ABSTRACT

Information Technology Department – E-Security Policy of Tamil Nadu 2010 – Approved - Orders Issued.

Information Technology (B4) Department

G.O.Ms.No.42 **Dated: 24.9.2010**

ORDER:

While moving the 'Demand No.31 - Information Technology Department' in the Tamil Nadu Legislative Assembly during the Budget 2009-2010, the Hon'ble Minister for Information Technology made an announcement that "E-Security Policy" will be released in 2009-2010.

2. With the increasing use of Information Technology, functions in Government are now dependant on a network of critical information infrastructure. As such, any disruption of operation of information systems of critical infrastructure will have a devastating effect on citizens, economy and Government services. In view of the potential impact, protection of critical information infrastructure is essential to ensure that disruptions are of minimal duration, manageable and cause the least damage possible.

3. Security relates to the protection of valuable assets against loss, misuse, disclosure or damage. In this context, "valuable assets" are the information recorded on, processed by, stored in, shared by, transmitted or retrieved from an electronic medium. Such information must be protected against harm from threats leading to different types of vulnerabilities such as loss, inaccessibility, alteration or wrongful disclosure. Threats include errors and omissions, fraud, accidents and intentional damage.

4. Protection arises from a layered series of technological and non-technological safeguards such as physical security measures, background checks, user identifiers, passwords, smart cards, biometrics and firewalls. These safeguards should address both threats and vulnerabilities in a balanced manner.

5. In the ever-changing technological environment, security must keep pace with these changes to enable organisations to operate in an environment of 'trust and confidence'. Security must be dealt within a proactive and timely manner to be effective.

6. For most organisations, the security objective is met when:

- Information is available and usable when required, and the systems that provide it can appropriately resist attacks and recover from failures (*availability*)
- Information is observed by or disclosed to only those who have a right to know (*confidentiality*)
- Information is protected against unauthorised modification (*integrity*)
- Business transactions as well as information exchanges between organisation locations or with partners/users can be trusted (*authenticity and non-repudiation*)

7. With this in mind the Government of Tamil Nadu sets forth its E-Security Policy which is focused on Government Departments, Government undertakings and related agencies.

8. A core committee was formed under the guidance of the Principal Secretary, Information Technology Department and Managing Director of ELCOT for developing a Baseline Information Security Policy for Government of Tamil Nadu. This Information Security Policy is a statement of the minimum requirements required to establish and maintain a secure environment and achieve Government of Tamil Nadu's information security objectives. This policy shall serve as a best practice for all the Departments under the Government of Tamil Nadu Information Technology Infrastructure. All Departments shall develop detailed procedures that are relevant to their respective department's assets based on these guidelines.

9. Where conflicts exist between this policy and department's policy, the more restrictive policy will take precedence. The Information Security Policy encompasses information on all systems automated and manual, including systems managed or hosted by third parties on behalf of the department. It addresses all information, regardless of the form or format, which is created or used in support of Government Department's processes and procedures. This policy must be communicated to all departmental officers and others who have access to, manage, or have responsibility concerning Information Technology (IT) applications and systems.

10. The department-specific Information Security Policy is solely meant for internal circulation and all users shall hold the responsibility to keep it highly confidential. Any confidential information or material derived from here would need to obtain permission from the HOD after signing of a Non-Disclosure Agreement (NDA).

11. A Detailed booklet containing the "E- Security Policy" is annexed to this Order.

12. The implementation and monitoring in respect of this Policy shall be done by the Directorate of e-Governance in consultation with Government in Information Technology Department.

(BY ORDER OF THE GOVERNOR)

P.W.C.DAVIDAR
PRINCIPAL SECRETARY TO GOVERNMENT

To
All Departments of Secretariat, Chennai-9.
The Director, Directorate of e-Governance, 3rd floor, TUFIDCO-POWERFIN Building, 490/3, Anna Salai, Nandanam, Chennai - 35
The Chief Executive Officer, Tamil Nadu e-Governance Agency , 3rd Floor, TUFIDCO-POWERFIN Building, 490/3, Anna Salai, Nandanam, Chennai - 35
The Managing Director, ELCOT, Chennai-35.
The State Informatics Officer, National Informatics Centre, Chennai-90
The Chairman, Society for Electronic Transactions and Security [SETS], MGR Knowledge City, CIT Campus, Taramani Chennai - 600113
The Director of Information and Public Relations, Chennai -9.
The Works Manager, Government Central Press, Chennai-79.
(with a request to print 500 Copies)

Copy to :

The Secretary to Chief Minister, Secretariat, Chennai-9.
The Chief Minister's Office, Secretariat, Chennai 9.
The Secretary to Deputy Chief Minister, Secretariat, Chennai-9.
The Personal Assistant to Minister for Information Technology, Secretariat, Chennai-9.
The Personal Assistant to Minister for Finance,Secretariat, Chennai-9.
The Senior Private Secretary to Chief Secretary to Government, Secretariat, Chennai -9.
The Private Secretary to Principal Secretary to Government, Information Technology Department, Secretariat, Chennai -9.
SF/Scs.

/Forwarded by Order/

Section Officer

ANNEXURE TO G.O. (MS.) NO.42 DATED 24.9.2010

E-SECURITY POLICY 2010

GOVERNMENT OF TAMIL NADU

E- SECURITY POLICY
2010

TABLE OF CONTENTS

POLICY

The Government of Tamil Nadu is determined to maximize the gains of Information Technology in all Departments so as to improve its own administrative efficiency and at the same time make available online services to the people. This will ensure easy access and better monitoring in Government of actual delivery of services and thereby fulfill the basic expectations of the people with efficiency.

Considering that Information Technology will play a key role in the delivery of citizen centric services in the future, it becomes essential to ensure that all IT Security related issues are addressed. It is imperative that an E-Security Policy is released as a framework to be observed by all departments.

The purpose of this policy is to define a set of minimum information security requirements that shall be met by all departments of the Government of Tamil Nadu.

The Primary objectives of the Policy are to:

- Effectively manage the risk of security exposure within the department
- Communicate the responsibilities for the protection of IT applications and systems of Government and departments respectively.
- Reduce the opportunity for errors to be entered into an electronic system that supports procedures and processes of the department.
- Identify responsibilities of persons and steps to be taken in the event of an information asset misuse, loss of data or unauthorized disclosure.
- Promote, train and increase the awareness of information security in all departments.

The lead guidelines in implementing the policy of E-Security in Government are to be as follows:

1 The Information Security Policy shall be implemented, maintained and supported by the respective Head of the Department (Owner). The Director of e-Governance shall provide guidance wherever necessary.
2 Each Head of Department (HOD) shall designate two officers for implementing, enforcing and supporting the Information Security Policy as below:
    a Chief Information Security Officer (CISO)
    b Assistant Information Security Officer (Asst. ISO)
3 This document may be modified by each department according to their specific operations, processes, procedures, requirements

and citizen services in line with their e-Governance initiative. Each department may also use this policy as a parent document and create supporting documents in addition to this policy to address specific areas such as e-Mail Policy, Server Policy, Network Devices Policy, etc. This document shall be implemented in full if the department requirements are sufficiently met by this policy.

4 The Director of e-Governance may form a consultative group to assist departments in full compliance of the Information Security Policy. This group shall comprise of Government officials from NIC, CDAC, STQC, etc.

5 The respective departments are the owners of the processes, procedures, systems, applications and technologies and the information maintained in these systems even though they may be hosted elsewhere.

6 Each CISO and his/her team are responsible for providing education, training and assistance to employees in the department with respect to the Information Security Policy.

