TAMIL NADU
CYBER SECURITY POLICY
2020

INFORMATION TECHNOLOGY DEPARTMENT

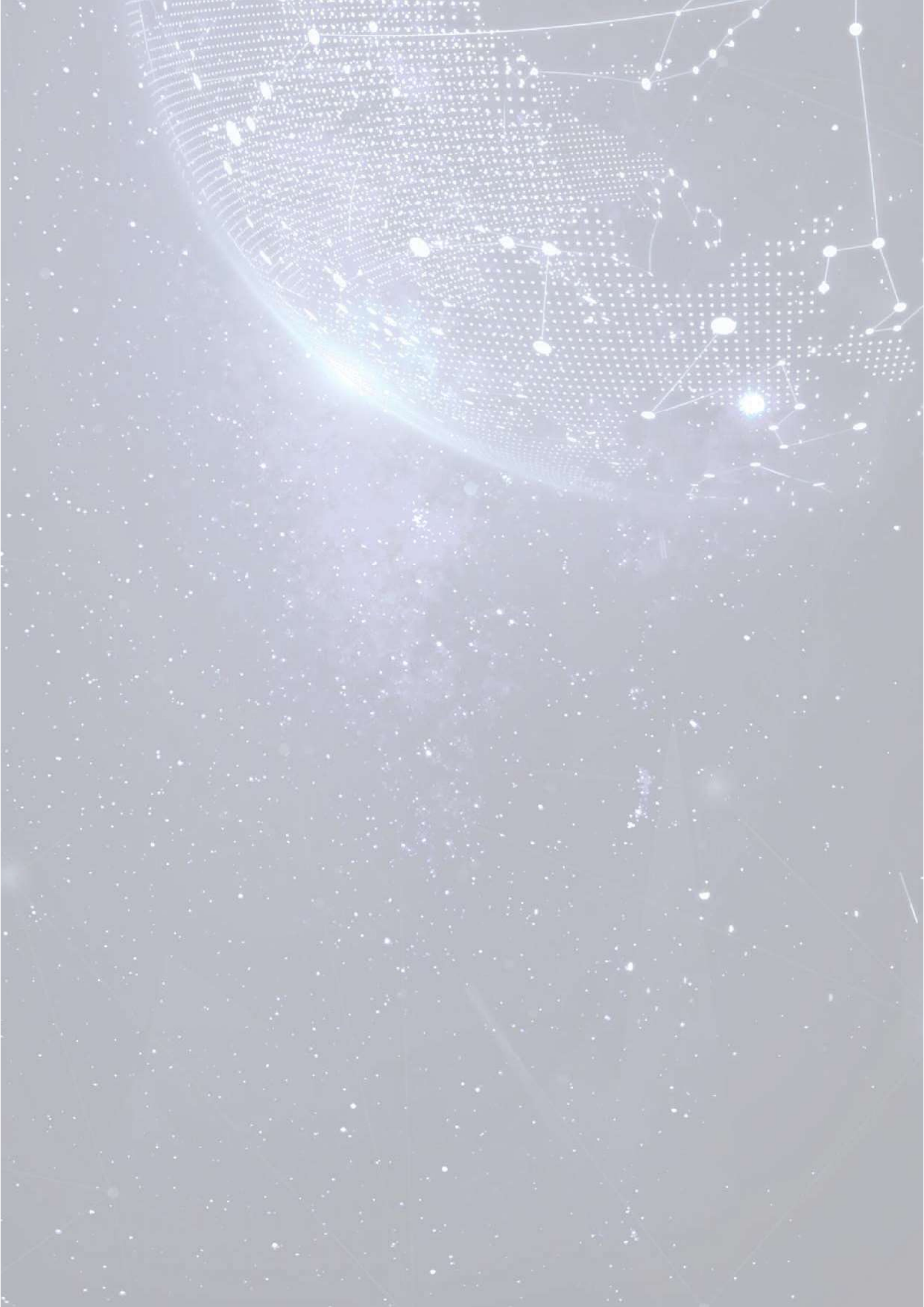


Table of Contents

CHAPTER - 1

OUTLINE OF CYBER SECURITY POLICY


01
02
03
04
45%
534547657568
675756756756
7867876889
7878678789789
87798797
7867886976
78979878978
23423435
5446565
6576565
786768
6786687
7867686
786767

CHAPTER - I

OUTLINE OF CYBER SECURITY POLICY

Preamble

1.1 The Digital Economy today comprises a significant portion of India's total economy and is one of the areas where Tamil Nadu plays a significant role. Tamil Nadu has been a leader in ICT enabled Governance as well as a Hub of IT Industry.

