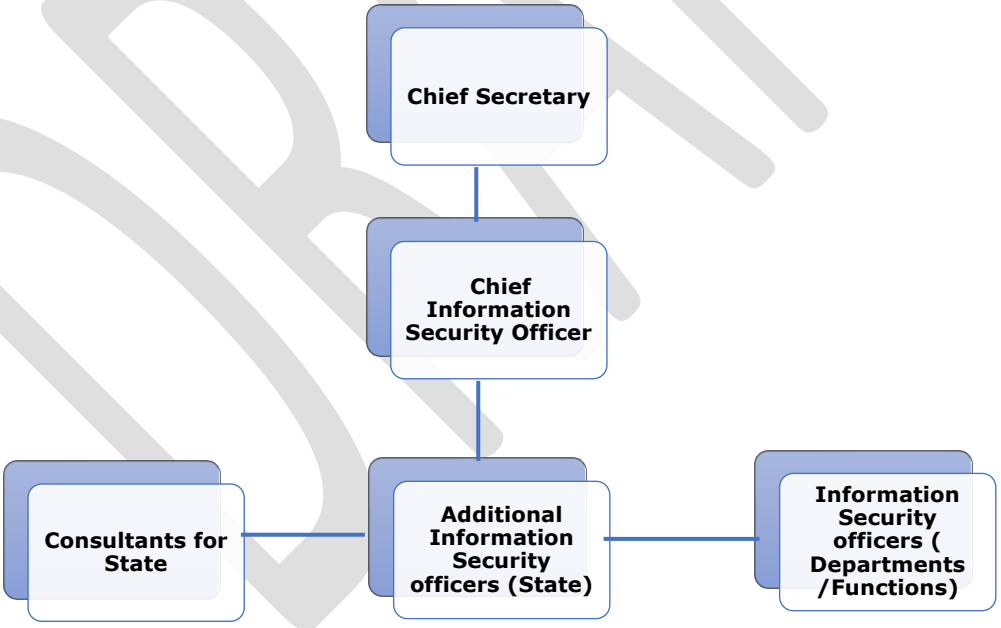

Figure 1: Cyber Security Committee (CSeC) structure

10.1. Structure of Cyber Security Committee

CSeC shall have the following members:

a) Chief Secretary (CS) – Chairperson
b) CISO (State)- Member
c) Additional Information Security Officers (State)- Member
d) Consultants (State) – Member
e) Information Security Officers (Departments/Functions)- Member
f) Any other offices deemed fit by CISO

10.2. Responsibilities, Rights and Duties of Cyber Security Committee (CSeC)

Chief Secretary

- Act as a management forum maintaining an oversight on Odisha State Cyber Security risk.
- Define and drive the organization-wide Information Security objectives, strategies, polices and awareness.
- Sanction funds and resources for Information Security of Odisha state
- Approve all policy matters related to Information Security and changes thereto.
- Approve exceptions on a case-by-case basis when the requirements of the Cyber Security policy cannot be met, provide a timeline for the exception and follow-up the exception condition till the Security Policy requirements are met.
- Initiate discussion of Information Security concerns and issues resolve these and ensure that effective procedures are implemented.
- Review status of Cyber Security implementations and Audits
- Setting up DRP/BCP committee.
- Monitor significant changes in the exposure of information assets to various threats.
- Identify, classify and periodically review the criticality and confidentiality requirements of all types of information resources.
- Guide the information security issues are appropriately addressed in the business plan.

Chief Information Security Officer (CISO)

- Responsible for articulating information and Cyber Security Policy for Odisha state.
- Be responsible for providing advice and support to management and information users in the implementation of Cyber Security policy
- Promote user awareness initiative within Odisha state.
- Provide the management and users assistance in correcting deficiencies.
- CISO shall be responsible for assisting CS for all the activities performed related to information and/or Cyber Security Policy for Odisha state.

Consultants (State)

- Developing efficient strategies for the Govt. of Odisha to protect the system, the networking infrastructure, data and information system against potential cyber risks.
- Routinely performing vulnerability testing threat analysis, system checks and security tests.
- To investigate and provide security solutions using business standard analysis criteria.
- To deliver technical reports and official papers relating to test findings
- To give professional supervision and guidance to security teams.
- To update and upgrade security systems as required.
- Managing meetings with department heads to fix cyber security related issues.

Additional Information Cyber Security Officers for State

- Shall interface with state CISO and its/Departments in relation to information / cyber security related issues.
- Act as a central point for their respective domain for Cyber Security policies, issues and concerns.
- Monitor and implementation of Security policies and Standards
- Provide guidance to System Administrators for implementation of security policies and standards.
- Monitor the security related activities carried out by System Administrators.
- Monitor and assess the compliance to security policies, procedures and standards on an ongoing basis and report exceptions to CISO.
- Suggest Cyber Security improvements to CISO.
- Administer the security awareness program among the employees.
- Facilitate the resolution of security conflicts within the organization and escalation of the same to the CISO.
- Ensure Incident Management including Incident Response.
- Conduct regular and spot audits to determine compliance to Cyber Security policy.
- Assist in developing contingency plans and assist in DR/BCP implementation.

Information/Cyber Security Nodal Officers

Information Security nodal officers have to ensure the compliance of Information and Cyber Security Policy of Odisha State in their respective regional offices (RO)/departments/functions in consultation with respective IT wing. Each department must have designated Information / Cyber Security officers. They have to:

- Hold the primary responsibility for defining the values and classification of assets within their control by participating in the risk management process and undertaking business impact assessment.
- Authorizing and approving access including designing and maintaining segregation of duties for individual users and groups including third parties to the information contained within the applications.

- Ensure implementation and compliance to Cyber Security policy are applicable for their business units.
- Coordinate with departments to ensure that Cyber Security efforts are consistent across state/ department/ agencies.
- Adhere, disseminate and enforce Odisha state's Information and/or Cyber Security Policy and Standards as updated from time to time.
- Monitor the implementation of Information Security Policies and Standards in their respective business units or departments.
- Ensure that Information Security requirements are implemented.
- Report to the Information Security Wing at Head Office (HO) with respect to their business unit or department specific security concerns and security implementation status.
- All points relevant to RO in entire Information and/or Cyber Security Policy are to be followed.

End User

- Reporting of any Cyber Security incidents including loss of assets such as laptops, mobile phones and devices configured with BYOD (Bring your own devices) services.
- Be aware and comply with all the requirements mandated by this policy.

11. Conclusion

Cyber Security is a complicated domain which has, from individual to national level implications. The threat landscape keeps changing in forms and scenarios within short span of time. In such situations, a cyber security policy enables the State and Electronics and Technology Department to adapt and take necessary procedures for response and mitigation to threats and incidents. The policy is to be implemented keeping in mind the best interests of the State and citizens.

Annexure I – References

Sr. No.	Circular Reference Number
1.	NIST guidelines for Cyber Security
2.	National Cyber Security Policy 2013
3.	COBIT (DS5.2, DS5,3) and (DS5.2, ME2.5, ME2.7) for Information Security Policies
4.	MeitY guidelines for Cyber Security