7 Provision of IT Security training to all IT personnel, computer administrators and users, IT Security staff, managers and other employees of each department.

8 Third-party IT Security Assessments of all IT devices, applications and assets shall be done annually.

The elements of the E-Security for all Government departments and related organisations are as follows:

- <u>Functional responsibility for E-Security with respective departments</u>
  To enable greater ownership and responsibility of all departments while utilizing Information Technology, the functional responsibility of developing and maintaining an E-Security policy shall vest with respective departments. The broad framework and guidelines developed herein shall guide each department but final accountability in finalizing and implementing a department specific E-Security Policy shall vest with respective departments.
- <u>Inventorisation of IT Assets</u>:
  Each department shall build an inventory of its IT assets and ensure both physical and environmental security
- <u>Testing and Scanning for Vulnerabilities</u>
  All IT applications that are inducted for departmental use and for Department - Citizen interface, shall as an indispensable precaution be subjected to testing and scanning for vulnerabilities both prior to large roll-out and at periodical intervals.

- Access control protocols and guidelines
  Access control protocols and guidelines for computer systems and software applications shall be laid out and staff of each department be trained and made aware of this. Apart from routine password formalities, super admin and admin access to the application will need to be monitored strictly.
- Guidelines for external connections:
  Considering the scope for departmental IT applications being influenced by third party unauthorized access and intrusions, guidelines as elaborated in the policy directives shall be followed in accessing wireless networks, external connections, portable devices together with the basic rules to be observed by Government /department staff while using the Internet.
- Information Access and Confidentiality levels:
  Access to Information shall be managed according to levels of confidentiality as determined by the authority structure in each department.
- Digital Signature
  While Digital Signatures are a natural process of e-Governance, each department will be required to identify its own levels at which the electronic signatures should be inducted and monitor its use apart from ensuring adequate training to the staff who have been entrusted with this authority.
- Independent development, testing & production environment
  The future of Governmental functioning will witness more and more IT applications being developed. The development, testing and production environment shall be separated from the actual deployment.
- Post- attack steps:
  While the entire focus of the E-Security policy in Tamil Nadu is on preventive and precautionary measures, in the event of E-Security being compromised, the policy based directives as laid out on the steps to be followed in a post-attack / intrusion scenario shall be strictly followed. The assistance of external agencies such as CERT-In, SETS etc shall be utilized in a routine manner to limit any damage on account of such unauthorized access or intrusion.

POLICY BASED DIRECTIVES

1. FUNCTIONAL RESPONSIBILITIES

1.1 Government Departments

Each department under the guidance of their respective HOD shall:

1. Establish a framework to initiate and monitor the implementation of information security within the department.

2. Nominate and train a Chief Information Security Officer (CISO) for every department. This officer should have adequate experience in the field of Information Technology.
3. Ensure the confidentiality, integrity, availability, and accountability of all Governmental information while it is being processed, stored, and/or transmitted electronically and the security of the resources associated with the processing functions.
4. Implement a third party Security Assessment and Penetration Test once every twelve (12) months for all devices and applications on the network in the department.
5. Develop and implement an IT Disaster Recovery Plan for critical IT Systems and review for relevance annually.
6. Establish a process to determine information sensitivity, based on best practices.
7. Ensure that the Head of each department will develop an organizational structure to
    a. Implement and maintain an information security program based on IT security standards, guidelines and procedures
    b. Implement a security awareness program.
    c. Identify security vulnerabilities within department systems and recommend corrective action.
    d. Develop a process to measure compliance with this policy.
    e. Communicate requirements of this policy and the associated Information Security Standards to third parties whenever required and address them in third party agreements.

1.2 Chief Information Security Officer (CISO)

The CISO assumes overall responsibility for ensuring the implementation, enhancement, monitoring, training and enforcement of the information security policies and standards for the department. The CISO is responsible for providing direction and leadership through:

1 Recommending, coordinating and implementation of information security policies, standards, processes, training and awareness programs; to ensure appropriate safeguards are implemented and to facilitate compliance with those policies;

2 Investigation of all alleged information security violations by following procedures and refer the investigation to other investigatory entities wherever necessary, including law enforcement agencies;

3 Provide consultation on security administration for the various computing platforms in a department to ensure proper implementation of security requirements;

4 Evaluate new security threats and countermeasures that could affect the department and make appropriate recommendations to the HOD and disseminate threats and controls to the Department to mitigate risks;

5 With the help of Asst. ISOs and System Administrators in the department, review preparedness for handling crisis per Incident Response Procedure in Appendix I and Appendix II. Complete the check lists in Appendix IV once every six months and file a hard copy of it for annual audit purposes;

6 Ensure appropriate security awareness and education to all employees in the department, including continuing education for existing IT staff and systems administrators in the latest technologies in IT security;

7 The CISO shall report to the HOD of the respective Department

1.3 Assistant Information Security Officer (Asst. ISO)

Asst. ISO in each department will be responsible for the implementation of the Information Security Policy and monitor the compliance of departmental employees to this policy. Asst. ISO is to educate employees with regard to information security issues and must explain the issues, such as why the policies have been established, and what role(s) they have in safeguarding information including consequences of non-compliance. Asst. ISO with the help of inside IT experts will monitor through the check list every month as per Appendix IV.

1 Asst. ISOs are responsible for ensuring that appropriate physical, logical, and procedural controls are in place on the assets to preserve the security properties of confidentiality, integrity, availability and privacy of departmental information

2 A report on suspected security incidents as and when it occurs to the appropriate manager and the CISO is to be submitted by the AISO

3 Monitor use of IT resources only for intended official purposes as defined by policies, laws and regulations

4 Monitor individual access to IT assets only to which they are authorized by the CISO

5 Asst. ISO will report to the CISO of the respective departments

1.4 Role of Head of Department

The Head of Department is responsible for the data processing infrastructure and computing network with the support of CISO, Asst. ISOs and others provided with computers to do office related work utilizing IT applications. It is his/ her responsibility to provide resources needed to enhance and maintain a level of information security control consistent with the department's Information Security Policy. The HOD will need to ensure:

1 That requirements, processes, policies and controls are identified and implemented related to security requirements as defined by departmental procedures

2 The participation of the CISO and Asst. ISOs in identifying and selecting appropriate, cost-effective security controls & procedures for ensuring information security.

3 That appropriate security requirements for user access to automated information are defined for files, databases, and physical devices.

1.5 Systems Administrator

System Administrators of respective departments in addition to their current responsibilities are responsible for:

1 Administering security tools, reviewing security practices, identifying and analyzing security threats and solutions and responding appropriately to security violations

2 Administration of all user-IDs and passwords and the associated processes for reviewing, logging, implementing access rights, emergency privileges and reporting requirements. (Note: Where a formal Security Administration function does not exist, the organization or officers responsible for the security administration functions described above will adhere to this policy. When such an individual or individuals exist, the individual or individuals will work closely with the Asst. ISOs and CISO of the department)

3 Report incidents to Law Enforcement Agency and maintain Incident Report forms as per Appendix III and Appendix IV within the document

4 Cyber crime incidents in Chennai city to be reported to the Commissioner of Police, Chennai and incidents outside Chennai to be reported to the Crime branch of Tamil Nadu Police and only then to be reported to CERT-In (refer Appendix III and IV within this document);

5 Information owners, Systems Administrators, other officers in IT related roles, IT users in the department will report to the Asst. ISO.

2. INFORMATION SECURITY MANAGEMENT

The purpose here is to identify Government sensitive information. Officers shall develop, train and implement standards, guidelines and procedures to protect intentional or unintentional unauthorized access, exposure, modification, destruction or loss of Government sensitive information.