1.2 The Citizens of Tamil Nadu and the TN Government need a secure Infrastructure to manage a large gamut of Information. Security of this Infrastructure and Data is a major concern of the Government. The secure design and delivery of Government Services will enable the State's Digital Transformation to prevent any damage to Government and public interests and recover the Data and Services if Information Security breaches occur.

2. Scope and Applicability

2.1. Information Security Management deals with the planning, implementation and continuous Security controls and measures to protect the confidentiality, integrity and availability of Information Assets and its associated Information Systems.

2.2. Information Security Management activities include the following functional aspects:

(a) Security Architecture Framework – SAF-TN

(b) Best Practices for Governance, Risk Management and Compliance (GRC)

(c) Security Operations – SOC-TN

(d) Incident Management – CERT-TN

(e) Awareness Training and Capability Building

(f) Situational Awareness and Information Sharing

2.3. This Policy is applicable to all Government Departments and associated Agencies. It covers Information Assets that may include Hardware, Applications and Services provided by these Agencies to other Government Departments, Industry or Citizens.

2.4. This Policy will be applicable to private Agencies when entrusted with specific work of Tamil Nadu Government. It may include Data of the Government/Citizens that are in the control of such private Agency and its Infrastructure. In case of any doubt, the contracting Government Arm/ the Information Technology Department of Government of Tamil Nadu must be approached.

2.5. This Policy applies to Central Infrastructure and Personnel who provide Services to the Tamil Nadu Government either on specific deputation or by specific tasking.

2.6. Nothing in these Policy contravenes any law of the Government of Tamil Nadu or the Union of India, nor existing Policies of either of the entities. If any contradiction is suspected, it must be brought to the notice of the Information Technology Department, Government of Tamil Nadu immediately.

3. Entities and Responsibilities

3.1. The Information Technology Department, Government of Tamil Nadu is the Nodal Department for IT Security of Tamil Nadu. The Information Technology Department will have the following roles with respect to Cyber Security :

(a) Provide safe hosting for Servers, Applications and Data of various Departments /Agencies.

(b) Advise Departments who are procuring IT Equipment or Services on Security aspects

(c) Establish and operate a Cyber Security Architecture for Tamil Nadu (CSA-TN) including the Security Operations Centre (SOC-TN) and Computer Emergency Response Team (CERT-TN)

(d) Carry out Training and Awareness Programmes for Departments and Citizens on Cyber Security.

(e) Formulate and issue Cyber Security related Policies for the Government of Tamil Nadu. It will also formulate and put up recommended statutory framework for ensuring legal backing of the Policies.

3.2. All Government Departments and Agencies are responsible for their IT assets. This includes Services, Software and Hardware under their control. While the Heads of the Department bears the overall responsibility for Security of their Assets, each Department will have a nominated Departmental Chief Information Security Officer (CISO). This Officer will be given training to identify and secure Assets and utilise the Security Advisories given by the Information Technology Department effectively.

4. Mission

4.1. Protect Information Assets of Government (Infrastructure, Software, Citizen Services) and maximize their availability to Government and the Citizens.

4.2. Develop a Comprehensive Security Risk Reduction Strategy.

4.3. Establish Enterprise Approach to Security Policy and Governance.

4.4. Establish Security Capabilities and Infrastructure for layered Security of Mission-Critical Systems and Data.

4.5. Foster a Security Awareness and Adoption among the Government Workforce.

CHAPTER - 2

SECURITY ARCHITECTURE FRAMEWORK - TAMIL NADU (SAF-TN)

CHAPTER - 2

SECURITY ARCHITECTURE FRAMEWORK - TAMIL NADU (SAF-TN)

1. The Security Architecture Framework of Tamil Nadu (SAF-TN) defines the overall ambit of the Cyber Security related Agencies in Tamil Nadu. The Cyber Security Architecture of Tamil Nadu (CSA-TN) is being executed by ELCOT in association with the Centre for Development of Advanced Computing (C-DAC), Chennai. The major components that constitute the CSA-TN are :-

   (a) Security Architecture Framework (SAF-TN)

   (b) Security Operations Centre (SOC-TN)

   (c) Cyber Crisis Management Plan (CCMP-TN)

   (d) Computer Emergency Response Team (CERT-TN)

2. The Architecture is an overall framework that allows Government Departments to access Central Resources of Audit, Compliance, Incident Handling Assistance and Monitoring without hampering their unfettered ownership and handling of their resources.

