For Official Use Only

GOVERNMENT of TAMIL NADU

INFORMATION SECURITY POLICY 2009

Publication Date: June 10, 2009
Revision Date: January 4, 2010
Version: 7.11

COMMITTEE MEMBERS

1	Thiru. P.W.C. Davidar, I.A.S.	Chairman/IT Secretary	ELCOT/Govt. of Tamil Nadu
2	Thiru. Santhosh Babu, I.A.S.	Managing Director	ELCOT
3	Thiru. M. Anbu Chezhan	GM Networks	ELCOT
4	Dr. Sudhakar	Asst. Commissioner	Cyber Cell, Chennai City Police
5	Thiru. M. Ram Swaroop	President	CYBER SECURITY WORKS Pvt. Ltd.
6	Thiru. Sambamoorthi	Member	Directorate eGovernance
7	Thiru. Iniya Nehru	Sr. Technical Officer	NIC
8	Thiru. Purusothaman	Member	NASSCOM
9	Thiru. Raghavan	Member	SICC
10	Selvi. Neeru	Member	SETS
11	Thiru. J. Kesavardhanan	C.E.O.	K7 Computing Pvt. Ltd.

Table of Contents

EXECUTIVE SUMMARY

A core committee was formed under the guidance of the IT Secretary 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 best practices for all the Government Departments (GDs) under the Government of Tamil Nadu Information Technology Infrastructure. All GDs shall use this as a guideline and develop detailed procedures that are relevant to their respective department's assets.

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

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 needs to obtain permission from the HOD and sign a Non-Disclosure Agreement (NDA).

The purpose of this policy is to define a set of minimum information security requirements that shall be met by all GDs of the Govt. of Tamil Nadu. The primary objectives:

- Effectively manage the risk of security exposure within GDs
- Communicate the responsibilities for the protection of GD information
- Reduce the opportunity for errors to be entered into an electronic system supporting GD procedures and processes
- Preserve GD's options in the event of an information asset misuse, loss or unauthorized disclosure
- Promote, train and increase the awareness of information security in all GDs

Salient features of this policy are:

1 This security policy shall be implemented, maintained and supported by the respective Head of the Department (Owner) within their department under the guidance of the Director of e-Governance.
2 The respective Head of the Department (HOD) shall create two positions for implementing, enforcing and supporting the information security policy.
    a Chief Information Security Officer (CISO)
    b Assistant Information Security Officer (Asst. ISO)

3 This document shall be modified by the individual GD according to their specific operations, processes, procedures, requirements and citizen services in line with their e-Governance initiative under the guidance of Director of e-Governance. They may also use this as a parent document and create supporting documents in addition to this policy to address specific policies such as email policy, server policy, network devices policy, etc. This document shall be enforced in full if the department does not have anything to modify.

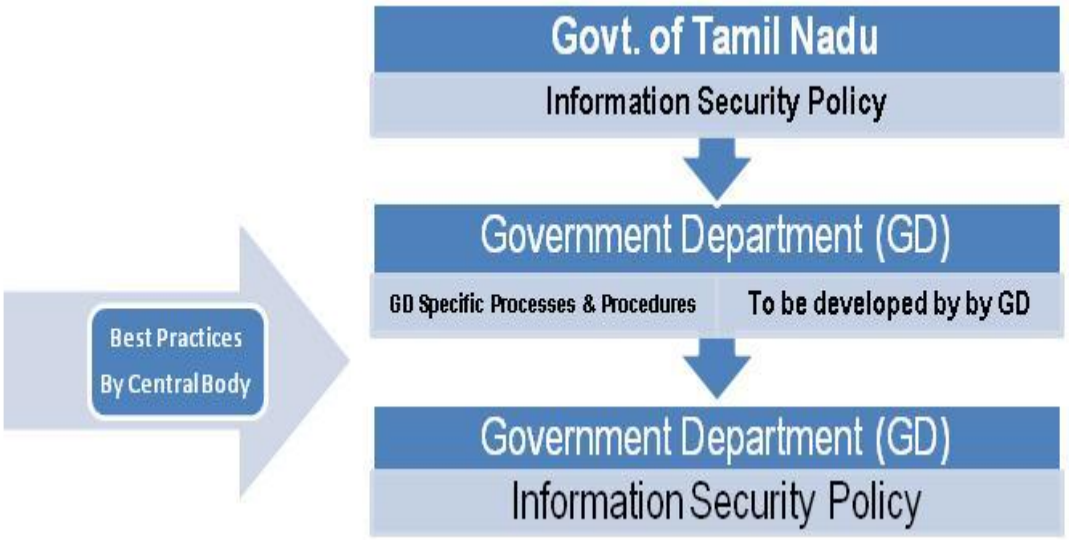
4 ELCOT/Director of e-Governance may form a committee to ensure the full compliance of this Information Security Policy. This committee shall comprise of government officials from NIC, CDAC, STQC, etc.

5 The respective GDs are the owners of the processes, procedures, systems, applications and technologies and the information maintained in these systems even though they are hosted and maintained by another government department. Respective Department Heads must ensure that the security policy is a part of all their IT operations within their respective departments/ELCOT.

6 CISO and his group 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 Govt. of Tamil Nadu.

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



1. BACKGROUND

With the increasing use of information technology, functions in GDs 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 infrequent, of minimal duration & manageable and cause the least damage possible.

Users of information resources must have skills, knowledge, and training to manage information resources, enabling the government departments to effectively serve the citizens through automated means

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. The 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.

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.

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'. It must be considered an integral part of the systems development life cycle process and explicitly addressed during each phase of the process. Security must be dealt with in a proactive and timely manner to be effective.

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*)

2. FUNCTIONAL RESPONSIBILITIES

2.1. Government Departments (GD)

Each GD under the guidance of their respective HOD will:

1. Establish a framework to initiate and control the implementation of information security within the GD;

2. Nominate and train a Chief Information Security Officer (CISO) for every GD. This officer should have had adequate experience in the field of Information Technology and an aptitude towards Information Security;
3. Assure 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 GD is recommended; i.e. ensure 100% system coverage for all IT assets in the GD; implement inter-department audits once every six months; if 100% coverage is not completed it defeats the purpose of a security assessment.
5. Develop and implement an IT Disaster Recovery Plan for critical GD IT Systems in accordance with IT Disaster Recovery plan guidelines, tested and reviewed for relevance at least annually;
6. Establish a process to determine information sensitivity, based on best practices, legal and regulatory requirements to determine the appropriate levels of protection for GD information and infrastructure.
7. Ensure that the head of each GD 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. Monitor significant changes in the exposure of information assets to major threats, legal or regulatory requirements;
    d. Identify security vulnerabilities within GD systems and recommending corrective action;
    e. Assume the lead role in resolving GD security and privacy incidents;
    f. Develop a process to measure compliance with this policy;
    g. Communicate requirements of this policy and the associated Information Security Standards to third parties and address them in third party agreements;
    h. Implement an IT Security Certification and Accreditation process used to approve new systems, applications and services for the life cycle of each GD's IT System;

2.2. Chief Information Security Officer (CISO)

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

1 Recommendation, coordination, 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 GD procedures and refer the investigation to other investigatory entities, including law enforcement;

3 Provide consultation with security administration and management or those serving in that capacity for the various GD computing platforms to ensure proper implementation of security requirements;

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

5 With the help of GD Asst. ISOs and System Administrators, 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 the annual audit purposes;

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

7 CISO shall report to the HOD

2.3. Assistant Information Security Officer (Asst. ISO)

Asst. ISO will be responsible for the implementation of this information security policy and the compliance of GD employees to this policy. Asst. ISO must educate GD employees with regard to information security issues. Asst. ISO must explain the issues, why the policies have been established, and what role(s) individuals have in safeguarding information including consequences of non-compliance. Asst. ISO with the help of inside IT experts will execute the check list once 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 GD information;

2 Report suspected security incidents to the appropriate manager and the CISO;

3 Use IT resources only for intended official purposes as defined by GD policies, laws and regulations;

4 Only access IT assets to which they are authorized by the CISO;

5 Asst. ISO will report to the CISO

2.4. Information/Asset Owners

Information owners report to the Asst. ISO on IT Security related issues and are responsible for:

1 Determining and documenting who should have access to protected resources within their jurisdiction, what those access privileges should be (read, update, etc.), and manage and document changes as needed. All actions will be reviewed by the Asst. ISO, CISO and approved by the information owner in writing

2 Communicating the legal requirements for access and disclosure of their data to the GD Asst. ISO and CISO;

3 Identifying all GD information assets and assigning responsibility for the installation, implementation, and maintenance of appropriate security measures such as:

   a Identifying assets, owners, inventory of, classifying, handling and labeling procedures assets;

   b Managing user access to their resources, etc. Access privileges must be in accordance with the user's job responsibilities;

   c Maintaining up to date Control Room details for respective assets, vendors, ISPs, etc.