2.1 Information Classification

Information shall be classified appropriately as applicable for each department into the following categories:

Top Secret:
It shall be applied to information unauthorized disclosure of which could be expected to cause exceptionally grave damage to the National/State security or National/State interest. This category is reserved for Nation's/State's closest secrets and to be used only in certain situations e.g. State security plans during elections, general State security plans, plans related to strategic sectors, passwords to protected systems, confidential records and so on.

Secret:
This is applied to information unauthorized disclosure of which could be expected to cause serious damage to the National/State security or National/State interest. This classification should be used for highly important information and is the highest classification normally used. e.g. Visits of VIPs, security arrangements during VIP visits and international events, information related to critical infrastructure such as configuration details of servers in data centers, etc.

Confidentiality:
This shall be applied to information unauthorized disclosure of which could be expected to cause damage to the security of the department or could be prejudicial to the interest of the department or could affect the department in its functioning.

Restricted:
This shall be applied to information which is essentially meant for official use only and which would not be published or communicated to anyone except for official purpose. The information under this category may be available to all the employees of the Government.

E.g. General employment related rules and policies including security policies, official circulars and the like.

Unclassified/Public:
Information in this category requires no protection against disclosure but may need protection against unauthorized modification and other security or integrity threats. e.g. Information published on departmental websites and so on.

The information or electronic files that may be classified into these categories will be specific to respective departments or organizations and proceedings issued accordingly.

Assign Responsibility for Asset
Each of the IT hardware must have a designated person who will be responsible for ensuring appropriate protection from unauthorized intentional, unintentional use, access, disclosure, modification or loss.

Build an Inventory of IT assets
At the minimum IT asset inventory must contain:

a List of all department IT hardware – Hardware documentation register
b Criticality of hardware in levels of importance
c System software and development tools on these assets;
d Access restrictions.

2.2. Contingency Planning

Contingency planning is required to prevent interruptions to normal operations for critical Government processes and procedures. Such interruptions could be due to natural disasters or man-made failures. An appropriate contingency plan with a standard response chart must be drawn up by each department.

2.3 Physical and Environmental Security

Certain procedures need to be institutionalized to ensure that only authorized access is made to IT infrastructure and particularly wherever servers, computers etc are placed. If necessary, bio-metrics/card readers or other appropriate methods may be introduced.

a. Environmental hazards such as fire, water and electrical fluctuations need to be factored in, while ensuring security of IT equipment.

b. The above threats need to be taken into consideration in electrical supply to such IT equipment inclusive of the cabling infrastructure.
c. To the extent possible, formal processes need to be in place for both disposal of old IT equipment and constant use of storage devices such as hard disk drives, pen drives and others.
d. Disposal or Re-use of Storage Media and Equipment:

   Formal processes must be established to minimize risk of disclosure through careless disposal or re-use of equipments such as storage devices (e.g. tape, diskette, CDs, DVDs, cell phones, digital copiers or other devices that store information)

2.4 Connectivity and Communication

2.4.1 Network Management

All departments will need to implement a range of network controls to maintain security in its internal network. All departments shall eventually migrate their data to a centralized data center hosted by ELCOT by using Tamil Nadu State Wide Area Network (TNSWAN). All departments that utilize the TNSWAN and consequently the ELCOT Data Center at Perungudi will require strict adherence to directives issued by the offices from time to time.

2.4.2 Vulnerability Scanning

Vulnerability Scanning and Penetration/Intrusion Testing will need to be done by either a Government body or a third party. This third party should neither be a Hardware vendor/dealer nor one selling IT security related hardware/software. Such vulnerability assessment will need to be comprehensive and must cover all devices and applications that form the departmental network (100% coverage). This includes servers, desktops, printers, routers, IP Telephones, Switches, web applications, databases, web servers, etc. This exercise becomes relevant whenever new network software or when major configuration changes have been made on the systems, network or the applications.

Analysis and testing will need be used to determine if an individual can make an unauthorized change to a system, network or an application; this will include the possibility of an unauthorized individual who may access and destroy or change any data or make it perform those originally unintended by the designer. In the process if vulnerabilities are detected, the risk involved will have to be mitigated. Information Technology department with assistance from ELCOT may empanel,

recommend or identify such third party vendors who would carry out the security assessments. Following reports by third parties and from internal efforts, appropriate preventive and precautionary steps may be taken to ensure adequate security.

2.4.3. Rules while connecting to Internet

A staff member/officer in Government utilizing a Government IP address while connecting to the Internet or sending mail, shall do so only for purposes determined by the concerned departments. The Internet connection shall not be used

a. for sending unsolicited email messages or sending of junk mail or the like.
b. for hacking into the computer system of the department/Government or any other organization.
c. for unauthorized copying or theft of electronic files.
d. for passing on sensitive information of the Government without authorization.
e. for sending of chain letters, religious images or messages or the like which may also lead to denial of service.
f. for circulating letters, appeals or any content that is likely to create ill-will, hatred, violence or damage the image of the Government.
g. for posting non-official related messages, groups on the Internet.
h. for introduction of malicious programs into the network or server such as Viruses, Worms, Trojan, email bombs and the like.
i. for any form of harassment via email.
j. for violation of any Government policy protected by copyright act, trade secret, patent or other intellectual property.
k. for exporting software, technical information, encryption software or technology
l. for revealing the user name and password to others or allowing the use of the account by others.
m. for transmitting or viewing any material that is pornographic in nature or contributes to sexual harassment.
n. for port scanning or sniffing (i.e., monitoring network traffic) except for those authorized to do so as part of their job.
o. Blogging by officers and employees, whether using departmental systems or personal systems, is subject to terms and restrictions. Blogging from departmental systems is subject to monitoring by the department. Employees shall not engage in any Blogging that may harm or tarnish the image of

the department. Employees should represent themselves while Blogging and shall not represent themselves as a representative of the department.

2.4.4 External Connections

Any connection from the Government network to an external network (wired or wireless) should be done or permitted only after the third party network / account has been approved by the system administrator or the officer in charge of information security in the department. Such clearances may be given after it is ascertained that the network / account has acceptable security controls, appropriate security measures and procedures (firewalls, filters etc) are in place. The integrity of the Government and department network should be preserved.

The System Administrator or the Information Security Officer will need to regularly review audit trails and system logs of external network connections for abuses and anomalies.

2.4.5 Security of Electronic Mail

Electronic Mail provides an expedient method of creating and distributing messages both within and outside the organization. Users, employees and officers of the Departmental e-mail system are visible representatives of the State and must use the systems in a legal, professional and responsible manner. Commercial Mails (Yahoo, Gmail, Hotmail etc.) may be accessed only when immediate superior gives prior approval if it is found to be necessary.

2.4.6 Portable Devices

Portable devices ranging from laptops, notebooks, mobile phones, pen drives etc will need to be secured to prevent compromise on the integrity of the department's systems. Periodic back up may be necessary. Basic procedures and precautions are required while connecting mobile facilities to the networks.

2.4.7 Wireless Networks

Wireless is a shared medium. Everything that is transmitted over the radio waves can be intercepted if the interceptor is within the coverage area of the radio transmitters. This represents a potential security issue in the wireless Local Area Networks (LANs). The security exposure is more evident if the wireless LANs are deployed or used in public areas such as airports, hotels or conference centers;

1 No wireless network or wireless access point shall be installed without a risk assessment being performed and the written approval of the CISO given.
2 Suitable controls such as address restriction, authentication, and encryption must be implemented to ensure that a wireless network or access point cannot be exploited to disrupt Departmental information services or to gain unauthorized access to Departmental information. When selecting wireless technologies, 802.11x wireless network security features on the equipment must be available and implemented from the beginning of the deployment;
3 Access to systems that hold GSI or the transmission of GSI via a wireless network is not permitted without appropriate approval by the CISO. Such measures must include authentication, authorization, encryption, access controls, and logging.

2.4.8 Mobile / Smart Phone

With the demand for constant connectivity while on the move, smart phones have emerged as an instrument of choice, for many Government officials.

The mobile phone devices with improved messaging features have gradually evolved to offer functionality equaling a desktop computer. In light of such advancements Government have also proposed to actively integrate such devices into its network to improve their process flow. However, integration of such mobile devices poses a threat towards the information security if allowed unrestricted. Such smart phones and related devices should be regularly screened for applications that are deemed to be dangerous.

2.4.9 Modem Usage

Connecting dial-up modems to computer systems which are also connected to the department's local area network or to another internal communication network is prohibited unless the CISO gives a written approval; a risk assessment is performed and risks are appropriately mitigated.

2.4.10 Other Steps for Securing IT Infrastructure

a Develop a Technology and Security patches Upgrade Policy for the development, which includes but is not limited to operating system upgrades on Servers, Routers, and Firewalls.
b Develop a Firewall Configuration Policy for the department, which must require creation and documentation of a baseline configuration for each firewall, updates of the documentation

for all authorized changes, and periodic verification of the configuration.

c Develop a Server Configuration Policy for the department which must clearly address all servers that have any interaction with Internet, Extranet or Intranet traffic.

d Develop a Server Hardening Policy for the department which must cover all servers throughout the department. Further, the policy must address and be consistent with the department's policy for making security upgrades and security patches.

e Develop a Software Management and Software Licensing Policy for the department which must address acquisition from reliable and safe sources and must clearly state the department's policy about not using pirated or unlicensed software.

f Ensure that the use of peer-to-peer technology for any non-Governmental purpose is prohibited. This includes, but is not limited to, transfer of music, movies, software, and other intellectual property. Governmental use of peer-to-peer technologies must be approved by the HOD and CISO.

Tamil Nadu e-Governance Agency (TNeGA) shall play a key role in the formulation of the above policies which may be in turn adapted by each department for its own use.

2.4.11 Electronic Signatures

Digital signatures have the same validity as a signature affixed by hand. Each department shall identify the levels at which final orders are passed and shall then process those identified for digital signatures with the signature authority resource. (Certain agencies have been authorized to issue Digital signatures eg. NIC etc.)

3 OPERATIONS

3.1 Segregation of Security Duties

Segregation of duties is required to reduce the risk of accidental or deliberate system misuse. Whenever separation of duties is difficult to achieve, other compensatory controls such as:

1 Monitoring of activities

2 Audit trails

3 Management supervision must be implemented. At a minimum the security audit must remain independent and segregated from the security function.

3.2 Separation of Development, Test and Production Environments

1 Development software and tools must be maintained on computer systems isolated from the production environment or separated by access controlled domains or directories.

2 Logon procedures and environmental identification must be sufficiently unique for production testing and development.

3 Development and testing can cause serious problems to the production environment if separation of these environments does not exist. The degree of separation between the production and test environments must be considered by each department to ensure adequate protection of the production environment.

3.3 System Planning and Acceptance

Storage and memory capacity demands must be monitored and future capacity requirements projected to ensure adequate processing and storage capability is available when needed. This information will be used to identify and avoid potential bottlenecks that might present a threat to system security or user services.

3.4. Protection against Malicious Code

Software and associated controls must be implemented across departmental systems to prevent and detect the introduction of malicious code. The introduction of a malicious code such as a Computer Virus, Network Worm Program and Trojan Horse can cause serious damage to networks, workstations and Government data.

3.5 Software Maintenance

1. All system software must be maintained at a vendor-supported level to ensure software accuracy and integrity, unless CISO approves otherwise in writing.
2. Maintenance of software developed by the department will be logged to ensure changes are authorized, tested, and accepted by the CISO.
3. All known security patches must be reviewed, evaluated and appropriately applied in a timely manner to reduce the risk of security incidents that could affect the confidentiality, integrity and availability of departmental data or software integrity.

4 ACCESS CONTROL

4.1 User Registration and Management

1. Each department will need to formalize a set of processes that will manage users effectively. This will include:
    a) Enrolling of new users
    b) Granting and removing privilege accounts to users
    c) Periodic review of users privilege accounts
    d) Processing and resetting of passwords
2. The level of users being able to access information as against accessing and modifying information will need to be determined by the HOD and/or Secretary concerned.
3. In departments where external users are required to be registered, the scope of access will need to be appropriately determined. Accordingly, standards and procedures must be designed by each department.
4. Privilege Accounts will need to be monitored carefully and any suspected misuse must be properly investigated. In all multi-user privilege accounts, the passwords must be changed more frequently.
5. Users Password Management:

    Whether it be an individual computer, system, LAN or a Network, a system of authentication is necessary. Passwords are most commonly used to ensure authorized access to an information system or service. Therefore, proven password management practices are essential to ensure that the IT system is secure. Some of the best practices for password management are listed below.

    a) Passwords should be kept confidential.
    b) Passwords should not be stored in clear text, must never be written down or stored online.
    c) At the first logon, temporary passwords must be changed.
    d) Password must be changed at regular intervals, i.e. atleast once in six months.
    e) Common passwords such as family name, date of birth, pet names, friends name, spouse's name, company names or number patterns such as 123456, 336699 etc should be avoided.
    f) Avoiding including passwords in any automated logon process ie. stored in a macro or function key, web browser or in application code.

6. User Authentication – Advanced.

   All remote connections to a computer must be made through managed central points of entry. Also, when the computers, networks etc are being accessed by a vendor or a maintenance person, such access will need to be logged. Such user-ids should be deactivated after the maintenance period to ensure that unauthorised use or access is not permitted.

   a) A secure network, when connected to another network, would need to have proper controls in place with routers, switches, firewalls and the like to control access.

   b) Access to the source code, services and commands must be restricted only to those who have been given responsibilities concerning it. Similarly, all functional applications must be accessed only by those whose job description requires them to do so.

   c) Regular monitoring and analysis is necessary to detect deviation from the access control policy. Regular Audit logs are necessary.

   d) Encryption is an important security layer to protect confidentiality of information and in certain cases multiple encryption levels will need to be built in. The cryptography used to encrypt and decrypt information will need to be stored in a secure manner. Access to the keys will need to be selective, as a compromise in this can lead to greater damage.

4.2 Logon Banner

Logon banners must be implemented on all systems where that feature exists, to inform all users that the system is for all department's processes and procedures. Logon banners are usually presented during the authentication process. Users will be notified that their actions will be monitored.

5. APPENDIX

5.1 . Appendix I

Incident Response activities during the First Hour

1. Introduction
   The primary objective of incident response actions during the first hour is to contain the damage due to the incident, notify appropriate authorities about the incident and ensure continuity of essential activities and services of the organization. The following guidelines describe the actions to be taken within the affected organisation during the first hour of the incident. The guidelines also facilitate detailed incident analysis and determination of recovery and response actions and possible escalation within and outside the organisation.

2. Triggers for First Reaction
   The reaction by the users or administrators within an organisation could be triggered by observation of certain symptoms and anomalies in the functioning of Systems, networks and processes. The trigger for response action could be infection, attack or intrusion or malfunctioning of a system. Further, the actions could be triggered when alerts are received from external organizations such as CERT-In and other Incident Response teams and security agencies. The anomalies and abnormal conditions that require response actions need to be detected by Users, System/Network Administrators, technical tools and external alerts from security agencies such as CERT-In.