3. It is emphasized that while Policy remains consistent, several aspects of the Architecture will be dynamic in adapting to technological changes.

CHAPTER - 3

BEST PRACTICES - GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE

CHAPTER - 3

BEST PRACTICES - GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE

1. The Best Practices and Guidelines for maintenance of IT Assets have been drawn from Industry Guidelines, Security Policies of various Organizations and other Public Domain Repositories.

2. The Policies are indicative in nature and may be treated as minimum mandatory requirements.

3. The Security Policies of each Department will follow these Guidelines and Best Practices, as customised to their specific assets. The Departmental Chief Information Security Officers (CISOs) will generate the Security Policies for the Assets under their control, seeking the help of Information Technology Department, if necessary.

4. The Guidelines and Practices will themselves adapt to changes and the latest version will be available online in the CERT-TN Portal. The Policies / Guidelines listed in the Portal will pertain only to the IT Security aspects and will not infringe on the other aspects of the process involved (eg. Procurement Policy). Therefore, Policies that overlap multi-entity responsibilities and Policies that need Enforcement Regulations will be added once they are approved by due process.

5. Procurement Policy

a) To create and maintain testing infrastructure and facilities for IT Security Product Evaluation and Compliance Verification as per global standards and practices.

b) To build trusted relationships with Product / System Vendors and Service Providers for improving end-to-end supply chain security visibility.

c) 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

d) To encourage entities to adopt Guidelines for Procurement of Trustworthy ICT Products and provide for procurement of indigenously manufactured ICT Products that have security implications.

6. e-Mail & e-Mail Retention Policy

6.1 It is very much essential to have an e-Mail Retention Policy in all the Servers of Tamil Nadu Security Operations Centre (SOC) for a number of reasons – the major two reasons being the need to save space on e-Mail Server and the need to stay in line with Federal and Industry Record-Keeping Regulations. The first stumbling block is that different Departments will advocate for different retention windows.

6.2 The recommended Retention Periods may vary significantly, based on the Industry the Servers belong to and the Geo-location of the Servers. For Tamil Nadu, the e-Mail Retention Policy is designed in such a way that Spam Messages are never retained, General Correspondence is retained for 5 years, Administrative and Human Resource for 7 years, and then Invoices, Sales Records and CEO Correspondence is kept for a period of 10 years or forever.

6.3 By implementing proper e-Mail Retention Policies, it will be possible to track the outbound, inbound and internal communication to ensure compliance. e-Mail Archiving Solutions allow the Admin to define e-Mail Retention Policies based on various criteria (Type of data, Regulations, Department Preferences), retain the e-Mail as long as necessary and then purge the information only after the retention period expires in order for the data not to become an unnecessary liability. For instance, if a Policy is set to last for 7 years, the delete functionality will make sure that all e-Mails are automatically deleted, immediately after the retention period expires.

7. Social Media Policy

7.1 A Social Media Policy describes how the Government Departments and its employees should conduct themselves via the Web. It helps to protect the online reputation of the Department.

7.2 **Online Social Media Activities:** Let the subject matter experts respond to negative posts. An employee may come across negative or disparaging posts, or see third parties trying to spark negative conversations. Unless they are a certified Online Spokesperson, avoid the temptation to react Pass

the post(s) to the Official Spokespersons who are trained to address such comments.

7.3 **Protect Information:** Since Profiles on Social Network are linked more often to individuals and not Organisations, for the Organisation's site/ page, a separate Work Profile may be created which can then be linked to a general e-Mail Address and made accessible to anyone in the Team, enabling them to administer the Social Networks without compromising individual privacy.

7.4 **Be Transparent and Disclose:** If the Departments/Agencies are collecting personal information on a Social Media Platform, the same must be stated upfront. For example, while seeking inputs on a particular Policy, it may not be necessary to save the e-Mail ID of each and every respondent and just saving the responses may suffice.

7.5 **Social Media Account Ownership:** There have been legal disputes over who owns a Social Media Account and the followers of an Organization Account in the past. The Department should clearly define the boundaries for the employee over account ownership.

8. Password Policy

8.1 Reusing passwords or using the same password for all the Servers in Government Departments is like carrying one key that unlocks the House, Car, Office, Briefcase and Safety Deposit Box. If the same passwords are reused for more than one Computer, Account, Website or other Secured Systems, then all such systems will be only as secure as the Least Secured System.