4 Responsibility for implementing security measures may be delegated, though accountability remains with the identified owner of the asset;

5 Ensure that critical data and recovery plans are backed up and kept at a secured off-site storage facility and that recovery of backed-up media will work if and when needed;

6 Information owners, other officers in IT-related roles, IT users in the department will report to the Asst. ISO with respect to information security issues.

2.5. IT Management

IT management (i.e. HOD of the GD) is responsible for the data processing infrastructure and computing network with the support of CISO, GD Asst. ISOs and information owners. It is the responsibility of IT management to provide resources needed to enhance and maintain a level of information security control consistent with their GD's Information Security Policy. IT Management will:

1 Ensure requirements, processes, policies and controls are identified and implemented relative to security requirements defined by the GD's procedures

2 Ensure the participation of the CISO and Asst. ISOs in identifying and selecting appropriate, cost-effective security controls & procedures for protecting information assets;

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

2.6. Systems Administrator

System Administrators 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 to security violations;

2 Administration of all user-IDs and passwords and the associated processes for reviewing, logging, implementing access rights, emergency privileges, exception handling, 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 GD Asst. ISOs and CISO);

3 Report incidents to Law Enforcement Agency and maintain Incident Report forms per Appendix III and Appendix IV;

4 Cyber crime incidents in Chennai city must be first reported to Commissioner of Police, Chennai and incidents outside Chennai must be reported to Crime branch of Tamil Nadu Police and only then it shall be reported to Cert-In (refer Appendix III and IV);

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

3. INFORMATION SECURITY POLICY

Information security policy management is used to identify government sensitive information (GSI); officers shall develop, train and implement these policies, standards, guidelines and procedures to protect intentional or unintentional unauthorized access, exposure, modification, destruction, or loss of GSI.

3.1. 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 or state security or national or state interest. This category is reserved for nation's/state's closest secrets and to be used with great reserve. e.g. State security plans during elections, general State security plans, plans related to strategic sectors, passwords to protected systems, etc.

Secret:
This shall be applied to information unauthorized disclosure of which could be expected to cause serious damage to the national or state security or national or state interest or cause serious embarrassment in its functioning. 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 like 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 organization or could be prejudicial to the interest of the organization, or could affect the organization in its functioning. Most information will on proper analysis be classified no higher than confidential. E.g. development plans of specific departments, etc.

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, etc.

Unclassified/Public:
This is the classification of information that requires no protection against disclosure but may need protection against unauthorized modification and other security or integrity threats. e.g. Information published on websites, newspapers and other media, etc.

The above classification is generic in nature and the information assets listed as examples are suggestive in nature. The actual assets that may be classified into these categories will be specific to the respective departments or organizations. Hence each department has to classify its information assets into the above categories.

Asset Controls

All physical assets such as servers, desktops, networking devices, etc. must be properly managed from installation through disposal.

Assign Asset Responsibility

All the physical assets mentioned above will have an owner who will be responsible for ensuring appropriate protection from unauthorized intentional, unintentional use, access, disclosure, modification or loss.

Build an Inventory of Assets

At a minimum an asset inventory must contain:

a Asset list, i.e. identify all GD's assets;

b Criticality of assets;

c Asset documentation;

d Archived information;

e System software and development tools on these assets;

f Necessary support equipment;

g Locations;

h Access restrictions.

3.2. Contingency Planning[1]

Contingency planning is used to prevent interruptions to normal governmental operations for critical government processes and procedures, from natural or man-made failures or disasters, and at a determined period of time restore normal operations. A contingency plan must include four (4) basics steps.

1 Scope and Plan Initiation;
2 GD Impact Assessment (GDIA)
3 GD Continuity Plan Development
4 Plan Approval and Implementations

[1] Reference document: "Information Security Policy Guidelines by Cyber Security Works Inc., USA and CAaNES LLC., USA."

Outline of a disaster recovery plan:

1. Planning Phase
    a. Incorporate GDIA into DRP
        i Define critical information, infrastructure, processes etc.
        ii Define threats
        iii Define controls
        iv Define system environment, dependencies, and interconnecting systems
        v Define roles & responsibilities

    b. Establish priorities for processing and operations
        i Mutual aid agreements
        ii Subscription services
        iii Multiple centers
        iv Critical Information Backups Services
        v Alternative data center backups
    c. Determine Recovery Strategies
        i Preventative
        ii Maintenance
        iii Corrective
2. Data processing continuity planning
3. Data Collection
4. Data recovery plan maintenance
    a. Testing
    b. Maintenance
5. Approve Plan

3.3. Physical and Environmental Security Policy

Physical security practices prevent unauthorized physical access, damage, and interruption to GD's assets. Physical security practices for each facility must be adequate to protect the most sensitive information technology application housed in that facility. GDs must take the appropriate physical security measures to provide for:

a. Physical Security Perimeter
    i Access Controls, such as bio-metrics or card readers shall be implemented.
    ii The GD will perform a threat and risk assessment to determine the extent of the perimeter and types of controls necessary to mitigate the risk.
b. Equipment Security
    i Computer equipment must be physically protected from security threats and environmental hazards (such as fires, water, electrical fluctuations).
    ii Special controls may also be necessary to protect supporting facilities such as electrical supply and cabling infrastructure. This protection will include, but is not limited to, data centers, wiring closets, server rooms, and storage facilities where computers and computer peripherals are stored.
c. Disposal or Re-use of Storage Media and Equipment
    Formal processes must be established to minimize risk of disclosure of GSI through careless disposal or re-use of equipment.
    i Storage devices such as hard disk drives and other media (e.g. tape, diskette, CDs, DVDs, cell phones, digital copiers, or other devices that store information) or

paper containing GSI must be physically destroyed or securely overwritten to prevent the unauthorized disclosure of GSI.

ii Disposal of e-waste (old monitors, keyboards, etc.) shall comply with the e-waste policy of Govt. of Tamil Nadu.

3.4. Connectivity and Communication Policy

3.4.1. Network Management

All GDs must implement a range of network controls to maintain security in its trusted, internal network, and to ensure the protection of connected services and networks. Individuals in the GD will be assigned operational responsibility for networks. All GDs shall eventually migrate their data to a centralized data center hosted by ELCOT by using Tamil Nadu State Wide Area Network (TNSWAN).

3.4.2. Vulnerability Scanning

Vulnerability scanning must be completed by third party vendor and not by the vendor who implemented the security systems. Such third party security vendors must neither be a dealer/reseller or an agent for selling or distributing IT security related hardware or software products. Vulnerability assessment must be completed on all devices and applications that are on the GD's network, i.e. 100% coverage must be done on all IT assets. Sampling or having these assessments in phases should not be an option as it defeats the purpose of a security assessment. A minimum of ten well known scanners (well known in IT Security) should be used in order to ensure that false positives and false negatives are weeded out of these scanner reports. IT department/ELCOT may empanel or recommend qualified third party vendors for performing these security assessments.

a. All GD owned hosts (servers, desktops, printers, routers, IP telephones, switches, etc.) that are or will be accessible from inside or outside the GD network must be assessed for vulnerabilities and weaknesses. For both internal and external systems, scans will be performed at least annually to ensure that no major vulnerabilities have been introduced into the environment. The frequency of additional scans will be determined by the CISO and the information owner(s), depending on the criticality and sensitivity of the information on the system.

b. Network vulnerability scanning will be conducted after new network software or major configuration changes have been made on systems and applications. Annual scans on all systems have to be performed. The output of the scans will be reviewed in a timely manner by the CISO and any vulnerability detected will be evaluated for risk and mitigated. The tools used to scan for vulnerabilities will be updated periodically to ensure that recently discovered vulnerabilities are included in scans.

c. Where a GD has outsourced a server, application or network services to another GD, the responsibility for vulnerability scanning must be coordinated by both GDs.

d. Anyone authorized to perform vulnerability scanning must have a process defined, tested and followed at all times to minimize the possibility of disruption. Reports of exposures to vulnerabilities will be forwarded to the CISO and GD Asst. ISOs.

e. Any vulnerability scanning performed on GD systems and networks must be conducted by firms that have the appropriate credentials and should be authorized by the GD.

3.4.3. Penetration & Intrusion Testing[2]

All GD computing systems that provide information through a public network, either directly or through another service that provides information externally (such as the World Wide Web), will be subjected to penetration analysis and intrusion testing.

1 Analysis and testing will be used to determine if an individual can make an unauthorized change to an application; (A user may access the application and cause it to perform unauthorized tasks) OR an unauthorized individual may access, destroy or change any data OR an unauthorized individual may access the application and cause it to take actions unintended by the application designer(s).

2 The output of the penetration and intrusion testing will be reviewed in a timely manner by the CISO and any vulnerability detected will be evaluated for risk and mitigated appropriately.

3 The tools used to perform the penetration testing will be updated to ensure that recently discovered vulnerabilities are included in testing.

4 Where a GD has outsourced a server, application or network services to another GD, penetration testing must be coordinated by both GDs.

5 Only individuals authorized by the GD will perform penetration testing. The CISO must give approval prior to each penetration test. Any other attempts to perform such penetration testing will be deemed an unauthorized access attempt.

3.4.4. Intranet, Internet, E-Mail and Blogging un-Acceptable Usage[2]

When GD employees connect to the Internet using GD Internet address designation or send electronic mail using the GD designation, it should be only for GD purposes. The following is not an all-inclusive list and provides only examples of behavior that could result in security breaches. Specifically, the Internet and electronic mail shall not be used:

1 To represent yourself as someone else by modifying email header information (i.e., “spoofing”);

2 Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spamming);

3 For unauthorized attempts to break into any computing system whether GD’s or another organization’s (i.e., cracking or hacking);

4 For theft or unauthorized copying of electronic files

5 For posting GSI without appropriate authorization from GD

6 For any action which creates a denial of service, such as by forwarding "chain letters", "religious images" or other "pyramid" schemes of any type

7 For “Port Scanning” or “sniffing” (i.e., monitoring network traffic), except for those authorized to do so as part of their job responsibilities.

[2] Reference document: “Information Security Policy of State of NM, USA”

8 Sending unsolicited email originating from within GD's networks or to advertise, any service hosted by GD or connected via GD's network.

9 Posting non-official related messages to large numbers of usenet newsgroups (newsgroup spam).

10 Any form of harassment via email.

11 Violations of any government policy protected by Copyright Act, trade secret, patent or other intellectual property, or similar laws (IT Act and Right to Information Act) or regulations, including, but not limited to, the installation or distribution of "pirated" or other products that are not appropriately licensed for use by the GD.

12 Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs or other copyrighted sources, copyrighted movies and music, and the installation of any copyrighted software for which the GD or the end user does not have an active license is strictly prohibited.

13 Exporting software, technical information, encryption software or technology, in violation of export laws, is illegal. The appropriate officer should be consulted prior to export of any material that is in question.

14 Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.)

15 Revealing your account username and password to others or allowing the use of your account by others. This includes family and other household members when work is being done at home.

16 Using a GD's computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment is strictly prohibited.

17 Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

18 Circumventing user authentication or security of any host, network or account.

19 Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

20 Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

21 Blogging by officers and employees, whether using GD's systems or personal computer systems, is subject to the terms and restrictions set forth in this Policy. Limited and very occasional use of GD's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner (for official purpose only), does not otherwise violate GD's policy, is not detrimental to GD's best interests, and does not interfere with an employee's regular work duties. Blogging from GD's systems is subject to monitoring.

22 GD's Confidential Information policy also applies to blogging. As such, employees are prohibited from revealing any GSI while blogging.

23 Employees shall not engage in any blogging that may harm or tarnish the image, reputation of the GD and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging.

24 If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of the GD. Employees assume any and all risk associated with blogging.

3.4.5. External Connections[3]

1 As the Internet is inherently insecure, access to the Internet is prohibited from any device that is connected (wired or wireless) to any part of a GD network unless specifically authorized by CISO. This includes accounts with third party Internet service providers. Users will not use the GD's Internet accounts to establish connections to these third party services, unless authorized by the CISO.

2 All connections from the GD network to external networks (vendor) must be approved in writing by the CISO. Connections will be allowed only with external networks that have been reviewed and found to have acceptable security controls and procedures or appropriate security measures have been implemented by the GD. A risk analysis will be performed to ensure that the connection to the external network will not compromise the GD's private network. Additional controls, such as the establishment of firewalls and a DMZ (demilitarized zone) maybe implemented between the third party and the GD. These connections will be periodically reviewed by the GD to ensure the:

   a Use case for the connection is still valid and the connection is still required;

   b Security controls in place (filters, rules, access control lists, etc.) are current and functioning correctly.

3 This policy requires that connection to the GD network be done in a secure manner to preserve the integrity of the GD network, data transmitted over that network, and the availability of the network. The security requirements for each connection will be assessed individually, and be driven by the departmental needs. Only GD Asst. ISOs or qualified third party individuals will be permitted to use scanners, sniffers or similar technology on the network to monitor operational data and security events.

4 GD Asst. ISO and System Administrator will regularly review audit trails and system logs of external network connections for abuses and anomalies.

5 Third party network and/or workstation connection to a GD network must:

   a Have an internal GD sponsor for establishing a network connection.

   b A GD non-disclosure agreement must be signed by a duly appointed representative from the third party organization who is legally authorized to sign such an agreement.

   c In addition to the agreement, the third party's equipment must also conform to the State's security policies and standards, and be approved for connection by the CISO.

[3] Reference document: "Information Security Policy of State of NM, USA and State of NY, USA"

d Any connection between GD firewalls over external networks that involves GSI must use encryption to ensure the confidentiality and integrity of the data passing over the external network.

3.4.6. Security of Electronic Mail[4]

Electronic mail provides an expedient method of creating and distributing messages both within the organization and outside of the organization. Users, employees and officers of the GD e-mail system are a visible representative of the State and must use the systems in a legal, professional, and responsible manner. Unless prior IT management approval has been obtained, GD users must not connect to commercial e-mail systems from any GD system or workstation (i.e., AOL, Yahoo, Gmail, Rediffmail, etc.). Users of GD e-mail systems must comply with this policy and be knowledgeable of their responsibilities as defined under Communications and Network Management Policy & Intranet, Internet, Electronic Mail and Blogging Un-Acceptable Use Policy.

3.4.7. Portable Devices[4]

1 All portable computing resources and information media must be secured to prevent compromise of confidentiality or integrity. No computer device may store or transmit GSI without suitable protective measures that are approved by the CISO.

2 When using mobile computing facilities such as notebooks, palmtops, laptops and mobile phones, special care must be taken to ensure that information is not compromised. Approval is contingent on satisfaction of the requirements for physical protection, access controls, cryptographic techniques, back-ups, virus protection and the rules associated with connecting mobile facilities to networks and guidance on the use of these facilities in public places.

3 It is important that when such facilities are used in public places care must be taken to avoid the risk of unauthorized persons viewing information on-screen.

4 Procedures against malicious software shall be developed and implemented and be kept up to date. Equipment will be available to enable the quick and easy back up of information. These back-ups must be given adequate protection against theft or loss of information.

5 Equipment containing GSI must be attended at all times or physically secured.

6 Training must be provided to officers using mobile computing resources to raise their awareness on the additional risks resulting from this way of working and the controls that will be implemented.

7 Employees in the possession of portable, laptop, notebook, palmtop, and other transportable computers must not check these computers in airline luggage systems. These computers must remain in the possession of the traveler as hand luggage.

[4] Reference document: "Information Security Policy of State of NM, USA"

3.4.8. Wireless Networks[4]

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 will be installed without a risk assessment being performed and the written approval of the CISO.

2 Suitable controls, such as Media Access Control (MAC) address restriction, authentication, and encryption must be implemented to ensure that a wireless network or access point cannot be exploited to disrupt GD information services or to gain unauthorized access to GD 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 (refer to Access Control Policy, Monitoring System Access and Use)

3.4.9. Modem Usage

Connecting dial-up modems to computer systems which are also connected to GD'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.

3.4.10. Other Policies for Securing IT Infrastructure[5]

a Technology and security patches upgrade policy, which includes, but is not limited to operating system upgrades on servers, routers, and firewalls. The policy must address application and testing of upgrades in addition to departmental criteria for deciding which upgrades to apply.

b Firewall configuration policy, 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 to ensure that it has not changed during software modifications or rebooting of the equipment.

c Server configuration policy which must clearly address all servers that have any interaction with Internet, extranet, or intranet traffic. The policy must require creation and documentation of a baseline configuration for each server, updates of the documentation for all authorized changes, and periodic checking of the configuration to ensure that it has not changed during software modifications or rebooting of the equipment.

d Server hardening policy which must cover all servers throughout the department; not only those that fall within the jurisdiction of the department's IT area. The policy must include the process for making changes based on newly published vulnerability information as it

[5] Reference document: "Information Security Policy Guidelines by Cyber Security Works Inc., USA and CAaNES LLC., USA."

becomes available. Further, the policy must address and be consistent with the department's policy for making security upgrades and security patches.

e Software management and software licensing policy 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*.

g Access to GD computer, computer systems, and networks where the information owner has identified the GD's need for limited user access or information integrity and accountability must be provided through the use of individually assigned unique computer identifiers; known as user-IDs or other technologies including biometrics, token cards, etc.

h Requiring that if a data file is downloaded to a mobile device or desktop computer from another computer system; the specifications for information integrity and security which have been established for the original data file must be applied in the new environment.

i Establishing policy requiring encryption or equally effective measures for all governmental sensitive information (GSI) that is stored on portable electronic storage media (including, but not limited to, CDs and thumb drives) and on portable computing devices (including, but not limited to, laptop and netbook computers).

3.4.11. Public Websites Content Approval Process[6]

The content of each GD's public site shall be reviewed according to a process that will be defined and approved by the GD. A process shall be established for reviewing and approving updates to publicly available content. These reviews shall include consideration of copyright issues (both the potential publication of copyright material and the appropriate protection of GD copyright materials), the type of information being made available (confidentiality, privacy and sensitivity of the information), the accuracy of the information and potential legal implications of providing the information.

GSI shall not be made available through a server that is available to a public network without appropriate safeguards and written approvals from CISO. CISO will implement safeguards to ensure user authentication, data confidentiality and integrity, access control, data protection and logging mechanisms.

The design of a hosting service shall be reviewed and approved in writing by the CISO to ensure that the security of the web server, protection of GD networks, performance of the site, integrity, and availability considerations are adequately addressed.

[6] Reference document: "Information Security Policy Guidelines by Cyber Security Works Inc., USA and CAaNES LLC., USA."

3.4.12. Electronic Signatures

Each GD shall provide the respective officers with signature authority resources for obtaining digital signatures. This digital signature shall have the same validity as a signature affixed by hand.

3.4.13. Public Key Infrastructure (PKI)

In order for the GD to operate with PKI-based security architecture, the following requirements must be satisfied.

1. An appropriate trust model must be defined to include all of the stakeholders. The resulting trust domain or multiple trust domains must be supported by the appropriate certificate policies and certification practice statements. These apply to the stakeholders and users of GD systems and data.
2. Where PKI is used for digital signatures or encryption, it must operate under and comply with the Policy for Digital Signatures and Encryption and any associated rules and regulations issued by Controller of Certifying Authorities.

4. OPERATIONS POLICY

All GD information processing facilities must have documented operating instructions, management processes, and formal incident handling procedures related to information security matters that define roles and responsibilities of affected individuals who operate or use GD information processing facilities.

Computing hardware, software, or system configurations provided by GD must not be altered or added to or in any way unless exempted by documented written policy, procedures, or specific written approval of CISO.

Where a GD provides a server, application, or network services to another GD; operational and management responsibilities must be coordinated by both GDs.

4.1. 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 audit of security must remain independent and segregated from the security function.

4.2. Separation of Development, Test and Production Environments[7]

Separation of the development, test, and production environments is required; either logically or physically. Processes must be documented and implemented to govern the transfer of

[7] Reference document: "Information Security Policy of State of NM, USA and State of NY, USA"

software from the development environment to the production platform. The following controls must be considered:

1 Development software and tools must be maintained on computer systems isolated from the production environment. Contain development software on physically separate machines or separate them by access controlled domains or directories.

2 Access to compilers, editors, and other system utilities must be removed from production systems when not required.

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

4 Controls must be in place to issue short-term access to development officers to correct problems with production systems allowing only necessary access.

5 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 GD to ensure adequate protection of the production environment.

6 Separation must also be implemented between development and test functions. Each GD must consider the use of a stable quality assurance environment where user acceptance testing can be conducted and changes cannot be made to the programs being tested.

4.3. System Planning and Acceptance

Advance planning and preparation must be performed to ensure the availability of adequate capacity and resources. The security requirements of new systems must be established, documented, and tested prior to their acceptance and use.

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.

Acceptance criteria must be developed and documented for new information systems, upgrades, and new versions of existing systems. Acceptance testing will be performed to ensure security requirements are met prior to the system being migrated to the production environment. CISO and GD Asst. ISOs will ensure that the security requirements and criteria for acceptance are clearly defined, agreed, documented, and tested.

4.4. Protection against Malicious Code

Software and associated controls must be implemented across GD systems to prevent and detect the introduction of malicious code. The introduction of malicious code such as a computer virus, network worm program, and Trojan horse can cause serious damage to networks, workstations, and GD data. Users must be made aware of the dangers of unauthorized or malicious code. The types of controls and frequency of updating signature files, is dependent on the value and sensitivity of the information that could be potentially at risk.

4.5. 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 GD developed software will be logged to ensure changes are authorized, tested, and accepted by 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 GD data or software integrity.

5. ACCESS CONTROL POLICY[8]

5.1. User Registration and Management

The user management process must include the following sub-processes:

a Enrolling new users;

b Removing user-IDs;

c Granting "privileged accounts" to a user;

d Removing "privileged accounts" from a user;

e Periodic reviewing "privileged accounts" of users;

f Periodic reviewing of users enrolled to any system; and

g Assigning a new authentication token (e.g. password reset processing).

The appropriate information owner or GD Asst. ISO will make requests for the registration and granting of access rights for GD employees.

For applications that interact with individuals that are not employed by the GD, the information owner and Asst. ISO are responsible for ensuring an appropriate user management process is implemented. Standards and procedures for the registration of such external users must be defined, such requests must be validated, and the scope of access that may be provided must be evaluated. For all such requests the credentials must be provided to prove the identity of the user requesting registration.

5.2. Logon Banner

Logon banners must be implemented on all systems where that feature exists, to inform all users that the system is for all GD's processes and procedures. Logon banners are usually presented during the authentication process. Users will be notified that their actions will be monitored and that they do not have any expectation of privacy.

5.3. Privileged Accounts Management

The issuance and use of privileged accounts will be restricted and controlled. Inappropriate use of system account privileges is often found to be a major contributing factor to the failure of systems that have been breached. Processes must be developed to ensure that uses of privileged accounts are monitored and any suspected misuse of these accounts is promptly investigated. Passwords of multi-user system privileged accounts must be changed more often than normal user accounts.

[8] Reference document: "Information Security Policy of State of NM, USA and State of NY, USA"

5.4. User Password Management

Passwords are a common means of authenticating a user's identity to access an information system or service. Password standards must be developed and implemented to ensure all authorized individuals accessing GD resources follow proven password management practices. These password rules must be mandated by automated system controls whenever possible. These password best practices include but are not limited to:

a passwords must not be stored in clear text

b use passwords that are not easily guessed or subject to disclosure through a dictionary attack

c keep passwords confidential – do not share with other individuals

d change passwords at regular intervals – once every six (6) months

e change temporary passwords at the first logon

f when technology permits, passwords must contain a mix of alphabetic, numeric, special, and upper/lower case characters

g Passwords must not be inserted into email messages or other forms of electronic communication

h Common passwords such as family name, date of birth, pet names, friends name, spouses name, company names or number patterns such as '123456', '654321' or 'abcdefg' should be avoided

i A strong password should consist of an upper case, lower case character, special symbol and digits. It should be at least 8 characters in length

j Passwords must never be written down or stored on line

k Do not include passwords in any automated logon process, e.g., stored in a macro or function key, web browser or in application code

l To ensure good password management, password standards must be implemented on all GD platforms when technically feasible

5.5. Network Access Management

Access to a GD's trusted internal network must require all authorized users to authenticate themselves through use of an individually assigned user-ID and an authentication mechanism, e.g., password, token, smart card, etc. Network controls must be developed and implemented to ensure that an authorized user can access only those network resources and services necessary to perform their assigned job responsibilities.

5.6. User Authentication for External Connections (RAS)

1 Individual accountability is to be maintained at all times, including during remote access.

2 Advance written approval for any such connection must be obtained from the CISO. An assessment must be performed and documented to determine the scope and method of access, the risks involved and the contractual process, and technical controls required for such connection to take place.

3 Because of the level of risk inherent with remote access, use of a stronger password or another comparable method is required prior to connecting to any GD network. All sessions are subject to periodic monitoring.

4 When accessing a GD network remotely, identification and authentication of the entity requesting access must be performed in such a manner as to not disclose the password or other authentication information that could be intercepted and used by a third party.

5 Use of a common access point is required. This means that all remote connections to a computer must be made through managed central points-of-entry. Using this type of entry system to access a GD computer provides many benefits, including simplified and cost effective security, maintenance, and support.

6 For a vendor to access GD computers or software, individual accountability is also required. For systems (hardware or software) where there is a built-in user-ID for periodic maintenance, this account must be disabled until the user-ID is required. The actions performed while this vendor user-ID is in use must be logged. Since these accounts are not regularly used, the vendor user-ID must be disabled, the password changed, or other controls implemented to prevent or monitor unauthorized use of these privileged accounts during periods of inactivity.

7 In the special case where servers, storage devices, or other computer equipment have the capability to automatically connect to a vendor to report problems or suspected problems; the CISO must review all such connections and document such a process to ensure that connectivity does not compromise the GD's information or other third party connections.

8 Working from a remote location must be authorized by the CISO and appropriate arrangements made for this function through written policy and procedure, to ensure the work environment at the remote location provides adequate security for GD data and computing resources. Training must be in place to protect against theft of GD equipment, unauthorized disclosure of GD information, misuse of GD equipment, unauthorized access to the GD internal network, or other facilities by anyone including family and friends. The following controls must be considered and appropriately implemented, monitored and audited:

   a The physical security of the remote location, including using a laptop at any location other than an employee's work station. Physical security of the equipment used for remote access (e.g. such as cable locking device, or locking computer cabinet/secure storage area)

   b The accessing mechanism and the method of transmitting information given the sensitivity of GD's internal system

   c Appropriate continuity procedures including backing up critical information

   d A definition of the classification of the information, the systems and services that the remote user is authorized to access

   e Documented procedures and necessary tools allowing for secure remote access such as authentication tokens and/or passwords, including procedures for revocation of authorization, and return of equipment

   f Hardware and software support and maintenance procedures including anti-virus software and maintenance of current signature files

   g Implementation of suitable network boundary controls to prevent unauthorized information exchange between GD networks connected to remote computers and externally connected networks; such as the Internet. Such measures include firewalls and intrusion detection techniques at the remote location.

5.7. Segregation of Networks

When the GD network is connected to another network or becomes a segment on a larger network, controls must be in place to prevent users from other connected networks access to sensitive areas of the GD's private network. Routers, switches, firewalls or other technologies must be implemented to control access to secured resources on the GD network.

5.8. Operating System Access Control

Access to operating system code, services, and commands must be restricted to only those individuals necessary in the normal performance of their job responsibilities. All individuals (systems programmers, database administrators, network and system administrators, etc.) will have a unique privileged account (user-ID). These individuals should also have a second user-ID when performing normal departmental transactions; such as, when accessing the GD e-mail system for their personal and sole use so that actions can be traced to the responsible person.

1. User-IDs on Operating Systems must not give any indication of the user's privilege level, e.g., Supervisor, Manager, Administrator, etc.
2. In certain circumstances, where there is a clear requirement or a system limitation, the use of a shared user-ID/password for a group of users or a specific job can be used. Written approval by CISO must be documented in these cases. Additional compensatory controls must be implemented to ensure accountability is maintained.
3. Where technically feasible, default administrator accounts must be renamed, removed, or disabled. The default passwords for these accounts must be changed if the account is retained, even if the account is renamed or disabled.

5.9. Application System Access Control

Access to GD functional applications must be restricted to those who need to access those applications or systems as part of their job responsibilities. Access to source code for applications and systems must be restricted and these accesses should be further restricted so that only authorized GD Asst. ISOs and GD authorized contractors can access only those applications and systems they directly support.

5.10. Monitoring System Access and Use

Systems and applications must be monitored and analyzed to detect deviation from the access control policy and record events to provide evidence and to reconstruct lost or damaged data. Audit logs, recording exceptions and other security-relevant events must be maintained in record retention schedules.

6. SYSTEMS DEVELOPMENT and MAINTANANCE POLICY[9]

To ensure that security is built into all GD information systems; all security requirements including the need for rollback arrangements must be identified during the requirements phase of a project. Such requirements must be justified, agreed to, and documented as part of the overall function for a GD information system. To ensure this function is performed, the CISO must be involved in all phases of the system development lifecycle, right from the requirements definition phase, through implementation, up-gradation and eventual application retirement.

[9] Reference document: "Information Security Policy Guidelines by Cyber Security Works Inc., USA and CAaNES LLC., USA."

A process must be established and implemented for each application to:

a Address the functional risks and develop a profile of the data to help to understand the risks;

b Identify security measures based on the risk profile and protection requirements;

c Identify and implement specific controls based on security requirements and technical architecture;

d Implement a method to test the effectiveness of the security controls;

e Identify processes and standards to support changes, ongoing management and to measure compliance.

Controls in systems and applications can be placed in many places and serve a variety of purposes. The specific control mechanisms must be documented at the application level, GD's System Development Methodology, and in the GD's security standards documents.

6.1. Cryptographic Controls

a. Encryption is an important security layer that is used to protect the confidentiality of information. Encryption is an effective tool in mitigating the threat of unauthorized access to data. However, there are other threats, such as a hacker gaining access to an authorized user account. In such cases more stringent controls such as the use of multiple encryption levels must be considered.

b. Based on a risk assessment, the required level of protection must take into account the length of the cryptographic key employed. The larger the key length, the greater the cryptographic strength. In deciding what is best for the GD the benefits of both stand-alone and enterprise level encryption solutions must be considered.

c. A secured environment must be established to protect the cryptographic keys used to encrypt and decrypt information. Keys must be securely distributed and stored. Access to these keys must be restricted to only those authorized GD Asst. ISOs who have a functional need to access the keys. Compromise of a cryptographic key would cause all information encrypted with that key to be considered unencrypted.

6.2. Protection of System Test Data

Test data is intended to test the expected behavior of software, systems and applications. Test data is developed to test a comprehensive set of conditions and outcomes; including exception processing and error conditions to demonstrate accurate processing and handling of information and the stability of the software, system, or application.

Once test data is developed it must be protected and controlled for the life time of the application software. In those cases where test data is reused, whenever modifications are made to the software, system or application then the test data must be protected and controlled during the entire useful life. This protection mechanism is essential to ensuring a valid and controlled simulation with predictable outcomes.

Production data may be used for testing only if the following controls are applied;

a A functional use case is documented, approved in writing by the information owner and access controls, system configurations, and logging requirements for the production data are applied to the test environment; or

b A functional use case is documented, approved in writing by the information owner, and GSI will be masked or overwritten with fictional information and the data will be deleted as soon as the testing in completed.

6.3. Change Control Procedures

To minimize the possibility of corruption of information systems, strict controls over changes to information systems must be implemented. These change control procedures will apply to GD software applications as well as systems software used to maintain operating systems, network software, hardware changes, etc. Each GD is responsible for developing, implementing, and enforcing a formal change control procedure for software applications, which ensures:

1 Security and control procedures are not compromised;

2 Support programmers are given access only to those parts of a system necessary to perform their jobs;

3 A formal agreement and approval processes for changes are implemented;

4 As changes occur, the necessary changes in associated documentation and disaster plan occur;

5 In addition, access to source code libraries for both GD software applications and operating systems must be tightly controlled to ensure that only authorized information owners have access to these libraries and that access is logged to monitor actions.

7. COMPLIANCE POLICY

7.1. Monitoring

Consistent with applicable laws (IT Act, Right to Information Act and Copyright Act) and GD policies; the GD reserves the right to monitor, inspect, and/or search at any time, all GD information systems. Since GD's computers and networks are provided for official purposes, employees shall have no expectation of privacy in the information stored in, or sent through these information systems. GD IT management additionally retains the right to remove from its information systems any unauthorized material

7.2. Compliance

7.2.1. Successful implementation of information security must be developed and tailored to each specific GD's functions and objectives. The approach of implementing information security policy in a GD shall be based on International Standard ISO/ISE 27001.

7.2.2. Compliance with this policy is mandatory. Each user must understand his/her role and responsibilities regarding information security issues and protecting GD's information. The failure to comply with this or any other security policy that results in the compromise of GD's information confidentiality, integrity, privacy, and/or availability may result in appropriate action as permitted by law, rule and regulation. Each GD will take every step necessary, including legal and administrative measures, to protect its assets and shall establish the post of CISO to monitor compliance with policy matters.

7.2.3. At the State Government level, each GD shall implement a process to determine the level of compliance with this policy. A review to ensure compliance with this policy must be conducted annually by a third party agency and the HOD will review and certify this report regarding the GD's level of compliance to the entire GD by December 31st of each year. Areas where compliance with the policy requirements is not met will be documented and a plan will be developed to address the deficiencies.

7.2.4. GD Asst. ISO, supervisors and information owners will ensure that all security processes and procedures within their areas of responsibility are followed. In addition,

all official units within the GD may be subject to regular reviews to ensure compliance with security policies and standards.

7.3. Enforcement and violation Handling

7.3.1. Any compromise or suspected compromise of this policy must be reported to the appropriate GD officer. Any violations of security policies may be subject to disciplinary or other appropriate action in accordance with IT Act, rules, regulations or policy.

7.3.2. Security incident reports indicating the risk level of the violation must be reported to responsible official units. Access authorization for user accounts involved in a compromise may be suspended during the time when a suspected violation is under investigation. Automated violation reports generated by the various security systems will be forwarded to the appropriate Security Officer for timely resolution.

7.4. Document Change Management

Requests for changes to this policy must be presented by the CISO to the HOD. If the HOD agrees to the change, he or she will formally draft the change and have it reviewed and approved through the normal policy approval process. Each CISO will be responsible for communicating the approved changes to their individual units. This policy and supporting policies and standards will be reviewed at a minimum on an annual basis.

7.5. Information System Policy Violations

GDs are required to identify all applicable laws, regulations and other government directives as applicable to their specific domain of work. Besides this they are also required to implement the following Acts and their associated regulations:

1 IT Act
2 Right to Information Act
3 Copyright Act
4 Evidence Act.

Failure to follow the guidelines set forth in this document or referenced shall be punishable as per applicable Government laws and regulations.

8. CONFIDENTALITY

A confidentiality statement similar to the one below shall be incorporated in the department specific information security policy.

8.1. The contents of this document shall not be commercially used or disclosed. This document is essentially meant for internal circulation within the *GD,* therefore all users shall hold the responsibility to keep it highly confidential. The policy can also be disclosed to a third parties on the following terms mentioned hereafter.

8.2. Any confidential information or materials derived from here available to any other person or entity other than the persons in the direct employment of the *GD* who have a need to access to and knowledge of the information solely for the purpose authorized above, needs to obtain permission from the Head of the Department. The confidential information may be disclosed to consultants only if the consultant has executed Non-Disclosure Agreement (NDA) with the *GD* that contains terms and conditions that are no less restrictive than these and such consultant shall also be liable to the Original disclosing party to any unauthorized use or disclosure. *GD* shall take appropriate measures by giving instructions and a written agreement prior to disclosure to such entities to assure against unauthorized use or disclosure. The Receiving

Party agrees to notify the *GD* immediately if they learn of any use or disclosure of *GDs* confidential information and violation of the terms of this Agreement.

8.3. Definition and Acronyms[10]

Approved Storage Facility:	GD physically secured central servers/*data* centers and other facilities as approved in writing by *Head of Department*, upon the recommendation of *CISO*. These facilities include the internal *data* communication networks.
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.
Availability:	This is the property of being operational, accessible, functional and usable upon demand by an authorized entity (e.g. a *system* or *user*).
Biometric Data:	Unique physical or behavioral characteristics, such as fingerprints or voice patterns, used as a means of verifying personal identity.
Official Risk:	This is the combination of *sensitivity*, *threat* and *vulnerability*.
CIO:	Chief Information Officer
Classification:	The designation given to information or a document from a defined category on the basis of its *sensitivity*.
Computer:	All physical, electronic and other components, types and uses of computers, including but not limited to hardware, software, central processing units, electronic communications and systems, databases, memory, Internet service, information systems, laptops, *PDAs* and accompanying equipment used to support the use of computers, such as printers, fax machines and copiers, and any updates, revisions, upgrades or replacements thereto.
Confidentiality:	The property that *information* is not made available or disclosed to unauthorized individuals, entities, or processes.
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.

[10] Reference document: "Information Security Policy of State of NM, USA"

Data:	See *Information*.
Denial of Service:	An attack that takes up so much of the company's official resource that it results in degradation of performance or loss of access to the company's official services or resources.
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 in the accomplishment of the *GD's* objectives as determined by *GD's* officer.
DMZ:	Demilitarized zone; a semi-secured buffer or region between two networks such as between the public internet and the trusted private *GD* network.
Electronic Storage Media:	Media used to record and store *data*, including, but not limited to hard drives, tapes, removable drives of any kind, flash drives or other USB storage media, CDs, diskettes, etc.
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*.
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 Custodian:	An individual, organizational unit (e.g., IT, Operations, Systems, Network) or entity acting as caretaker of *information* on behalf of its owner.

Information Owner:	An individual or a group of individuals that has responsibility for making *classification* and *control* decisions regarding use of *information.* See Organizational and Functional Responsibilities.
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.
ISO:	Information Security Officer.
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*. All mainframes, servers and microcomputers are *multi-user systems*, but most personal *computers*, laptops and workstations are not.
Need to Know	Refer *Least Privilege*.
Passphrase:	A sequence of words or other text used to control access to a *computer system*, program or *data*, similar to a password in usage, but generally longer for added security (e.g., betty was smoking tires and playing tuna fish).
PDA:	Refer *Personal Digital Assistant.*

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 extended, unauthorized or elevated privileged 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 (GSI):	Any *information* where *unauthorized access*, disclosure, modification, destruction or disruption of access to or use of such *information* could severely impact the *GD*, its critical functions, its employees, its customers or *third parties*. This term shall be deemed to include, but is not limited to, the *information* encompassed in existing statutory definitions. *GSI* includes, but is not limited to: • *Information* concerning a person which, because of name, number or other identifier, can be used to identify that person, in combination with: ❖ driver's license number or PAN card number or Ration Card number; or ❖ mother's maiden name; financial services account number or code; savings account number or code; checking account number or code; debit card number or code; automated teller machine number or code; electronic serial number. • Other *information* which could be used to assume a person's identity or gain access to a person's financial resources or credit. • *Information* used to authenticate the identity of a person or process (e.g., PIN, password, *passphrase*, *and biometric data*). This does not include distribution of one-time-use PINs, passwords, or *passphrases*. • *Information* that identifies specific structural, operational, or technical *information*, such as maps, mechanical or architectural drawings, floor plans, operational plans or *procedures*, or other detailed *information* relating to electric, natural gas, steam, water supplies, nuclear or telecommunications *systems* or infrastructure, including associated facilities, including, but not limited to: ❖ training and security *procedures* at sensitive facilities and locations as determined by the GD location; ❖ plans for disaster recovery and functional continuity; and

	❖ 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 *GDs* IT management.
Physical Security:	The protection of *information* processing equipment from damage, destruction or theft; *information* processing facilities from damage, destruction or unauthorized entry; and personnel from potentially harmful situations.
GSI:	Government *Sensitive Information*.
Privacy:	The right of individuals and organizations to control the collection, storage, and dissemination of *information* about themselves.
Privileged Account:	The user-ID or account of an individual whose job responsibilities require special *system authorization*, such as a network administrator, system administrator, etc. Special *authorization*s are allocated to this account such as auditor, UNIX root or Microsoft Administrator.
Procedures:	Specific operational steps that individuals shall take to achieve goals stated in this policy.
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.
Risk:	The probability of suffering harm or loss. It refers to an action, event or a natural occurrence that could cause an undesirable outcome, resulting in a negative impact or consequence.
Risk Assessment:	The process of identifying *threats* to *information* or *information systems*, determining the likelihood of occurrence of the *threat*, and identifying *system vulnerabilities* that could be exploited by the *threat*.
Risk Management:	The process of taking actions to assess *risk*s and avoid or reduce *risk* to acceptable levels.
Role-Based Access Control:	An approach to restricting *system* access where permissions to perform certain operations are assigned to specific job functions.
GD:	Government Department
Security Administration:	The actions and responsibility for administering the security mechanisms including identification and *authentication* establishment and *authorization* maintenance.

Security Management:	The responsibility and actions required to manage the security environment including the *security policies* and mechanisms. Imposed for all *users*. These rules usually rely on a comparison of the *sensitivity* of the resources being accessed and the possession of corresponding.
Security Policy:	The set of criteria for the provision of security services based on global rules imposed for all *users*. These rules usually rely on a comparison of the *sensitivity* of the resources being accessed and the possession of corresponding attributes of *users*, a group of users, or entities acting on behalf of *users*.
Sensitivity:	The measurable, harmful impact resulting from disclosure, modifications, or destruction of *information*.
Sniffing:	Monitoring network traffic.
Spamming:	Blindly posting something to a large number of groups.
Spoofing:	Representing yourself as someone else.
Standard:	Sets of rules for implementing policy. *Standards* make specific mention of technologies, methodologies, implementation *procedures* and other detail factors.
State:	The State of TAMIL NADU
Systems(s):	An interconnected set of *information* resources under the same direct management control that shares common functionality. A *system* may include hardware, software, *information, data*, applications or communications infrastructure.
Technical Security Review:	A *technical security review* would consist of reviewing the *controls* built into a *system* or application to ensure they still perform as designed and are in compliance with documented security policies and *procedures*. It would also include reviewing security rules such as access control lists, testing of *firewall* rules, etc. This type of testing includes intrusion and/or *penetration testing* of *controls*.
Third Party:	Any non-*GD* employee such as a contractor, vendor, consultant, intern, another *GD employee* (e.g., ELCOT), etc.
Threat:	A force, organization or person, which seeks to gain access to, or compromise, *information*. A *threat* can be assessed in terms of the probability of an attack. Looking at the nature of the *threat*, its capability and resources, one can assess it, and then determine the likelihood of occurrence, as in *risk assessment*.
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.

User:	Any *GD* employee or authorized third party contractor(s) or any other individual(s) who are authorized by *GD* to access a *system* for a legitimate government purpose.
Value:	A measure of worth which can be expressed in monetary terms or in terms of importance to the *GD*.
Virus:	A program that replicates itself on *computer systems* by incorporating itself into other programs that are shared among *computer systems*. Once in the new *host*, a *virus* may damage data in the host's memory, display unwanted messages, crash the host or, in some cases, simply lie dormant until a specified event occurs (e.g., the birth date of a historical figure).
Volume Level Encryption:	Protects data by encrypting the entire partition of a disk or, in the case of a single partition hard drive, the entire drive.
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.
World Wide Web (WWW):	A hypertext-based *system* designed to allow access to information in such a way that the information may physically reside on locally or geographically different servers. This access was greatly improved through the introduction of a graphical interface to the *World Wide Web* called a web browser. Netscape, Fire Fox and Internet Explorer are few of the most popular web browsers.
Worm:	A program similar to a virus that can consume large quantities of network bandwidth and spread from on network to another.

9. APPENDIX

9.1.Appendix I

Incident Response activities during the First Hour

1. Introduction

The primary objective of incident response actions during 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 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.

a. Mean of Detection

The means of detecting anomalies and abnormal conditions that require response actions are Users, System/Network Administrators, technical tools and external alerts from security agencies such as CERT-In

3. Symptoms of incidents and response actions

Table 3.1 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 3.2 outlines Indications of different types of Cyber Crises generally noticeable by trained users, System Administrators & tool based detection mechanisms and response actions required and authorities responsible for the actions.

Table 3.1 General symptoms of incidents noticeable by all types of users & System Administrators and related response actions.

Symptoms/Alerts	Source of detection	Response Actions	Who to Handle
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
Symptoms/Alerts	**Source of detection**	**Response Actions**	**Who to Handle**
• 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 or successful social engineering attempts	• User • System Administrator	• Collect all details such as email content, header, etc. and examine. • Alert other users	• 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 & Antispyware • Antivirus and Antispyware shall be updated regularly	• User • System Administrator
• 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 parches / 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

Table 3.2 Indications of different types of Cyber Crises generally noticeable by trained users, System Administrators & tool based detection mechanisms and Response actions

Symptoms/Indications /Alerts	Source	Response Actions	Who to Handle
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 logos.	• Website Administrator • Network Administrator • Asst. ISO
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	• Asst. ISO • Network Administrator • System Administrator
SPAM attacks			
• Abnormal surge in SMPT 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 • Asst. ISO

Symptoms/Indications/ Alerts	Source	Response Actions	Who to Handle
Attacks on Mail Servers			
• Non availability 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 • Asst. ISO
Identity Theft Attacks through spoofing			
• Detection of suspicious network connections • Detection of packets with suspicious source address • Emails from masqueraded account name	• 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) • Enforce email authentication • Report to local Incident Response Team/CERT-In	• Network Administrator • Asst. ISO
Phishing attacks			
• Reporting of phishing email/website	• Users • Antiphishing/ fraud detection services • CERT-In/external agencies	• Report phishing incident to local IR Tea,/ CERT-In • Report phishing URL to phishing filters • Send phishing emails and details of phishing website to CERT-In	• Users • Asst. ISO
Denial of Service (DoS) attacks			
• Non availability of services such as website, email etc • System crashes • Bandwidth congestion • Surge in traffic	• Users • Website Administrator	• Indentify the type of attack such as flooding of particular types of packets/requests (TCP SYN, ICMP etc) by examining logs of Router/IPS/IDS/Firewall • Indentify the attack sources • Block the attack sources at Router/Packet filtering device • Check Router Configuration and implementing Egress and Ingress filtering to	• Asst. ISO • Network Administrator • System Administrator

		• 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	Who to Handle
Distributer 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	• Indentify 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 • Asst. ISO • System 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 servers • Restrict zone transfers to Secondary name servers only • Block invalid DNS	• Network Administrator • Asst. ISO

		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 indentify rouge 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 • Asst. ISO
Application Level attacks			
• Unauthorized changes to Data • Suspicious user activity • Elevation of privilege of user accounts • Presence of malicious links/ content	• 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 sources from applications logs validation • Enforce Input Validation • Apply latest patches/ updates • Report to local Incident Response Team/CERT-In	• Web Administrator • Database Administrator • Asst. ISO

Symptoms/Indications /Alerts	Source	Response Actions	Who to Handle
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 indentify 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	• Indentify the other devices due to which RF interference occurs and physically remove them. • Detect rouge access points and remove them • If attack persists switch critical functions to wires networks • Report to local Incident Response Team/CERT-In	• Network Administrator • Asst. ISO
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	• Indentify the type of scans/ probes by examining logs of Router /IDS/IPS/Firewall • Indentify the sources of scanning • Report the incidents with relevant logs to CERT-In other incident response teams	• Network Administrator

4. Conditions for escalation and detailed analysis

It is quite possible to come to a conclusion that there would be situations that call for:

- Actions within the organisation
- Actions beyond an organisation

The users observing the symptoms/indications mentioned in Table 3.1 and 3.2 shall immediately report the same to the concerned system/network administrator or designated authority within the organisation.

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.

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

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. What needs to be reported to law enforcement authority and 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 spyware, 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 applications such as e-Governance, etc.

9.2.Appendix II

Incidents Response Activities in the in the First 24 Hours

9.2.1.Introduction

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 guideline prescribe the incidents calling for detailed root cause analysis of the problem, possible escalation within and beyond an organisation to derive appropriate incident response support and satisfactory remedial actions.

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 organisations shall be prepared to respond appropriately.

9.2.2.What is an incident

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

9.2.3.Incident 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 called computer security incident Response Team (CSIRT). A CSIRT operates under a defined constituency and authority. Depending upon the services to be performed by the CSIRT, a team structure and operations hours are defined. CSIRT performs its operations as per defined policies and standard operating procedures (SOPs)

9.2.3.1. Phases of incident Response

The incident response process had several phases, from initial preparation through post – incident analysis. The initial phase involves establishing and training an incident response team, and acquiring the necessary tools and

resources for incident analysis and response. During preparation, the organization also attempts 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, residual risk will inevitably persist after controls are implemented. Furthermore, no control is fool proof. Detection of security breaches is thus necessary to alert the organization whenever incidents occur.

In keeping with the severity of the incident, the organization can act to mitigate the impact of the incident by containing it and ultimately recovering from it. After the incident is adequately handled, the organization issues a report that details the cause and cost of the incident and the steps the organization take to prevent future incidents. The major phases of the incident response process thus are pre-incident preparation, detection and analysis, containment, mitigation and recovery, and post – incident activities as shown in the incident occurs. Proper mix of technologies and processes need to be in place so that the people involved in incident response know exactly what to do, and they have the appropriate tools and the pre- approved support of their management.

9.2.3.2. Essential Incident Response Steps during an Attack

Too often, individuals do not feel empowered to act or are not provided with enough information to know what steps they are supposed to take. The teams that are responsible for monitoring the network systems and environment are not usually responsible for incident response activities. Incidents in progress can be discovered by a wide variety of different people, most of whom cannot be given response roles, so they need to know who to notify to start the response process. The success of this step relies on the person being notified to be in a position to respond. Every functional area shall have a sufficiently detailed set of contingency plans so that everyone responsible for incident response knows what his or her first steps shall be in any specific attack or failure situation.

Notification — Review the attack response matrix to identify who to contact. Notify the incident response lead/manager as soon as an incident is suspected. If such a person is not available, then notify the operational manager for the area requiring containment. For example, bandwidth-consuming worm attacks require modifications to firewall and router settings or signature updates and/or configuration changes to security defenses, such as an intrusion prevention system (IPS).

Detection and analysis — during the first minutes of an 'attack, organizations shall work toward identifying the attack type, scope and vectors (detection and analysis) and then implement the appropriate controls to contain the attack and quarantine any compromised hosts (containment). Depending on the attack type and its impact on the organisation, the initial step may be containment. Although it is preferable to understand the full scope of the incident before taking action, if it becomes apparent that significant damage is quickly spreading, then the plan

shall allow for a significant emergency response. This would be the digital equivalent of closing the bulkhead doors or turning on the fire sprinklers.

Containment — An essential part of containment is decision-making (e.g., shut down a system, disconnect it from a wired or wireless network, disable certain functions or stop some of services). Such decisions are much easier to make if strategies and procedures for containing the incident have been predetermined. Containment strategies vary based on the type of incident.

Mitigation — Update security defenses to limit any continued impact. Generally this involves updating host-based security products with the latest vendor updates; antivirus, anti-spyware, host-based intrusion prevention and personal firewalls may also need configurations changed. In many cases, these tasks shall be performed within the first 24 hours.

9.2.3.3. Attack Detection and Analysis

Most security incidents initially appear as an IT operational issue or failure and are identified by observation of certain IT conditions, including performance issues, anomalous behavior, policy violations and service disruptions. Identifying the scope of an attack can be very difficult if one is manually auditing system logs and event data, most of which is extremely voluminous and irrelevant.

The following technologies provide capabilities for effective attack detection and analysis:

Security Information and Event Management (SIEM) – SIEM products provide situational awareness through the collection, aggregation, correlation and analysis of disparate data from various sources. The information provided by these tools help in understanding the scope of an incident.

Intrusion Detection and Prevention systems (IDS and IPS) – IPS products that have detection capabilities shall be fully used during an incident to limit any further impact in the organization.IDS and IPS products are often the primary source of information leading to the identification of an attack. once the attack has been identified, it is essential to enable the appropriate IPS rule sets to block further incident propagation and to support containment and eradication.

Network Behaviour Analysis (NBA) – Network wide anomaly –detection tools will provide data on traffic patterns that are indicative of an incident. Once an incident has been identified through the use of these tools, it is important to capture that information for the purpose of supporting future mitigation activities, including operational workflow to ensure that the information from these tools is routed to the appropriate response team.

Managed Security Service Provider (MSSP) – If an organization has outsourced security event management to an MSSP, the latter shall provide notification when an incident requires attention. Organization shall obtain as much information on the incident as possible from MSSP and implementation remediation steps as recommended by MSSP.

9.2.3.4. Containment

Once the scope of the attack is understood, it is time to contain and eradicated the attack. Many attacks take advantage of known, patchable vulnerabilities. Although it is important to eliminate the root cause by applying patches and reconfiguring devices, attempting to perform these actions as part of the response to an in-progress incident can only be effective if patching can be accomplished more quickly than the attack itself. Additional hosts may become infected during such an update; consequently, in many causes, it is important to implement shielding controls as a first stage of containment before talking the time for a more – comprehensive response.

The better-prepared the organisation is, the easier it will be to use technology to effectively automate much of the containment phase and to couple the technology with already-established incident response and business continuity programs

Shield – IPSs provide in time blocking and containment capabilities at the network level. Additionally, various desktop security products can perform containment of malware or other compromises at the host level. These shall be updated immediately and configured to further block the attack.

Block – Access Control Lists on networking devices can limit the ability of an automated malware attack to replicate throughout the network and it can contain a potential virus or worm outbreak to a single device. As soon as an attack has been identified ACL's shall be updated to limit any further attack damage.

9.2.3.5. Mitigation and Recovery

Once the failure rate has been brought down to an acceptable level, either through shielding, isolation or powering off, then it is time to start putting a more – comprehensive mitigation into effect although this often takes the form of patching, it shall also be considered as an opportunity to determine whether a particular bit of code actually needs to be in use. All systems that suffered attack damaged, or are suspected of having been damaged shall be examined before they can be restored. Depending on the type of attack, it may be desirable to maintain a complete copy of the compromised system for further analysis and potential prosecutorial efforts. Sometimes, the examination of the damage may indicate that a repair is infeasible. For example, in the case of a root kit "Trojan horse" or other incident that results in an attacker gaining full administrative control of a device, the only option may be to revert to an archived copy of the device. However, knowing which image to restore would require reliable

knowledge of exactly when the device was compromised. If this cannot be determined, then the most prudent action would be to rebuild the system from scratch.

In recovery, administrators restore systems to normal operation and (if applicable) harden systems to prevent similar incidents. Recovery may involve such actions as restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing pass words, and tightening network perimeter security (e.g., firewall rule sets, boundary router access control lists). It is often desirable to employ higher levels of system logging or network monitoring as part of the recovery process.

9.2.3.6. Post – Incident Activity

Each Incident response team shall evolve to reflect new threats, improved technology, and lessons learned. Many organizations have found that holding a "lessons learned" meeting with all involved parties after a major incident, and periodically after lesser incidents, is extremely helpful in improving security measures and the incident handing process itself.

Another important post-incident activity is creating a follow-up report for each incident, which can be quite valuable for future use. First, the report provides a reference that can be used to assist in handing similar incidents. Creating a formal chronology of events (including time stamped information such as log data from systems) is important for legal reasons, as is creating a monetary estimate of the amount of damage the incident caused in terms of any loss of software and files, hardware damage, and staffing costs (including restoring services)

Example of an Attack Response Matrix

S.No	Attack Type	Severity Level	Target(s)	Asset Value	Response	Who to Handle (Role)	Owner (Group)
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. Indentify the sources of scans 4. Block the sources of scanning	Network Administrator	Network operations
2	Denial of Service (DOS)	High	External web server Router	High	1. Indentify targets i.e. IPs which are under DoS attack 2. Indentify IPs which are doing DoS attack i.e. attack vector; restrict attack vector (through network access control list modification, firewall rules or constrainment of the endpoint itself) 3. Implement alternative services and resources as required to allow for continued providing of services	Web server Administrator Network Administrator	Web services, Network operations
3	Denial of Services	Low	Intrusion detection system (IDS)	Low	1. Disable Intrusion Detection System(IDS) 2. Deploy an Intrusion Prevention System (IPS)	Network Administrator	Network operations
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. Indentify database servers that are not updates, and quarantine if infected 5. Download and distribute software patches if applicable 6. Notify staff of issues; provide information and status for interruption of services	Network Administrator System Administrator	Network operations
5	Malicious Code (Virus/ Worm/ Trojan) Outbreak	Medium	User desktops	Medium	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. Indentify devices that are	Network administrator, Individuals Users	Desktop Administration /e-mail support Network operations

					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])		
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. Indentify 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	Network operations
7	Privilege Escalation Root kit	Critical	File server or any other server	High	1. Quarantine the server 2.Switch to alternative server 3. Perform forensics analysis 4. Re-image server (once infected with a root kit, the entire system is suspect).	System Administrator Security forensic analyst	Security response and auditing
8	Website Defacement/ Intrusion	Critical	Website/ Web server	High	1. Disconnect web server 2. Host and run website from a 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	Web server Administrator, Asst. ISO	Web Services

9.3.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 *(Obtain 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:

BSNL *(To be obtained from BSNL)*

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 for Sify *(To be obtained from Sify)*

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 for Airtel *(To be obtained from Airtel)*

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 for Reliance *(Obtain from Reliance)*

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:

9.4.Appendix IV

9.4.1.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	❑

9.4.2.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	❑

9.4.3.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	❑

9.4.4.Check List for Information Owners

Every morning review all application logs for abnormalities	❑
Document all types of requests submitted to system administrator on a daily basis	❑
Take backups of critical applications and respective database's as per required frequency	❑
Verify by restoring backup's as per criticality of the application or database	❑

9.5.Appendix V

Incident Reporting Form

Form to report Incidents to CCRT-In		
For official use only		Incident Tracking Number : **CERTIn-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 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	❑ Anomalies	

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

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		

10. BIBLIOGRAPHY

10.1. Doc No.: CERT-In/NISAP/01 – Information Security Policy for Protection of Critical Information Infrastructure, Revision 1 by CERT-In, May 2006.
http://www.cert.org.in/ITSAuditing/Info_Sec_Policy.pdf

10.2. Information Security Management Implementation Guide for Government Organizations, Ver. 1.1 by STQC Directorate, New Delhi, August 2007.
http://www.cert.org/archive/pdf/07tn020.pdf

10.3. Information Security Policy Guidelines by Cyber Security Works Inc., USA and CAaNES LLC., USA.

10.4. Information Security Policy of State of NM, USA and State of NY, USA.

10.5. Governing for Enterprise Security, Implementation Guide by US-CERT.
http://www.cert.org/archive/pdf/07tn020.pdf

10.6. Crisis Management Plan for Countering Cyber Attack and Cyber Terrorism by CERT-In, Jan 2009

10.7. The Appendix in this document (Section 9) is a compilation from two documents mentioned in section 10.1, section 10.5 and section 10.6

10.8. Definitions and acronyms from section 8.6 is a compilation from a document listed in section 10.4