3. Symptoms of incidents and response actions
   Table 5.1 outlines the general symptoms indicating occurrence of incident noticeable by all types of users, source of detection, response actions required and persons responsible for the actions.

   Table 5.2 outlines indications of different types of Cyber Crisis generally noticeable by trained users, System Administrators & tool based detection mechanisms and response actions required and authorities responsible for the actions.

4. Immediate Action:
   a. The users observing the symptoms/indications mentioned in Table 5.1 and 5.2 shall immediately report the same to the concerned System/Network Administrator or designated authority within the

organisation.

b. The System/Network Administrators shall escalate the reports of incidents affecting or could affect critical business functions or services to appropriate authorities within the organisation, local Incident Response Team, local law enforcement authority and CERT-In.

c. Cyber Crime incidents in the city of Chennai shall be reported to Commissioner of Police, Chennai and incidents outside Chennai may be reported to the Crime branch of Tamil Nadu Police. After reporting to the appropriate law enforcement authority, CERT-In shall be informed.

d. After the response actions within 1st hour of incident, the procedures and actions described in the Appendix III "Incident response during first 24 hours" need to be followed for detailed incident analysis and follow-up actions.

5. Scope for complaint to CERT-In

The following cyber security incidents shall be reported to CERT-In in the format prescribed in Appendix I, within one hour of occurrence of the incident or noticing the incident.

- Targeted scanning /probing of critical networks /systems networks
- Compromise of critical Systems/Information
- Unauthorised access of IT Systems/Data
- Defacement of website, intrusion into a website, unauthorized changes such as insertion of malicious code, links to external websites etc.
- Malicious code attacks such as spreading of Virus or Worms or Trojans or Spy ware, Botnets, etc.
- Attacks on Servers such as Database, Mail and DNS and Network devices such as Routers.
- Identity Theft, Spoofing and Phishing attacks
- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks
- Attacks on Critical infrastructure, SCADA Systems and Wireless networks
- Attacks on e-Governance applications.

Table 5.1 General symptoms of incidents noticeable by all types of users & System Administrators and related response actions.

Symptoms/Alerts	Source of detection	Response Actions	Action by whom
Common Symptoms			
• Non-availability of computer system (failure to start)	• User	• Boot with alternate OS / recover media. • Check the booting process for specific errors. • Report to the System Administrator	• User • System Administrator
• Frequent system crashes • Unexplained poor system performance • Presence of new files • Presence of unknown processes • Changes in the file size or dates	• User	• Scan the system with updated Antivirus & Antispyware • Report to the System Administrator	• User • System Administrator
• New suspicious user accounts	• User	• Report to the System Administrator	• System Administrator
• Failed log in attempts by unauthorized users	• Technical tools • Supervisory review of logs	• Determine the timing, sources of activities • Trace the attack sources from logs of system / directory server	• System Administrator
• Unusual time of usage • Unauthorized user accounts	• Supervisory review of logs	• Correlate with physical access by users • Correlate with logs of perimeter devices to find external intrusion.	• System Administrator • Network Administrator
• Virus / Worm infections	• User • System Administrator	• Disconnect system from network • Boot with a different OS and scan with Antivirus &	• User • System Administrator

Symptoms/Alerts	Source of detection	Response Actions	Action by whom
		Antispyware • Antivirus and Antispyware to be updated regularly	
• Suspicious probes	• Technical tools (IDS/IPS/ Firewall)	• Close the ports and services that are not required • Send the logs to incident response team for examination	• Network Administrator
• Abnormal surge in traffic (inbound/ outbound)	• Technical tools (IDS/IPS/ Firewall) • Network behaviour analysis • Router	• Trace the specific service / protocol • Detect the source of generation of abnormal traffic • Correlate with alerts from CERT-In	• Network Administrator
External Alerts			
• Alert for new vulnerability	• CERT-In	• Apply appropriate patches / updates • Implement suggested workarounds for zero-day vulnerabilities	• System Administrator
• Alert on propagation of malicious code	• CERT-In	• Update the Antivirus Signatures • Follow the counter measures suggested in the specific advisory and in this table	• System Administrator

***Source**: Doc No.CERT-In/NISAP/01- Information Security Policy for protection of Critical Information Infrastructure, Revision 1 by CERT-In, May 2006*

Table 5.2 Indications of different types of Cyber Crisis generally noticeable by trained users, System Administrators & tool based detection mechanisms and Response actions

Symptoms/ Indications /Alerts	Source	Response Actions	Action by whom
Website defacement and semantic attacks			
Detection of defacement/ intrusion of website	• Users • Website Administrators • External Agencies	• Disconnect the Web Server hosting the defaced/ compromised website • Examine the compromised system/ website for specific unauthorized changes • Restore the website content, host the website from a different trusted system by making appropriate DNS changes to the new system • Collect relevant logs of Server and application. Submit them to the IR team of the organization. • Report the incident to Law Enforcement and CERT-In with logs	• Website Administrator • Network Administrator
Malicious Code Attacks (Virus, Worm, Trojans, Botnets, Spyware)			
• Unexplained poor system performance • Presence of suspicious process/files on system • Surge in traffic on ports/ services used by malware • Connections to suspicious remote systems • Unusual ports open	• User • System administrator • Alerts from antivirus, NIDS • External agencies	• Disconnect infected systems from Network • Scan with updated Antivirus and Anti-spyware • Apply appropriate countermeasures in Consultation with local Incident Response Team/CERT-In	

Symptoms/ Indications /Alerts	Source	Response Actions	Action by whom
SPAM attacks			
• Abnormal surge in SMTP traffic • Bandwidth congestion • Slow response of Mail Servers	• Users • Network Administrators • Network Behaviour analysis	• Check the mail servers for open relays and disable • Close ports not required in the Mail server • Identify possible sources of spam from email headers and invoke blacklist such as SBL, XBL and PBL • If attack persists report to local Incident Response Team/CERT-In	• Network Administrator • Mail Server Administrator
Attacks on Mail Servers			
• Non availability of mail accounts • Compromised mail accounts	• Users • Mail server administrator	Mail server compromise: • Disconnect Mail Server • Activate standby Mail Server • Check logs of Mail Server and identify attack source • Send the logs to Incident Response Team/CERT-In User account compromise: • Reset the password • Enforce strong passwords (minimum 8 digit and alphanumeric) • Enforce email best practices	• Mail Server Administrator
Identity Theft Attacks through spoofing			
• Detection of suspicious network connections • Detection of packets with suspicious source address	• Alerts from IPS/IDS • Email headers	• Examine the email header and find the actual origin of email • Notify and alert users • To counter spoofing, implement Egress and Ingress filtering at perimeter (Router)	• Network Administrator

Symptoms/ Indications /Alerts	Source	Response Actions	Action by whom
• Emails from masqueraded account name		• Enforce email authentication • Report to local Incident Response Team/CERT-In	
Phishing attacks			
• Reporting of phishing email/website	• Users • Antiphishing/ fraud detection services • CERT-In/external agencies	• Report phishing incident to local IR Team/ CERT-In • Report phishing URL to phishing filters • Send phishing emails and details of phishing website to CERT-In	• Users • Designated persons
Denial of Service (DoS) attacks			
• Non availability of services such as website, email etc • System crashes • Bandwidth congestion • Surge in traffic	• Users • Website Administrator	• Identify the type of attack such as flooding of particular types of packets/requests (TCP SYN, ICMP etc) by examining logs of Router/IPS/IDS/Fire wall • Identify the attack sources • Block the attack sources at Router/Packet filtering device • Check Router Configuration and implementing Egress and Ingress filtering to block spoofed packets • Disable the non essential ports/ services • Report to local Incident Response Team/ CERT-In with relevant logs	

Symptoms/ Indications /Alerts	Source	Response Actions	Action by whom
Distributor Denial of Service (DDoS) attacks			
• Non availability of services such as website, email etc • System crashes • Bandwidth congestion • Surge in traffic	• Network Administrator • Alerts of IPS/IDS/ Firewalls • Network Behaviour Analysis • CERT-In	• Identify the type of attack such as flooding of particular types of packets /requests by examining logs of Router / IPS/IDS/Firewall • Apply appropriate rate limiting strategies at the local perimeter and if necessary consult ISP • Implement Egress and Ingress filtering to block spoofed packets • Use appropriate DoS prevention tools • If problem persists shift web/mail services hosting to alternate Internet Protocol addresses (IPs) • Report to local Incident Response Team/CERT-In with relevant logs	• Network Administrator
Dos Attacks on DNS Server			
• Slow response or non-availability Web/ Mail services	• User • Network Administrator	• Change the Primary DNS server • Implement source address validation through ingress filtering (Implement IETF BCP 38/RFC 2827) • Use Unicast Reverse Path Forwarding to mitigate problems that are caused by malformed or forged IP source addresses • Run separate DELEGATED and RESOLVING name	• Network Administrator

Symptoms/ Indications /Alerts	Source	Response Actions	Action by whom
		servers • Restrict zone transfers to Secondary name Servers only • Block invalid DNS messages to an authoritative name server at the network edge. This includes blocking large IP packets directed to an authoritative name server. • Report to local Incident Response Team/CERT-In	
DNS Cache poisoning attacks			
• Redirection of legitimate web/mail traffic to suspicious websites/mail servers	• User • Network Administrator	• Purge cache • Restart DNS server • Replace DNS records with content from trusted backup • Examine DNS forwarding traffic to identify rogue DNS server and block • Restrict rights of configuration changes to Administrator only • At client side, delete any additional entries in HOSTS file • Report to local Incident Response Team/ CERT-In	• Network Administrator
Application Level Attacks			
• Unauthorized changes to Data • Suspicious user activity • Elevation of privilege of user accounts • Presence of malicious links/	• Web/Database Administrator • Application logs	• Disable suspected user accounts • Reduce the interactive features and run with min. essential features • Restore data from trusted backup • Identify attacks	• Web Administrator • Database Administrator

Symptoms/ Indications /Alerts	Source	Response Actions	Action by whom
content		sources from applications logs validation • Enforce Input Validation • Apply latest patches/ updates • Report to local Incident Response Team/CERT-In	
Router level attacks			
• Unexplained packet loss • Non availability of Gateway/ Internet services	• Users • Network administrator • Review of Router configurations	• Replace the router with a securely configured standby router with Egress and Ingress filtering • Check the logs and configuration files of compromised router to identify attacks • Replace the configuration files with trusted backup • Apply appropriate patches/updates • Block the attack source • Report to local Incident Response Team/ CERT-In	• Network Administrator
High Energy RF based Denial of Service Attacks			
• Non availability of wireless connection • Degraded Signal to Noise Ratio • Increase Noise levels in the airwaves	• Users • Network Administrator • Alters of IDS/IPS	• Identify the other devices due to which RF interference occurs and physically remove them. • Detect rogue access points and remove them • If attack persists switch critical functions to wired networks • Report to local Incident Response Team/CERT-In	• Network Administrator

Symptoms/ Indications /Alerts	Source	Response Actions	Action by whom
Targeted Scanning, Probing and Reconnaissance of Networks and IT Infrastructure			
• Huge amount of IPS/IDS/ alerts • High volume of dropped packets by Firewalls • Surge in specific traffic	• User • Network Administrator • Logs of relevant devices	• Identify the type of scans/ probes by examining logs of Router /IDS/IPS/Firewall • Identify the sources of scanning • Report the incidents with relevant logs to CERT-In other incident response teams	• Network Administrator

***Source**: Doc No.CERT-In/NISAP/01- Information Security Policy for protection of Critical Information Infrastructure, Revision 1 by CERT-In, May 2006*

5.2. Appendix II

Incidents Response Activities in the First 24 Hours

The first 24 hours of an attack are the most critical in limiting the impact of an incident. The organisations shall be prepared to respond to an attack, detect, analyze and contain the attack through a combination of technologies and processes. The following guidelines will help to analyze the problem, tackle it and if necessary escalate to higher levels within the organization or outside to benefit from appropriate response to tackle the problem.

When an organisation is under cyber attack, minutes really do matter, for instance, the "SQL Slammer" worm infected 75,000 hosts within its first 10 minutes, doubling every 8.5 seconds during the first minutes of the outbreak. Cyber Crime is now driving targeted and stealthier malware attacks, decreasing the available time to effectively respond. So, all departments need to be prepared to respond quickly.

Defining an Incident

An incident is a violation or imminent threat of violation of computer security policies. Incidents are broadly categorized as Denial of Service, injection and spread of malicious code, unauthorized access and inappropriate usage of Information (IT) infrastructure.

Incidents Response

Incident Response (IR) is a structured process to respond to security incidents occurring in an organization. A dedicated team is required to perform incident response activities. This team is generally referred to as Computer Security Incident Response Team (CSIRT) and will need to perform its operations according to pre-defined policies and standard operating procedures. It is expected of each department to form its own internal team which will then need to be trained. TNeGA will assist all such Teams in advanced training.

Phases of Incidents Response

The initial phase involves establishing and training an Incident Response Team (CSIRT), and acquiring the necessary tools and resources for incident analysis and response. During preparation, the organization will also attempt to limit the numbers of incidents that will occur by selecting and implementing a set of controls based on the results of risk assessments. However, no control is fool proof. Prompt detection of security breaches is

thus necessary to alert the organization whenever incidents occur.

After the incident has been tackled, it is essential to issue a report on the details of the incident inclusive of the cause and cost and the steps that are necessary to prevent such incidents in the future.

To sum up, the major phases in an incident process are pre-incident preparation, detection and analysis, containment, mitigation, recovery and issue of a final report.

Notification: All staff in the department need to know who to notify in the event of an incident. A matrix has been drawn up to assist the departments. Each department must notify the staff for this purpose.

Table 5.3
Example of an Attack Response Matrix

S. No	Attack Type	Severity Level	Target(s)	Asset Value	Response	Action by whom
1	Scanning, Probing and Reconnaissance of network and IT Infrastructure	Medium to High	Any System	Medium to High	1. If no obvious damage is occurring, more information can be collected by monitoring it to determine what the attacker is trying to accomplish 2. Identify the type of scans/ Probes 3. Identify the sources of scans 4. Block the sources of scanning	Security Analyst
2	Denial of Service (DOS)	High	External web server Router	High	1. Identify targets i.e. IPs which are under DoS attack 2. Identify IPs which are doing DoS attack i.e. attack vector; restrict attack	Web server Administrator Network Administrator

S. No	Attack Type	Severity Level	Target(s)	Asset Value	Response	Action by whom
					vector (through network access control list modification, firewall rules or constrainment of the end point itself) 3. Implement alternative services and resources as required to allow for continued providing of services	
3	Denial of Services	Low	Intrusion detection system (IDS)	Low	1. Disable Intrusion Detection System(IDS) 2. Deploy an Intrusion Prevention System (IPS)	Security analyst
4	Malicious Code (Virus/Worm / Trojan) Outbreak	High	Data base server Personal Computers	High	1. Modify environment defenses to prevent further spread of worm (that is, modify IPS blocking rules, modify firewalls and routers to disable vectors used by malware and so forth) 2. Disconnect system from Local Area Network (LAN) and wide Area Network (WAN) 3. Download and distribute latest antivirus updates 4. Identify database servers that are not updated, and quarantine if infected	Security analyst

S. No	Attack Type	Severity Level	Target(s)	Asset Value	Response	Action by whom
					5. Download and distribute software patches if applicable 6. Notify staff of issues; provide information and status for interruption of services	
5	Malicious Code (Virus/ Worm/ Trojan) Outbreak	Medium	User desktops	Mediu m	1. Modify environment defenses if applicable (that is, modify e-mail attachment blocking until virus is contained, rate limit messages and so forth) 2. Disconnect system from Local Area Network (LAN) 3. Download and distribute latest antivirus updates 4. Identify devices that are not updated (managed or unmanaged nodes), and quarantine if infected 5. Download and distributed software patches if applicable 6. Notify staff of virus and mitigation procedures (important for remote users not connected through a Virtual Private Network [VPN])	Network administrator, Individuals , owning and operating personal computer

S. No	Attack Type	Severity Level	Target(s)	Asset Value	Response	Action by whom
6	Malicious Code (Virus/ Worm/Trojan) Outbreak Excessive Network Bandwidth consumption	High	User desktops Network bandwidth	High	1. Modify environment defenses to prevent further spread of Worm (that is, modify IPS blocking rules, modify firewalls and routers to disable vectors used by malware, and so forth) 2. Download and distribute latest antivirus updates 3. Identify devices that are not updated (managed or unmanaged nodes), and quarantine if infected 4.Download and distribute software patches if applicable 5. Notify staff of virus and mitigation procedures (important for remote users not connected through a VPN)	Network administrator
7	Privilege Escalation Root kit	Critical	File Server or any other Server	High	1. Quarantine the server 2.Switch to alternative server 3. Perform forensic analysis 4. Re-image server (once infected with a root kit, the entire system is suspect)	Server Administrator Security forensic analyst
8	Website Defacement/ Intrusion	Critical	Website/ Web server	High	1. Disconnect Web Server 2. Host and run website from a	Web server Administrator

S. No	Attack Type	Severity Level	Target(s)	Asset Value	Response	Action by whom
					different trusted system 3. Examine compromised server and trace and remove the defaced pages/ malicious content 4.Extract logs from relevant applications, server and system 5. Examine the logs as well as submit the same to appropriate Incident Response Team	

***Source**: Doc No.CERT-In/NISAP/01- Information Security Policy for protection of Critical Information Infrastructure, Revision 1 by CERT-In, May 2006*

5.3 Appendix III
Contact Information Forms

Control Room Details within *GD*
(To be obtained from ISO)

Primary Contact		
Name	Designation	Contact Details
		Tel. Nos. Off: Res: FAX: Mobile: Email:
Alternate Contact		
Name	Designation	Contact Details
		Tel. Nos. Off: Res: FAX: Mobile: Email:

Control Room Details -Commissioner of Police
(To be obtained from ISO)

Primary Contact		
Name	Designation	Contact Details
		Tel. Nos. Off: Res: FAX: Mobile: Email:
Alternate Contact		
Name	Designation	Contact Details
		Tel. Nos. Off: Res: FAX: Mobile: Email:

Service Provider
(To be obtained from Service Provider)

Primary Contact		
Name	Designation	Contact Details
		Tel. Nos. Off: Res: FAX: Mobile: Email:
Alternate Contact		
Name	Designation	Contact Details
		Tel. Nos. Off: Res: FAX: Mobile: Email:

***Source**: Doc No.CERT-In/NISAP/01- Information Security Policy for protection of Critical Information Infrastructure, Revision 1 by CERT-In, May 2006*

5.4. Appendix IV
Check Lists

1. Check List for CISO (once every six months)

Plan and Organize training for all employees and IT users w.r.t IT Security	❑
Review and document training imparted to employees w.r.t IT Security	❑
Document incidents reported during the past six months and plan for improvement	❑
Review the results of the latest third party external security assessments	❑

2. Check List for *Asst. ISO* (once a month)

Review all the training programs under implementation	❑
Get an update on all logs from system administrators and information owners	❑
Review the roles and privileges assigned to new users created in the past month	❑

3. Check List for System Administrator

Every morning review all system, security, event and audit logs for abnormalities	❑
Document a daily list of all users accounts created & modified with their privileges listed	❑
Document daily all changes made on all devices (routers, firewall, servers, printers, etc.)	❑
Document and take backups of all configurations on devices as per required frequency	❑
Verify by restoring backup's as per criticality of device	❑

***Source**: Doc No.CERT-In/NISAP/01- Information Security Policy for protection of Critical Information Infrastructure, Revision 1 by CERT-In, May 2006*

5.5. Appendix V
Incident Reporting Form

Form to report Incidents to CERT-In			
For official use only Incident Tracking Number : **CERT-In-xxxxxx**			
1. Contact Information for this Incident:			
Name:	Organisation:		Title:
Phone / Fax No:	Mobile:		Email:
Address:			
2. Sector: (Please tick the appropriate choices)			
❑ Government ❑ Financial ❑ Power	❑ Transportation ❑ Manufacturing ❑ Health	❑ Telecommunications ❑ Academia ❑ Petroleum	❑ InfoTech ❑ Other
3. Physical Location of Affected Computer/ Network and name of ISP:			
4. Date and Time of Incident Occurred:			
Date:	Time:		
5. Is the affected System/Network critical to the organization's mission? (Yes / No). Details.			
6. Information of Affected System:			
IP Address:	Computer/ Host Name:	OS (including ver./release no.)	Last Patched/ Updated	Hardware Vendor/ Model
7. Type of Incident:			
❑ Phishing ❑ Network scanning! Probing ❑ Break-in/ Root Compromise ❑ Virus/Malicious Code ❑ Website Defacement ❑ System Misuse	❑ Spam ❑ Bot/Botnet ❑ Email Spoofing ❑ Denial of Service(DoS) ❑ Distributed Denial of Service(DDoS) ❑ User Account Compromise	❑ Website Intrusion ❑ Social Engineering ❑ Technical Vulnerability ❑ IP Spoofing ❑ Other	

8. Description of Incident:	
9. Unusual behavior/symptoms (Tick the symptoms)	
❑ System crashes	❑ Door knob rattling
❑ New user accounts/ Accounting Discrepancies	❑ Unusual time of usage
❑ Failed or successful social engineering Attempts	❑ Unusual usage patterns
❑ Unexplained, poor system Performance	❑ Unusual log file entries
❑ Unaccounted for changes in the DNS tables, router rules, or firewall rules	❑ Presence of new setuid or setgid files
❑ Unexplained elevation or use of Privileges	❑ Changes in file lengths or dates
❑ Operation of a program or sniffer device To capture network traffic;	❑ Attempts to write to system
❑ An indicated last time of usage of a user account that does not correspond to the actual last time of usage for that User	❑ Data modification or deletion
❑ A system alarm or similar indication from an intrusion detection tool	❑ Denial of service
❑ Altered home pages, which are usually the intentional target for visibility, or other pages on the Web server	❑ Changes in system directories and files
❑ Anomalies	❑ Presence of cracking utilities
❑ Suspicious probes	❑ Activity during non-working hours or holidays
❑ Suspicious browsing	❑ Other (Please specify)
❑ New files	
10. Has this problem been experienced earlier? If yes, details.	
11. Agencies notified	

❑ Law Enforcement	❑ Private Agency.	❑ Affected Product Vendor	❑ other

12. When and How was the incident detected:	
13.	Additional Information (Include any other details_ noticed, relevant to the Security Incident.)

❑ Whether log being submitted	Mode of submission:

OPTIONAL INFORMATION				
14. IP Address of Apparent or Suspected Source:				
Source IP address:		Other information available:		
15. Security Infrastructure in place:				
	Name	OS	Version/ Release	Last Patched/ Updated
Name OS Version/Release Last Patched / Updated				
Anti-Virus				
Intrusion Detection/ Prevention Systems				
Security Auditing Tools				
Secure Remote Access/ Authorization Tools				
Access Control List				
Packet Filtering/Firewall				
Others				
16. How Many Host(s) are Affected				
❑ 1 to 10	❑ 10 to 100		❑ More than 100	
17. Actions taken to mitigate the intrusion/attack:				
❑ No action taken ❑ System Binaries	❑ Log Files examined ❑ System(s) disconnected from network.		❑ Restored with a good backup ❑ Other	
Please fill all mandatory fields and try to provide optional details for early resolution of the Security Incident				
Mail/Fax this Form to: CERT In, Electronics Niketan, CGO Complex, New Delhi 110003 Fax:+91-11-24368546 or email at: incident@cert-in.org.in and to ceotnega@tn.gov.in , secyit.tn@nic.in				

Source: Doc No.CERT-In/NISAP/01- Information Security Policy for protection of Critical Information Infrastructure, Revision 1 by CERT-In, May 2006

5.6.Appendix VI

Definition and Acronyms

Authentication:	The process to establish and prove the validity of a claimed identity.
Authorization:	The granting of rights, which includes the granting of access based on an authenticated identity.
Biometric Data:	Unique physical or behavioral characteristics, such as fingerprints or voice patterns, used as a means of verifying personal identity.
CIO:	Chief Information Officer
Controls:	Countermeasures or safeguards that are the devices or mechanisms that are needed to meet the requirements of policy.
Copyright:	A property right in an original work of authorship fixed in any tangible medium of expression, giving the holder the exclusive right to reproduce, adapt, distribute, perform and display the work
Cracking:	Breaking into or attempting to break into another system in excess of one's access rights or authorization with or without malicious intent.
Cryptographic:	Relating to a method of storing and transmitting data in a form that only those it is intended for can read and process.
Cryptographic Key:	A binary number used by an encryption algorithm to perform calculations.
Data:	See Information.
Denial of Service:	An attack results in degradation of performance or loss of access to the IT services or resources of the department.
Disaster:	A condition in which information is unavailable, as a result of a natural or man-made occurrence, that is of sufficient duration to cause significant disruption to normal functioning of IT systems.
DNS:	Domain Name System
Encryption:	The cryptographic transformation of data to render it unintelligible through an algorithmic process using a cryptographic key.
Field Level Encryption:	Protects data by encrypting data in certain fields of a database.
File Level Encryption:	Protects data by encrypting data on a file by file basis.

Firewall:	A security mechanism that creates a barrier between an internal network and an external network.
Folder Level Encryption:	Protects data by encrypting data on a folder by folder basis.
Full Disk Encryption:	Protects data by encrypting the entire drive no matter how many partitions it holds. This can be either hardware or software based.
Host:	A system or computer that contains official, functional and/or operational software and/or data.
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
Incident:	Any adverse event that threatens the confidentiality, integrity or availability of information resources.
Incident Response:	The manual and automated procedures used to respond to reported network intrusions (real or suspected); network failures and errors; and other undesirable events.
Information:	Any representation of facts, concepts or instructions created, stored (in temporary or permanent form), filed, produced or reproduced, regardless of the form or media. This may include, but is not limited to reports, files, folders, memoranda, statements, examinations, transcripts, images, communications, electronic or hard copy.
Information Security:	The concepts, techniques and measures used to protect information from accidental or intentional unauthorized access, modification, destruction, disclosure or temporary or permanent loss.
Information Security Architecture:	A framework designed to ensure information security. Principles are defined and integrated into functional and IT processes in a consistent manner.
Integrity:	The property that data has not been altered or destroyed from its intended form or content in an unintentional or an unauthorized manner.
Intranet:	An internal (i.e., non-public) network that uses the same technology and protocols as the Internet.
Internet:	A system of linked computer networks, international in scope, that facilitate data transmission and exchange, which all use the Standard Internet Protocol, TCP/IP, to communicate and share data with each other.
Intrusion Detection:	The monitoring of network activities, primarily through automated measures, to detect, log and report upon actual or suspected authorized access and events for investigation and resolution.

IPS	Intrusion Prevention System
LAN	Local Area Network
Least Privilege:	User, program or process is granted only the access they specifically need to perform their official task and no more.
Malicious Code:	Malicious code refers to code that is written intentionally to carry out annoying, harmful actions or use up the resources of a target computer. They sometime masquerade as useful software or are embedded into useful programs, so that users are induced into activating them. Types of malicious code include Trojan Horses and Computer Viruses.
Media Access Control (MAC) Address:	A hardware address that uniquely identifies each node of a network
Multi-User System:	Refers to computer systems that support two or more simultaneous users.
Penetration Testing:	The portion of security testing in which evaluators attempt to exploit physical, network, system or application weaknesses to prove whether these weaknesses can be exploited by gaining unauthorized access to protected resources.
Personal Digital Assistant (PDA):	A small portable device, such as a Palm Pilot or Blackberry, which combines computing, telephone/fax and networking features. Also called palmtop, handheld and pocket computer.
Government Sensitive Information	Any information where unauthorized access, disclosure, modification, destruction or disruption of access to or use of such information could severely impact the department or its critical functions. Each department will need to classify the type of information that will be deemed to be sensitive. • Reports, logs, surveys or audits that contain sensitive information. • Security related information (e.g., vulnerability reports, risk assessments, security logs). • Other information that is protected from disclosure by law or relates to subjects and areas of concern as determined by departments IT management.
GSI:	Government Sensitive Information.
Privileged Account:	The user-ID or account of an individual whose job responsibilities require special system authorization, such as a network administrator, system administrator and so on.
Remote Access:	Any access coming into the GD's network from off the GD's private trusted network. This includes, but is not limited to, dialing in from another location over public

	lines by an employee or other authorized individual.
Role-Based Access Control:	An approach to restricting system access where permissions to perform certain operations are assigned to specific job functions.
Spamming:	Blindly posting something to a large number of groups.
SMTP	Simple Mail Transfer Protocol
TCP	Transmission Control Protocol
TCP SYN	Transmission Control Protocol Synchronize Flag
Trojan Horse:	Malicious code hidden in a legitimate program that when executed performs some unauthorized actions or function.
Unauthorized Access:	Insider or outsider who gains access to network or computer resources without permission or without valid authorization.
USB Flash Drive:	A solid state memory storage device integrated with a USB interface.
Vulnerability:	A weakness of a system or facility holding information which can be exploited to gain access or violate system integrity. Vulnerability can be assessed in terms of the means by which the attack would be successful.
Vulnerability Scanning:	The portion of security testing in which evaluators attempt to identify physical, network, system or application weaknesses to discover whether these weaknesses may be exploited by persons or machines seeking to gain either unauthorized or elevated privileged access to otherwise protected resources.
Worm:	A program similar to a virus that can consume large quantities of network bandwidth and spread from one network to another.

***Source**: Doc No.CERT-In/ NISAP/ 01- Information Security Policy for protection of Critical Information Infrastructure, Revision 1 by CERT-In, May 2006*

P.W.C.DAVIDAR
PRINCIPAL SECRETARY TO GOVERNMENT