8.2 **Enforce Password History Policy:** The Enforce Password History Policy will set how often an old Password can be reused. It should be implemented with a minimum of 10 previous Passwords remembered. This Policy will discourage users from reusing a previous Password, thus preventing them from alternating between several common Passwords.

8.3 **Minimum Password Age Policy:** This Policy determines how long, the users must keep a password, before they can change it. The Minimum Password Age will prevent a user from dodging the Password System by using a new Password and then changing it back to the old one. To prevent this, a specific minimum age should be set, making sure that users are less prone to switching back to an old password, but are still able to change it in a reasonable amount of time.

8.4 **Maximum Password Age Policy:** The Maximum Password Age Policy determines how long, the users can keep a Password before they are required to change it. This Policy forces the user to change the passwords regularly. To ensure a Network's Security, the value shall be set to 90 days for Passwords and 180 days for Passphrases.

8.5 **Minimum Password Length Policy:** This Policy determines the minimum number of characters needed to create a Password. It is generally required to set the Minimum Password Length to atleast eight characters since long passwords are harder to crack than short ones. For even greater security, the minimum password length could be set to 14 characters.

8.6 **Passwords Must Meet Complexity Requirements Policy:** The Passwords Must Meet Complexity Requirements Policy enables to go beyond the basic password and account policies and ensure that every password is secured following these guidelines:

(a) Passwords can't contain the user name or parts of the user's full name, such as their first name.

(b) Passwords must use at least three of the four available character types: Lowercase Letters, Uppercase Letters, Numbers and Symbols.

8.7 **Reset Password:** The Local Administrator Password should be reset every 180 days for greater security and the Service Account Password should be reset at least once a year during maintenance time.

8.8 **E-Mail Notifications:** Create e-Mail Notifications prior to password expiry to remind the users when it's time to change their passwords before they actually expire.

8.9 **Password Audit Policy:** Enabling the Password Audit Policy allows one to track all password changes. By monitoring the modifications that are made, it is easier to track Potential Security Problems. This helps to ensure user accountability and provides evidence in the event of a security breach.

CHAPTER - 4

COMPUTER EMERGENCY RESPONSE TEAM TAMIL NADU (CERT-TN)


****
OK

CHAPTER - 4

COMPUTER EMERGENCY RESPONSE TEAM – TAMIL NADU (CERT-TN)

1. Overview

1.1 The CERT-TN is the essential Nodal Agency for implementation of the Security Architecture Framework (SAF-TN). This Section lays down the Policy for the direction of the CERT-TN operation.

1.2 CERT-TN shall ensure timely and quality service to the Departments by Monitoring, Detecting, Assessing and Responding to the Cyber Vulnerability, Events causing Cyber Threats, Incidents and demonstrate Cyber Resilience.

1.3 Any external disclosure of Information Security Incident's Data must be reviewed and approved by the Competent Authority. CERT-TN should coordinate with State or National Computer Security Incident Response Teams (CSIRTs), Government Agencies, Law Enforcement Agencies, Research Labs or Information Analysis Centres. The CERT-TN is authorized to share Vulnerability, Incident or Artifact that identifies specific Information Asset of the Government Departments post specific approval of the Government.

Governance Risk and Compliance

1.4 CERT-TN in compliance with National and State Law shall act as a Statutory Body issuing Directives, Guidelines and Advisories to enforce Cyber Security Practices to the Departments. Government Departments and CERT-TN shall organize Cyber Security Preparedness Exercise and Emergency Evacuation Drill.

Security Policy

1.5 CERT-TN will establish, operate, maintain, monitor and improve the Information Security Management System to ensure Confidentiality, Integrity and Availability of its Data, Information, Information Systems, Operation and Facilities used to offer Services to the Government. CERT-TN Services shall demonstrate Security Best Practices in compliance with the legal and regulatory requirements.

Coordination Centre (CoC)

1.6 Coordination Centre (CoC) shall be the Nodal Intermediary between the CERT-TN and the Departments, CERT-In, State CERTs, Law Enforcement Agencies (LEA), Media and other Stakeholders in Service Delivery and in Cyber Crisis Management. CoC shall regularly monitor to address the Service Request, Delivery Timeliness, Quality, Disputes and Performance Improvement.

Incident Handling and Response (IHR)

1.7 Cyber incidents shall be promptly handled by the appropriate level of expertise for Receipt, Ticketing, Triage, Analysis and develop Containment or Response Plan to build a resilient ICT Infrastructure.

1.8 Standard Operation Process Manual must be appropriately documented, reviewed, approved and be up-to-date to support the activities of IHR.

1.9 Standards for prioritizing Cyber Incidents shall be defined based on the criticality of the affected resource and the impact the incident has on the Constituent. Response Expectation should be stated by the Incident Priority Level.

1.10 Data collection for Incident Analysis should be adaptive to necessity. Relevant Data should be collected and should exclude the Data not directly relevant. The Data lifecycle shall be in accordance with legal and regulatory requirement and maintain a fool-proof chain of custody.

Coordinated Vulnerability Disclosure Policy

1.11 The Incident Reporters may disclose newly discovered vulnerabilities in Software, Hardware, Online Application or Services affecting the Government Departments directly with the CERT-TN or with the respective Vendors.

1.12 The vulnerabilities in the affected e-Governance Service offered by the Government of Tamil Nadu shall be reported only to CERT-TN or to the respective Department. The Incident Reporter shall be supported to share the evidence of the vulnerability securely and shall not publish the vulnerability publicly until the Department or CERT-TN resolutions are available and affected Systems are controlled.

1.13 The Incident Reporter reporting in good faith will not be penalized, provided he cooperates with the stakeholders in resolving the vulnerability and minimizing the impact due to the Vulnerability. However, the Incident Reporter shall not attempt actions that could compromise the System, ex-filtrate Data, affect system availability or are intrusive in nature. CERT-TN shall coordinate with the suitable Agency to develop a patch, update or remove or mitigate the vulnerability, develop workaround and communicate advisories through authentic medium. The Incident Reporter's contribution in vulnerability discovery and resolution shall be credited publicly by the CERT-TN.

Vulnerability Handling Policy

1.14 Vulnerability shall be promptly handled by the appropriate level of expertise for Receipt, Ticketing, Triage, Analysis and develop Containment or Response Plan to build a resilient ICT Infrastructure.

1.15 The vulnerability resolution shall be communicated to the owners expeditiously. The reported vulnerability shall be contained immediately and the Department or the Vendor should patch the vulnerability within 30 days on the affected systems.

2. Security assessment of Department Assets

2.1 The Government's Critical Information Infrastructure (CII) shall be regularly assessed by CERT-TN for Security and Resilience Maturity through announced and unannounced engagements. The Department Nodal Officer shall liaison and provide user level and/or system level access to any computing, processing, storing or communication devices, access to log traffic, records or to monitor access to work areas or premises.

2.2 CERT-TN shall carry regular automated vulnerability scanning of the IT Assets in a non-intrusive manner. The effort may consider an authenticated scan to ensure accuracy without disrupting the operation. The scans shall be monitored by the experts to validate the reports manually. These may be unannounced.

3. Help Desk, Training and Communication

3.1 The Help Desk shall validate the contact of Nodal Officers of the constituent, State CERTs, CERT-In and update any changes monthly.

3.2 The helpdesk shall intake report for Incident, Artifact or Vulnerability only through the approved channels of CERT-TN. The report intake shall record and verify the reporter's identity as practicable.

3.3 The Helpdesk, on receipt of non-serving request, may direct it to relevant sources or shall convey 'out of scope' as response. All reports shall return the 'Report Identifier' to the Incident Reporter for further correspondence.

4. Training and Awareness Policy

4.1 The CERT-TN Team shall be trained on the respective Service Operation Processes, Procedures and Practices. The members should be subject to Refresher Training Program as required. The Team should be made aware of the Policy, Roles, Responsibilities and encourage adherence. They shall be subject to periodic General Quality and Security Awareness Program.

4.2 CERT-TN shall develop, update or deliver Awareness Program on Information Security Responsibilities, CCMP, Incident Response or Security Hygiene through Classroom or Massive Open Online Courses

(MOOC) for Government Officials and Public.

4.3 CERT-TN shall release timely Alerts and Advisories on Security Issues, Vulnerabilities and Exploits, Announcements, News Bulletins, Tips and Periodic Reports on its official Portal and Social Media Handles.

5. Department Policy

5.1 The Department, Organization or Body under the administrative control of the State Government of Tamil Nadu shall be a constituent of CERT-TN and the documents issued by the CERT-TN shall be directly applicable to the Constituents.

5.2 The Constituent shall be on-boarded through an Initial Cyber Security Preparedness and Maturity Assessment. They shall be graded by maturity of Cyber Security Practices and Resilience Strength by the Key Performance Indicators (KPIs).

CHAPTER - 5

CYBER CRISIS MANAGEMENT PLAN (CCMP)

CHAPTER - 5

CYBER CRISIS MANAGEMENT PLAN (CCMP)

1. Cyber Crisis Management Plan (CCMP) for countering Cyber Attacks and Cyber Terrorism has been proposed by CERT-In, Ministry of Electronics and Information Technology, Government of India. It emphasizes establishing strategic framework and actions to prepare for, respond to, and begin to coordinate recovery from a Cyber-Incident. CCMP provides Guidelines for handling Cyber Security-related crises like Cyber-Attacks and Cyber Terrorism.

2. CCMP is a process that will be technically addressed through Incident Handling and Response (IHR), Help Desk and Co-ordination Centre Services of the CERT-TN operation. Government of Tamil Nadu have constituted two Committees namely, the High Level Security Governance Committee and Technical Committee for Security Governance.

3. The State Government mandated the organizational structure for the CCMP. Under the CCMP, there will be Crisis Management Group (CMG) for each Department as follows :-

   (a) Secretary to Government as Chairman

   (b) Heads of all Organizations under the administrative control of the Department

   (c) CISO's / Deputy CISO's within the Department.

4. The Roles & Responsibilities of CMG will be as follows :-

   (a) Co-ordinate with CERT-TN during crisis situation

   (b) Deal with Cyber Crisis at Level 3 and report developments to the State Crisis Management Committee (SCMC)

   (c) Seek directions and guidance as and when required from the SCMC

(d) Ensure that all the directions that are obtained from the SCMC are implemented properly.

(e) Prepare detailed Contingency Plan in consultation with CERT-TN

(f) Periodically revise and update the contingency plan and submit to the SCMC and CERT-TN

(g) Conduct periodic review to ensure that the Crisis Management Cell (CMC) is implementing the directions provided.

5. Each organization will have a Crisis Management Cell (CMC) as follows :-

(a) Head of the organization

(b) CISO

(c) Head of HR / Admin

(d) In-Charge of IT Section

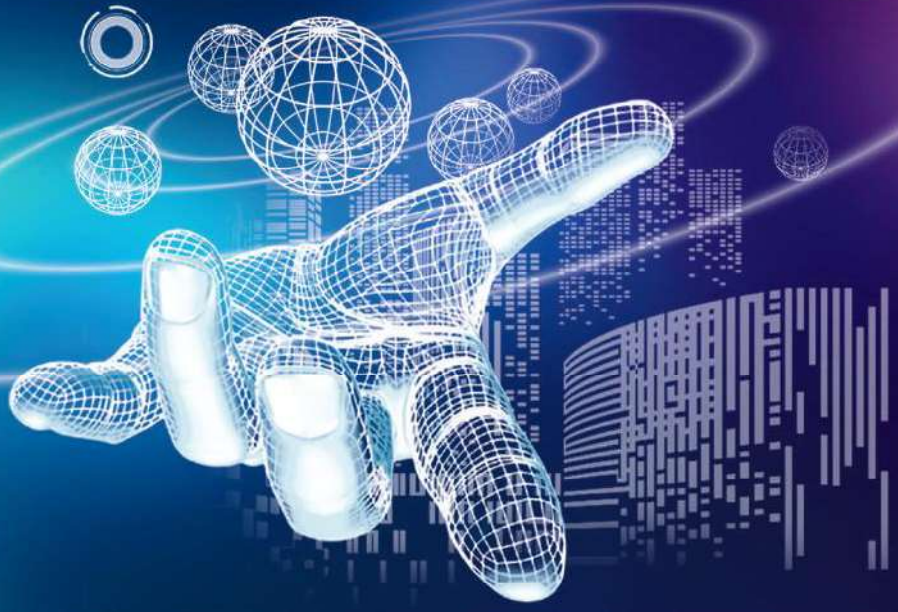
6. Each organization shall identify a senior officer preferably with adequate IT experience and nominate him/her as Chief Information Security Officer (CISO).

7. The priority of the CMC is to detect any possible fall-back or contingency scenario that would allow preserving continuity of operation or speedily restoring an acceptable level of service. The organizational CMC will co-ordinate with the respective CMG in crisis situation.

Disclaimer:

For all Stakeholders of the Tamil Nadu Cyber Security Policy-2020, this Policy document supersedes all prior Policy documents on e-Security and other orders and practices followed on Cyber Security.

GOVERNMENT OF TAMIL NADU



ELCOT

Adding value through IT

प्रगत संगणन विकास केंद्र
सी डैक
CDAC
॥ ज्ञानादेव तु केवल्यम् ॥
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING