BESSEGGEN INFOTECH LLP

Information and Cyber Security framework

Cyber Crisis Management Plan Policy

Reference No.: BESSEGGEN/I&CSF/CCMP

Version: 1.3

30th May 2025

Internal Use Only

Document Control			
Reference No.	BESSEGGEN/I&CSF/CCMP		
Document Name	**BESSEGGEN – Cyber Crisis Management plan**		
Version No.	1.1		
Document Status	Definitive		
Issue Date	08th Aug 2022		
Compliance Status	Mandatory		
Review Period	One year from the date of release or earlier if required		
Security Classification	Internal Use Only		
Distribution	Part of BESSEGGEN I&CSF		
	Name	**Role**	**Signatu re**
Authored by	BESSEGGEN INFOTECH LLP		
Reviewed by	Prince Kumar	Developer	
Approved by	Vibhu Garg	CISO	
Released by	BESSEGGEN INFOTECH LLP		

Document Revision History		
Version	**Release Date**	**Change Description**
1.0	08th Aug 2022	Issued
1.1	14th May 2024	Reviewed
1.2	21st Nov 2024	Reviewed
1.3	30th May 2025	Reviewed

Restriction on Use of this Document

The Cyber Crisis Management Plan is a restricted document as it contains proprietary information. For the purpose of this plan, 'proprietary information' is defined as the information that could have a negative impact **on BESSEGGEN INFOTECH LLP (henceforth named as "BESSEGGEN")**, if improperly released and which could be valuable to external parties/ competitors. Proprietary information is all non-public information rightfully obtained, developed or produced by or on behalf of BESSEGGEN and/or its employees for the benefit of BESSEGGEN. The proprietary information contained in this document is owned by BESSEGGEN and not by the employees.

This document is for restricted distribution only as it contains BESSEGGEN strategy for recovery of critical business processes, and the names, addresses and telephone numbers of the recovery team members. Therefore, the plan should be distributed on a need-to-know basis.

Each individual possessing a copy of the Cyber Crisis Management Plan is responsible for security and control of the document in accordance with the policies for the protection of confidential and proprietary information.

Table of Contents

1. PURPOSE

The purpose of this document is to create Cyber Crisis Management Plan (CCMP) for any unforeseen cyber security crisis incident i.e. virus or malicious software code, cyber-attack, etc. which may cause extensive damage to the critical information infrastructure of the BESSEGGEN INFOTECH LLP.

- To ensure that interruption or manipulations of critical functions/services in the BESSEGGEN are brief, infrequent and manageable and cause least possible damage.
- To enable to draw-up contingency plans in line for countering cyber-attacks and cyber terrorism, equip themselves suitably for implementation, implement, supervise implementation and ensure compliance among all the BESSEGGEN units within their domain.
- To assist BESSEGGEN to put in place mechanisms to effectively deal with cyber security crises and be able to pinpoint responsibilities and accountabilities right down to individual level.

The BESSEGGEN ensure to have a risk management program to undertake information security risk assessment for target environments (e.g. critical business environments, business processes, business applications, computer systems and networks) on a periodic basis.

Cyber security incident Cyber security management shall be prepared and implemented to discover Record, response, escalate and prevent information security events and weaknesses effectively as well timely communication of the govt agencies CERT-in as per defined procedures.

2. SCOPE

The policy guidelines are devised in the context of the BESSEGGEN INFOTECH LLP cyber crisis management plan that covers all the events/incidents within the BESSEGGEN & outside the organization which may have a bearing on the BESSEGGEN business. The scope of this POLICY covers all the BESSEGGEN facilities, premises, employees and third-party vendor supported systems and employees

3. CYBER CRISIS, POSSIBLE TARGETS AND IMPACTS

Term and Definitions Used:

Event

An event is any observable occurrence in a system or a network like a user connecting to a network file share or browsing a web page, or even sending an email, scanning network architecture, etc. Adverse events are those that have a negative consequence that can lead to a disruption of service and have a negative impact on business/ transaction. Examples of such events are system crashes, slow response on system/network, network flooding, high network utilization etc.

Cyber Security Incident

A security incident is defined as an adverse event in an information system and/or network that poses a threat to computer or network security. In other words, an incident is any event that causes, or may cause a breach of information security in respect of availability, integrity and confidentiality. Examples of such incidents could be unauthorized access to information systems, disruption of data, denial of services/availability, misuse of system resources, computer viruses etc. Any violations of an organization's information security policy would also classify as a security incident. A significant cyber incident is a set of conditions in the cyber domain that requires increased national coordination. This increase in national coordination is triggered when the threat level reaches level 3 and beyond

Cyber Security Crisis

A situation wherein security characters of information are compromised as a result of failure of a Network device, an IT system or network of IT systems, due to technical reasons, intentional acts or negligence, leading to consequences that may threaten lives, organizations trust, national security and public confidence. All cyber security crises are cyber security incidents; however, all cyber security incidents are not cyber security crises but may lead to crisis situations if not attended to in a timely manner.

3.1 Physical threats

The different type of physical threats / crisis may be:

a. **External physical threats**: Flooding, lightning, earthquake, wind, tornado, hurricane, ice, fire, chemical
b. **Internal physical threats:** Fire, environmental failure, liquid leakage, electrical interruption
c. **Human physical threats:** Theft, vandalism, sabotage, espionage, errors

3.2 Cyber Threats

3.2.1 Types of Cyber Security Incidents

Any real or suspected adverse event in relation to the security of computer systems or computer networks can be termed as a logical security breach. In other words, a logical security incident can be defined as network or host activity that potentially threatens the security of computer systems. Examples of such incidents could include activity such as:

▪ Attempts (either failed or successful) to gain unauthorized access to a network device/ system or its data

▪ Unwanted disruption or denial of service

▪ The unauthorized use of a device/ system for the processing or storage of data Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent

3.2.2 Nature of Cyber Crisis and Contingencies

Unlike physical attacks, cyber security incidents may be triggered on individual systems, simultaneously on multiple systems and networks in a single or multiple organizations, states and entire nation from places within the country or anywhere outside the country. Physical crises and cyber crises may happen concurrently or follow each other.

Cyber crisis has unique features which are different from a physical crisis. In some cases, the severity of the cyber crisis is high but confined to individuals or organizations in a limited area. In other cases, the severity may be low but widely spread to a larger area.

3.3 Security Requirements

The objectives of information security is preservation of

- Confidentiality: preventing unauthorized access to information.
- Integrity: preventing the unauthorized modification or theft of information.

- Availability: preventing the denial of service and ensuring authorized access to information.
- Non-repudiation or accountability: preventing the denial of an action that took place or the claim of an action that did not take place.

3.4 Nature of Cyber Crisis, Possible targets and Impact.

Table 1.0 provides a snapshot of the nature of cyber security incidents which include attempts (either failed or successful) that can trigger a crisis at individual / organization, multiple organizations, state level or national level.

Table 1.0: Nature of Cyber Crisis, Possible Targets and Impact

Type of Cyber Crisis	Possible Targets	Related impact
1. Targeted Scanning, Probing and Reconnaissance of Networks and IT Infrastructure	● Sensitive and Critical Information infrastructure ● Infrastructure at Data Centers and Network Operation Centers ○ Routers, Switches, Database and DNS Servers ○ Web portals	● Precursor to hacking and focused attack leading to cyber crisis ● Total/partial disruption of e-Governance, Public and Banking services
2. Large scale defacement and semantic attacks on websites ● A website defacement is when a Defacer breaks into a web server and alters the contents of the hosted website ● Attackers change the content of a web page subtly, so that the alteration is not immediately apparent. As a result, false information is disseminated	● BESSEGGEN INFOTECH LLP portal	● Loss of image, reputation etc. ● Total/partial disruption of services/activities ● Dissemination of false/misleading information ● Monetary loss, damage to reputation, loss of image etc.
3. Malicious Code attacks (virus/worm/ /Trojans/Botnets) ● Malicious code or malware is software designed to infiltrate or damage a computer system without the owner's informed consent. Malicious code is hostile, intrusive, or annoying software or program code. Commonly known malware are virus,	● Master consumer database. ● Consumer Billing details ● Company financials	● Hanging of Computer systems ● Partial or No response from Computer system ● Total/partial corruption of data bases ● Total/partial breakdown of internet access services

worms, Trojans, Ransomware, Crypto miner, spyware, adware and Bots **3.2 Malware affecting Mobile devices** ● Malicious code and malicious applications (apps) affecting operating systems/platforms used for mobile devices such as Symbian, Android, iOS, Windows Mobile etc. **3.3 Malware affecting IoT devices** ● Compromised IoT devices, such as cameras, routers, wearables, and other embedded technologies, infected with malware like Mirai	● Mobile devices using affected Operating System and connected Computer systems ● Sensitive and Critical Information infrastructure ● users (consumers/corporate)	● Monetary loss, damage to reputation, loss of image etc. ● Unauthorized disclosure of user's data and contact details ● Total/partial disruption of services/activities in one or more critical area ● Data Theft, possible espionage
4. Large scale SPAM attacks Spamming is the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages. SPAM mails may also contain virus, worm and other types of malicious software and are used to infect Information Technology systems. As a result, spamming could disrupt e-mail services, messaging systems and mobile phone communications.	● BESSEGGEN INFOTECH LLP	● Significant slowdown in network performance ● Total/partial disruption of E-mail communication services ● Severe drain on network resources. ● Significant reduction in access to critical network services. ● Increased possibility of virus/worm infection
5. Identity Theft Attack **Large scale spoofing** ● Spoofing is an attack aimed at 'Identity theft' ● Spoofing is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage	● High profile officials in BESSEGGEN	● Increased possibility of identity theft and root privileges compromise leading to penetration into sensitive IT systems and Databases ● Loss of sensitive data, monetary loss and loss of image.
● **Social Engineering** Art of manipulating people into performing disclosure actions or divulging confidential information	● Individual users such as senior executives & officials.	● Loss of sensitive personal data, monetary loss and loss of image and trust

● **Phishing attacks** Phishing is an attack aimed at stealing the 'sensitive personal data' that can lead to committing online economic frauds. Phishers attempt to fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication ● **Vishing attacks** Vishing is a combination of 'voice' and 'phishing'. It is the practice of using social engineering over the telephone system, most often using features facilitated by Voice over IP (VoIP), to gain access to private personal and financial information from the public for the purpose of financial reward. It exploits the trust in landline telephone services and uses VoIP to trick the user. ● **SMSihing attacks** These are phishing attacks launched through SMS service via Mobile phones.	● Network/System/Database Administrators ● Individual users such as senior executives & officials. ● High profile officials in BESSEGGEN	● Financial frauds ● Loss of user credentials ● Monetary loss to citizens
6. Denial of Service (DoS) attacks and Distributed Denial of Service (DDoS) attacks ▪ DoS is an attempt to make a computer resource unavailable to its intended users ▪ A distributed denial of service attack (DDoS) occurs when multiple compromised computer systems flood the communication link (called bandwidth) or resources of a targeted system. ▪ DDoS attacks are launched through a Botnet which is a	BESSEGGEN INFOTECH LLP ● Routers ● Consumer web portal ● Switches ● WLC's	● Total/partial disruption of services for prolonged periods ● Failed/aborted missions ● Possible damage to life and/or property ● Total/partial disruption of services for prolonged periods ● Monetary loss, damage to reputation, loss of image etc.

network of compromised computer systems called 'Bots'. ▪ Reflection based Distributed Denial of Service (RDDoS) Attack		
7. Domain Name Server (DNS) attacks ● DNS Hijacking refers to modification of DNS records with the intention of redirecting the victim to malicious domains/IPs. ● NXDOMAIN attacks are performed by flooding DNS servers with queries for invalid or non-existent domains therefore eating up the valuable resources and polluting DNS server cache with NXDOMAIN results. ● DNS Cache poisoning involves corrupting the DNS server's cache with fake values causing the name server to return incorrect results. This may result in traffic being diverted to the malicious systems.	● BESSEGGEN web portal ● BESSEGGEN network routers ● Internet usage at BESSEGGEN / Customers	● Total/partial disruption of '.in' registry services ● Possible damage of/inaccessibility to domain registry database or resolution services ● Illegal diversion of Internet and mail traffic to some other countries ● Total/partial disruption of internet traffic nationally/internationally ● Total/partial breakdown of on-line economic activities ● Monetary loss, damage to reputation, loss of image etc.
8. Application-Level Attacks Exploitation of inherent vulnerabilities in the code of application software such as web/mail/databases	● Business and O&M Applications	● Data manipulation which may result in huge economic fallouts including monetary as well as business loss ● Disruption of services ● Loss of sensitive data and loss of image & trust

9. Attacks on Trusted infrastructure Trust infrastructure components such as Digital certificates and cryptographic keys are used at various levels of cyber space ranging from products, applications and networks. Compromise of infrastructure of Certifying authority or key management systems of product/application owners may result in breakdown of trust of users and misuse of authentication mechanisms (i) Denial of Service attacks (ii) Rogue certificates	● VPN Servers ● SSL Servers ● Authentication infrastructures ● Secure Communication Protocols and systems ● Public Key Infrastructure	● Blocking of handshaking resulting in disruption of financial and authentication services ● Large scale Man-in-the-middle attacks resulting in disclosure sensitive data and user information ● Redirection of users to fake websites with dubious authentication ● Signing malicious code to make it appear as legitimate ● Large scale cyber espionage
10. Compound attacks ● By combining different attack methods, hackers could launch an even more destructive attack. The Compound attacks magnify the destructiveness of a physical attack by launching coordinated cyber-attack.	● Business Application ● NMS ● Portal	● Total/partial disruption of services/activities ● Significant slowdown in disaster/emergency response capabilities that can magnify the impact of a physical attack ● Huge economic fallouts including monetary as well as business loss ● Damage to reputation, loss of image etc.
11. Router level attacks ● Routers are the traffic controllers of the Internet and Intranet to ensure the flow of information (data packets) from source to destination. Routing disruption could lead to massive routing errors resulting in disruption of Internet communication	● Sensitive and Critical Information Infrastructure. ● Gateway routers ● Routers of BESSEGGEN, corporate networks etc. ● ADSL/Wi-Fi Routers used by small offices/home users ● Business applications ● Routers at client site	● Total/partial disruption of internet traffic nationally/internationally ● Total/partial breakdown of online economic activities ● Huge economic fallouts including monetary as well as business loss ● Total/partial breakdown of online economic activities

● **Border Gateway Protocol (BGP) attacks** BGP is a primary protocol used to route traffic between different networks, known as Autonomous Systems (AS), across the Internet. It works by exchanging routing and reachability information among different AS. BGP route manipulation: A router in the network announces a spurious route which upon propagating prevents traffic from reaching the intended destination. This can occur due to router misconfigurations (intentional / unintentional) or compromised router. BGP route hijacking (prefix hijacking): The attacker announces the more specific prefixes of the intended target network to reroute traffic through itself. Once successful, the hijacker could then perform Man-in-the-middle attacks, eavesdropping, modifying or blocking the traffic. BGP Denial of Service (DoS): A compromised router in the network sends unexpected or undesirable BGP traffic to another router. The target router stops processing valid BGP traffic due to excessive resource consumption.		● Huge economic fallouts including monetary as well as business loss ● Possession of Router's control by attackers and re-redirection to malicious websites through rogue DNS Server entries for conducting malicious activities ● Illegal diversion of internet / intranet traffic ● Monetary loss, damage to reputation, loss of image, etc. ● Total/partial breakdown of online activities. ● Loss of sensitive personal data. ● Total/partial disruption of internet traffic

12. Cyber Espionage and Advanced Persistent Threats Targeted attack resulting in compromise of computer systems through social engineering techniques and specially crafted malware. The data from the compromised system is siphoned off to remote locations. Common channel of attacks includes spoofed/compromised email accounts of key officials, social networking sites and drive-by-download through watering hole websites.	● BESSEGGEN Computer systems and Network	● Disclosure of sensitive information ● Data theft ● Compromise of critical internal systems
13. Client-Side attacks Attacks on user side vulnerable software applications like MS office applications, Adobe Acrobat reader, JAVA, Browsers Plugins, etc. usually via Sophisticated attack tool kits with various exploits available for compromising/rooting the client system.	● Individual users.	● Data Leakage. ● User system as bot or launch pad for launching further attacks.
14. Attacks using Social Network Sites (SNS) Attacks targeting social networking platforms for various malicious activities such as identity theft, fake social accounts, fake news, misinformation, command & control for Botnets, drive-by-download etc.	● Individual users such as senior executives & officials, celebrities	● Loss of sensitive personal data, loss of image and trust. ● Malware distribution.
15. Vendor / Supply chain risk / attack Attacker infiltrates through an outside partner or provider with access to organizations system / data or modifying the product	● BESSEGGEN as corporate	● Disclosure of sensitive information ● Cyber espionage

deliberately with malicious backdoor. ex. Includes Trojan, hardware manipulation and software supply chain		● Attack on critical infrastructure ● Advanced persistent threats
16. Threats due to Emerging Technologies (Iot, Big Data, Artificial Intelligence) Attacker can make use of the system / data / Compute power / components deliberately with malicious backdoor to attack organizational network	● BESSEGGEN as corporate	● Cyber espionage ● Attack on critical infrastructure ● Disclosure of sensitive information

4. Building Cyber Security Capabilities

4.1 Cyber Security Must Haves

BESSEGGEN has developed a culture of cyber security among them in every aspect of functionality. The Cyber Security Must Haves indicates the basic cyber security fundamentals applicable to BESSEGGEN. By deploying these Must Haves, organizations can defend against the most common form of basic cyber-attacks originating from the Internet. The defenses identified through these must have to deal with reducing the initial attack surface.

These Baseline requirements for cyber security helps BESSEGGEN to select as a starting point for implementing cyber security programs and provides an opportunity to benchmark against a minimum set of cyber security controls. Minimum set of cyber security controls can be used by BESSEGGEN as a starting point for the journey towards implementing a full-fledged cyber security framework. The figure given below illustrates the 5 Cyber Security Must Haves:

Figure: Cyber Security Must Haves

- **Inventory of Devices and Software**

  Inventory of Hardware & Software: BESSEGGEN has created and managed inventory of all hardware and software available on the organization's network. The inventory of devices and software will help in identifying what needs to be secured and also help in ensuring proper management of the access control. BESSEGGEN have to maintain the Asset register for the assets which are in the Organization or the third party. The comprehensive Information Asset Register shall be maintained by the BESSEGGEN IT Department. There shall be Information asset register, the ownership of these Asset Registers shall rest with the respective concerned Department Head.

- **Controlled Use of Administrative Privileges**

  The administrative privileges are restricted on software, operating systems, devices and networks. Access to the resources provided on a need-to-know basis. All logs of administrative privileges are being monitored periodically on a sample basis.

- **Secure Configurations for Hardware and Software**

  BESSEGGEN has implemented secure configuration of hardware and software installed within the network. Patching and updates of firmware and software are in place. Secure configuration control reduces the attack surface by only operating services and functionalities. All the changes go through a Change management process implemented by BESSEGGEN for any required change in the configuration of hardware & software. Secure configuration of hardware & software will shrink the attack surface by securing the access to assets in the network by only allowing what is necessary and removing/blocking unnecessary ports & services.

- **Malware Defense**

  Malwares are one of the biggest nuisances. Multiple solutions to detect and counter spreading & execution of malware should be deployed in organizations' networks. Controls for malicious code prevention & detection can be deployed at perimeter security devices, email servers, end-point devices, laptops and servers. Malware is a broad term that refers to a variety of malicious programs. Malware programs contain some lines of code that execute the desired task of the attacker when interacting with the victim system. Some malware does not require any user interaction. They work as a standalone program. Commonly malwares are adware, bots, bugs, spyware, ransomware, rootkits, keyloggers, Trojan horses, viruses, and worms. BESSEGGEN has implemented enough controls on the perimeter to safeguard from malwares. BESSEGGEN has implemented technologies like ATP (Advanced threat protection), Sandbox, Intrusion Prevention (IPS), Application control etc.

- **Vulnerability and Patch Management**

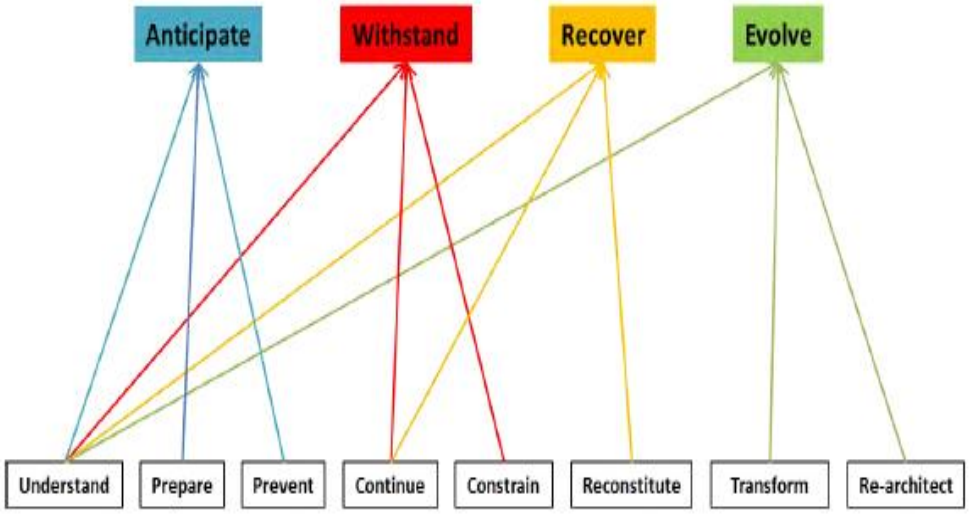
  Based on the cyber security alerts, disclosures of vulnerabilities & released exploits, BESSEGGEN implements vulnerability and patch management program for ICT environment and takes the suitable action as required. In addition to above, procurement of Network/ IT equipment is from Trusted Vendors only in accordance with CEA/MoP Trusted Vendor Guidelines.

4.2 Cyber Resilience

Cyber resilience is defined as the ability of an organization or business process to anticipate, withstand cyber-attacks and the capability to contain, recover rapidly and evolve to improved capabilities from any disruptive impact of such cyber-attacks. Resilience can be defined in various ways depending upon the area of application or the type of sector under consideration. Common aspects include preparing for, preventing, or otherwise resisting an adverse event; absorbing, withstanding, or maintaining essential functions in the face of the event; recovering from the event; and adapting to (changing processes, systems, or training based on) the event, its consequences, and its implications for the future

4.2.1 Principles of resilience

1. Anticipation, Protection and detection, including vulnerabilities, of cyber infrastructure & systems in organizations to understand, prepare and prevent cyber-attacks.
2. Withstanding and Localize containment of crisis and isolate trusted systems from untrusted systems to continue essential business operations in the event of cyber-attacks.
3. Dynamic & reliable automated recovery of crisis impacted systems to restore maximum continuity and operations by following predefined resilience rating or degree of confidence for each of system components and evolving to improved capabilities by making changes to existing processes or workflows and updating / modifying the threat model. At a conceptual level, the goals and principles can be shown as in the following diagram:



Cyber resiliency goals and principles

4.2.2 Protection and resilience of Organizations' infrastructure

Organization needs to work towards following to build cyber resiliency:

- Identification of key information and technology and Network assets that support the services of that organization
- Implementation of controls to protect those assets from cyber attack
- Implementation of controls to sustain the ability of those assets to operate under disruptive events and recover rapidly from disruption.

- Development of processes to maintain and repeatedly carry out the protection and recovery activities.
- Development of appropriate measures to drive these activities.
- To develop a plan for protection of organization Infrastructure and its integration with business plans and implement such plans. The plans shall include establishing mechanisms for secure information flow (while in process, handling, storage & transit), guidelines and standards, cyber crisis management plan, proactive security posture assessment and forensically enabled information infrastructure.
- To closely interact with the 24x7 National Critical Information Infrastructure Protection Centre (NCIIPC) by providing it the necessary and timely information.
- To ensure identification, prioritization, assessment, remediation, and protection of organization infrastructure and key resources based on the plan for organization Information Infrastructure.
- To ensure compliance to global security best practices, business continuity management and cyber crisis management plan by all entities within the domain of organization/ department, to reduce the risk of disruption and improve the security posture.

4.2.3 Cyber Resilience components & control matrix

Building cyber resilience begins with effective protection of five key components within any system (i.e. key information and technology assets) – the user identity, system processes, data and hardware & software platform along with network of connections between systems. These components are defined as follows:

Identity: The representation of a user or organization within a system.
System Processes: The actual programs running within the system that may be executing on behalf of the user or at root level within the operating system.

Hardware & Software Platform: Typically, this will be a physical manifestation of the system as hardware and software, but it may also be a virtualized platform residing on a cloud infrastructure or in the data center. The information security management system (ISMS) Risk Assessment Methodology and Procedures & controls based on ISO /IEC 27001 may be referred to at http://meity.gov.in/content/.
Data: The data either physically stored or held in memory within the system.

Network: The communication link between systems and all the protocols for establishing and securing that communication. Commonly, the gateways on the network act as enforced barriers to communication that may act as a boundary or filter to prevent some communications while enabling others such as network firewalls.

Achieving cyber resilience is about understanding the sensitivity and interdependency of critical assets and selecting appropriate technical controls for protection, detection, containment and recovery from cyber disruptive activities and assigning resilience rating for each system component by the organization depending on the services provided by them and their respective Service level Agreements (SLA). A matrix, showing relation between each of the components within system and their mapping to these controls, may be referred at **“Appendix V”**

Cyber Security Exercises
Cyber security mock exercises are to be conducted periodically to enable organizations under nodal Ministry of Electronics & Information Technology (CERT-IN) to assess their preparedness and resilience

in dealing with cyber crises. Cyber security exercises conducted with the help of CERT-In or sectoral CERT or state CERT or Ministry of Electronics & Information Technology as may be applicable shall help organizations to learn how to anticipate threats, protect their infrastructure and platform, detect incidents, withstand impacts, recover from attacks and improve their security posture.

5. CRITICAL INFORMATION INFRASTRUCTURE (CII)

As per NCIIPC, the following procedure should be adopted for identification of CII:

Relevant Acts and Rules

1. As per IT Act 2000 (amended 2008), Critical Information Infrastructure (CII) means 'Computer Resource, the incapacitation or destruction of which, shall have debilitating impact on National Security, Economy, Public Health or Safety'.

2. Section 70 of the IT Act 2000 lays down that the appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of CII, to be a 'Protected System'.

3. Gazette Notification G.S.R 18(E) dated 16 Jan 2014 designates the National Critical Information Infrastructure Protection Centre (NCIIPC), an organization under the National Technical Research Organization (NTRO), as the national nodal agency in respect of Critical Information Infrastructure Protection.

4. Gazette Notification G.S.R. 19(E) dated 16 Jan 2014 lays down the Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules, 2013.

Key sections of the Rules are:

(a) Section 2(e) of the Rules lays down that "Critical Sector" means sectors, which are critical to the nation and whose incapacitation or destruction will have a debilitating impact on national security, economy, public health or safety.

(b) Section 4(3) of the Rules mandates the identification of all critical information infrastructure elements for approval by the appropriate Government for notifying the same.

(c) Section 4(5) of the Rules mandates that the basic responsibility for protecting critical information infrastructure systems shall lie with the agency running that critical information infrastructure.

(d) Section 5 of the Rules lay down the Manner of Performing Functions and Duties and spell out the role and responsibilities of NCIIPC. It also lays down a mechanism for prioritization of actions against threats or vulnerabilities.

5. CII is very likely to be targeted by an attacker so as to disrupt or compromise an IT and Network-enabled capability, service or process of national importance. These capabilities and services are delivered by organizations and enterprises in the critical sectors through various Business and/or Industrial Processes, which run on the underlying Information Technology (IT) and Operation Technology (OT) systems.

6. In order to have a consistent approach for identification of CII within and across all the Critical Sectors, a set of generic guidelines are enumerated in succeeding paras.

Identification and Assessment of CII

7. Assess the criticality of the Functions and Services provided by the Organization / Entity and the magnitude of impact on National Security, National Economy, Public Health or Public Safety in case of incapacitation / destruction of its ICT infrastructure based on the following parameters: -

(a) Impact on Customers, Business & Government functions based on: -
  (i) Value of all types of Transactions per day.
  (ii) Total number of Transactions per day.
  (iii) Number of connected Devices and Network size.
  (iv) Number of Customers of different categories.

(b) Timeframe (hours / days / weeks) after which the impact level of non-availability of the ICT infrastructure will be very significant for National Security, National Economy, Public Health, Public Safety, Customers, Business and Government (shorter time frame indicates more critical).

(c) Geographical or Environmental impact, if any, of incapacitation / destruction of the underlying ICT infrastructure (area, city, district, state, region, nation-wide or even across international boundary).

(d) Level of Dependency to include: -
  (i) Cascading impact of non-availability of functions and services due to incapacitation or destruction of the underlying ICT infrastructure and degradation on other critical sectors / subsectors.
  (ii) Dependence of essential functions and services on other critical sectors / sub-sectors.

8. If the above assessment indicates that functions and services of the organization / entity have a significant impact nationally, there is a need to evaluate various Business and/or Industrial Processes of the organization / entity from the point of view of identifying those computer resources, the incapacitation or destruction of which may have a debilitating impact on National Security, National Economy, Public Health or Public Safety. Following parameters can be considered for identification of critical business and/ or industrial processes of the organization: -

(a) Size & Economic Value of the Business /Industrial Process based on: -
  (i) Value of all types of Transactions processed per day.
  (ii) Total number of Transactions processed per day.
  (iii) Number of connected Devices and Network size of the Business /Industrial Process.
  (iv) Number of Customers of different categories serviced.

(b) Criticality of the Business Process and estimated magnitude of impact on National Security, National Economy, Public Health, Public Safety, Customers, Business and Government in case of incapacitation/ destruction of the underlying ICT infrastructure.

(c) Timeframe (hours / days / weeks) after which the impact level of non-availability of the Business /Industrial Process will be very significant for National Security, National Economy, Public Health, Public Safety, Customers, Business and Government (shorter time frame indicates more critical).

(d) Level of Dependency.
  (i) Impact of non-availability of Business /Industrial Process due to incapacitation or destruction of the underlying ICT infrastructure and degradation on other Critical Sectors.
  (ii) Dependence of the Business / Industrial Process on other critical sectors/sub sectors.

9. Based on expert judgment and estimation of the above parameters, various Business and/or Industrial Processes are then grouped as critical or non-critical. NCIIPC may be consulted for any clarification in the CII identification process. Consequently, the underlying computer and network resources of critical processes along with their interconnected dependencies will be categorized to be CII.

10. The appropriate government may, in consultation with NCIIPC, declare the identified CII of the concerned organization through an 'Office Memorandum'. If needed, it may further choose to declare any computer resource which directly or indirectly affects the facility of CII, to be a 'Protected System' through notification in the Official Gazette.

11. For Protected Systems as well as the declared CIIs, 'Rules for the Information Security Practices and Procedures for Protected System', promulgated vide Gazette Notification dated 22 May 2018 (Regd No D.L.- 33004/99), shall be suitably adapted by the Information Security Steering Committee (ISSC) of the organization.

6. Botnet Cleaning and Malware Analysis Centre (Cyber Swachhta Kendra)

6.1 Introduction:

The "**Cyber Swachhta Kendra "** (Botnet Cleaning and Malware Analysis Centre) is a part of the Government of India's Digital India initiative under the Ministry of Electronics and Information Technology (MeitY) to create a secure cyberspace by detecting botnet infections in India and to notify, enable cleaning and securing systems of end users so as to prevent further infections. The Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) is set up in accordance with the objectives of the "National Cyber Security Policy", which envisages creating a secure cyber ecosystem in the country. This center operates in close coordination and collaboration with Internet Service Providers and Product/Antivirus companies. This website provides information and tools to users to secure their systems/devices. This center is being operated by the Indian Computer Emergency Response Team (CERT-In) under provisions of Section 70B of the Information Technology Act, 2000.
The Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) is a part of the Indian Computer Emergency Response Team (CERT-In). It has been set up for analyzing BOTs/malware characteristics and providing information and enabling citizens for removal of BOTs/malware. In addition, Cyber Swachhta Kendra (CSK) will strive to create awareness among citizens to secure their data, computers, mobile phones and devices such as home routers.

The Cyber Swachhta Kendra (CSK) collaborates with industry and academia to detect systems infected by bots. It also collaborates with the Internet Service Providers to notify the end users regarding infection of their system and providing them assistance to clean their systems. The center will also enhance awareness of common users regarding botnets, malware infections and measures to be taken to prevent malware infections and secure their computers / systems / devices.

Its mission is to enhance the cyber security of Digital India's IT infrastructure by providing information on botnet/malware threats and suggesting remedial measures.

6.2 Cyber Swachhta Kendra (CSK) in Insurance Sector:

It has been set up for analyzing BOTS/Malware characteristics and providing information and enabling organizations to disinfect the host IP infected with Botnet/Malware and host IP running vulnerable services within the organization. CSK collaborates with industry and academia to detect and notify about the infected systems and provide assistance to clean the systems. it is imperative that all Insurance sector utilities should be on-boarded on CSK so that computer systems may become cyber secure for smooth functioning of the connected equipment and related business function. The utilities on-boarding CSK are required to quickly respond to the advisories/ suggestions and take immediate remedial measures and respond back to the CSK team. The utilities may also be advised to coordinate

and closely work with respective Sectoral CERTs in Insurance for better management of cyber security issues.

6.3 Brief on CSK functioning:

CSK/CERT-In will be providing the following reports/feeds on daily basis:
1. Botnet/Malware infected hosts
2. Hosts running with vulnerable services.

6.4 Preparation and expected operations at organization end:

1. for malware reports – trace the end system and clean the same – take backup before cleanup in case of critical systems
2. For vulnerable systems – assess vulnerabilities and plug the same
3. Maintain logs of relevant systems/network and preserve, for further analysis.
4. Examine the reports sent by “Cyber Swachhta Kendra” and provide feedback at regular interval of time, detailing the usefulness of information.

For further clarifications/queries, one may write to Cyber Swachhta Kendra at "csk@cert-in.org.in".

7. THREAT IDENTIFICATION AND ANALYSIS

A key part of the threat analysis is determining the threat actions associated with each threat-source. These factors govern the probability and impact of a given threat-source to exploit vulnerabilities. A threat is the potential for a particular threat-source to successfully exercise a particular vulnerability. A vulnerability is a weakness that can be accidentally triggered or intentionally exploited. A threat-source does not present a risk when there is no vulnerability that can be exercised.

Threat Types	Motivation For Threat	Threat Action
Intentional and Unintentional Human Threats		
Hacker, Cracker	● Challenge ● Ego rebellion ● Destruction of information	● Hacking ● Social Engineering ● System Intrusion, breaking ● Unauthorized System Access ● Computer crime (e.g., cyber stalking)
Computer Criminal	● Illegal information disclosure ● Monetary gain ● Unauthorized data alteration	● Fraudulent Act (e.g. replay, impersonation, interception etc.) ● Information bribery ● Spoofing ● System intrusion
Terrorist	● Blackmail ● Destruction ● Exploitation Revenge	● Bomb/Terrorism ● Information warfare ● System attack (e.g., distributed denial of service) ● System penetration

Threat Types	Motivation For Threat	Threat Action
		● System tampering
Industrial Espionage (companies, foreign governments, other government interests)	● Competitive advantage ● Economic espionage	● Economic exploitation ● Information theft ● Intrusion on personal privacy ● Social engineering ● System penetration ● Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Poorly Trained Employee	● Unintentional errors and omissions (e.g., data entry error, programming error)	● Incorrect information ● Computer abuse ● Input of falsified, corrupted data ● Malicious code (e.g., virus, logic bomb, Trojan horse)
Disgruntled Employee	● Curiosity ● Ego ● Intelligence ● Monetary gain ● Revenge ● Unintentional errors and omissions (e.g., data entry error, programming error)	● Assault on an employee ● Blackmail ● Browsing of proprietary information ● Computer abuse ● Fraud and theft ● Information bribery ● Input of falsified, corrupted data ● Interception ● Malicious code (e.g., virus, logic bomb, Trojan horse) ● Sale of personal information ● System bugs ● System intrusion ● Unauthorized system access sabotage
Negligent Employee	● Curiosity ● Unintentional errors and omissions (e.g., data entry error, programming error)	● Browsing of proprietary information ● Computer abuse ● Input of falsified, corrupted data ● Malicious code (e.g., virus, logic bomb, Trojan horse) ● Unauthorized system access sabotage
Dishonest Employee	● Curiosity ● Ego ● Intelligence ● Monetary gain ● Revenge ● Unintentional errors and omissions (e.g., data entry error, programming error)	● Assault on an employee ● Blackmail ● Browsing of proprietary information ● Computer abuse ● Fraud and theft ● Information bribery ● Input of falsified, corrupted data ● Interception ● Malicious code (e.g., virus, logic bomb, Trojan horse) ● Sale of personal information ● System bugs ● System intrusion

Threat Types	Motivation For Threat	Threat Action
		● System Unauthorized system access sabotage
Terminated Employee	● Ego ● Intelligence ● Monetary gain ● Revenge	● Assault on an employee ● Blackmail ● Browsing of proprietary information ● Computer abuse ● Fraud and theft ● Information bribery ● Input of falsified, corrupted data ● Interception ● Malicious code (e.g., virus, logic bomb, Trojan horse) ● Sale of personal information ● System bugs ● System intrusion ● System Unauthorized system access sabotage
Hardware Failures	N/A	● Routine wear and tear ● Human carelessness
Software Failures	N/A	● Software defect ● License expiration
Telecommunication Outages	N/A	● Extreme weather conditions ● Telecom provider configuration issues ● Telecom provider hardware issues

For each identified vulnerability, the probability that a threat-source would be able to exploit it, may be determined based on the using the criteria presented in the Tables below-

Likelihood Rating	Threat Description
High (1.0)	The threat-source is in place, highly motivated and sufficiently capable. There are NO counter measures to prevent the threat from being exploited.
Moderate (0.5)	The threat-source exists, but countermeasures are in place that will impede successful exercise of the vulnerability, or the threat-source lacks motivation or is only marginally capable of carrying out the threat.
Low (0.1)	The threat-source lacks motivation or capability, security controls are in place to prevent successful exploitation of the threat, or significantly impede threat capability.

- BESSEGGEN CISO would analyze and compile the information/data regarding Threats and furnish the same to Cert-IN Depth within the Timeline for reporting given in this Document, i.e., within 24 hours of cyber threats and in the Quarterly report for all aspects within 1st week of next month.

8. CYBER SECURITY MOCK DRILLS AND INCIDENT PREVENTION

8.1 Cyber Security Mock Drills

Objective

- To enable BESSEGGEN to assess their ability and preparedness to deal with cyber crisis situations.
- To enable BESSEGGEN to secure their IT networks & systems and resist cyber-attacks by way of effective implementation of Information Security Management System (ISMS) and Sectoral Cyber Crisis Management Plans
- To detect cyber-attacks and determine appropriate response, mitigation and recovery actions

Cyber security mock drills are to be conducted annually by CERT-In empaneled auditors to enable BESSEGGEN to assess their preparedness and resilience in dealing with cyber crisis. These drills shall help BESSEGGEN to learn how to anticipate threats, protect their infrastructure and platform, detect incidents, withstand impacts, recover from attacks and improve their security posture.

Cyber security drill is a confidence building and learning exercise based on simulated cyber security incident scenarios that resemble occurrence of a cyber security crisis. Cyber Security drills are intended to be a collaborative and coordinated exercise between CERT-In and organizations. A proper record of the mock drills is maintained by BESSEGGEN.

In addition, cyber security mock drills would also help in

- Promoting cross sector and critical infrastructure relationships / partnerships
- Identifying preparedness gaps
- Addressing gaps by improving processes, communication and information sharing
- Enhancing response to cyber incidents Reducing cyber risk
- Create awareness among BESSEGGEN employees & CERT-In besides imparting training and education for responding to cyber security incidents

After a period of maturity in the cyber security drills at participants' end, BESSEGGEN will carry out mock drills on their own with necessary guidance from CERT-In, as may be required. BESSEGGEN may approach CERT-In for conducting regular mock drills as per the guidance on CERT-In.
BESSEGGEN CISOs will furnish the report on Mock drill within the Timeline for reporting given in this Document, i.e., within 07 days of Mock drill and also in the Quarterly report for all aspects within 1st week of next month

8.2 Incident Prevention

Incident Prevention and Precautionary Measures
BESSEGGEN has implemented the following precautionary measures to prevent cyber security incidents:

- **Nomination of Cyber Crisis Management Group (CMG)**

A team of senior officers of the organization **(Annexure A**) nominated as CMG having the main functions as-

- Declaration of the disaster or Emergency after consultation with CISO
- Periodic status review of corrective & preventive action decided after an event.

- **Nomination of Chief Information Security Officers (CISO)**

BESSEGGEN has nominated a Chief Information Security Officer (CISO) to coordinate the security related issues/implementation within the organization as well as coordination and interface with CERT-In and Intelligence Bureau. The main function of CISO is:

- To create secure cyber ecosystem
- To implement cyber security measures as per ISO 27001 framework and coordinate cyber security related issues
- Define contingency plan / disaster recovery plan
- Damage Assessment in case of a disaster
- Declaration of the disaster or Emergency in absence of CMG Head
- Communication to the CMG Head
- Pre & Post Coordination with various teams i.e. Recovery Team, Security & safety team, Administrative Team, Infrastructure Team
- Monitoring the recovery process and communicate the same to CMG Head
- Conduct periodic CMG training and deployment in the event of a disruptive situation requiring plan activation
- Conduct periodic mock drills
- Contact fire station
- Prepare Recovery Test Plan etc.

▪ **Information Security Policy and Implementation of Best Practices**

BESSEGGEN has formulated Information Security Policy, identified and implemented appropriate information security management practices keeping in view their business needs.
BESSEGGEN has implemented **Information Security Management System (ISMS)** Best Practices as per **ISO/IEC 27001**

▪ **Business Continuity Plan (BCP)**

Define Contingency Plan (Business Continuity Plan) to counteract interruptions to business operations/activities and protect critical operations/business processes from effect of major disaster.
Refer BESSEGGEN Information Security Policy
Refer BESSEGGEN BCP DR Procedure

▪ **Disaster Recovery Plan (DRP)**

Establish Disaster Recovery (DR) Plans with adequate redundancy to take over the operation in case of the need.
Refer BESSEGGEN BCP DR Procedure

▪ **Security of Information Infrastructure and Network**

BESSEGGEN has secured the entire IT infrastructure and network by implementing appropriate hardening measures. Guidelines on "Important Security Controls for Effective Cyber Security and Continuous Security Policy Compliance" are given in **Appendix I.**

- Security devices are installed at all levels. Servers, Local Area Network (LAN) and Wide Area Network (WAN) infrastructure should be secured by installing appropriate perimeter security devices such as firewalls, Intrusion Prevention System and anti-virus system. Configuration of these security devices are checked at the time of installation as well as at the time of significant changes for the needed functionalities and security features.
- The security mechanism includes appropriate devices and methods to log and monitor the events to detect network scanning, probing, reconnaissance and flooding attempts on the Network and IT

infrastructure. These attempts should be regularly reviewed and analyzed for initiating necessary preventive measures

- The remote monitoring and maintenance of the security devices are strictly restricted to authorized persons only
- The software at network, system and application level are regularly upgraded by applying/installing upgrades and updates

Application Security Best practices includes:

- Implementation of application security controls for both web and mobile applications.
- Secure application development is enhanced by applying security checkpoints and techniques at early stages of development as well as throughout the software development life cycle (SDLC). Special emphasis applied to the coding phase of development. Security mechanisms include, threat modeling, risk analysis, static analysis, digital signature, among others.
- Comprehensive security assessments of application performed before final deployment of application, and after any major changes or upgrades to the system.
- Application design and development compliance to policy and regulation as applicable.

Network Traffic Scanning

The network traffic scanning technique provides visibility into the state of the network and identifies deviations from baselines that may indicate abnormal or suspicious behavior. The traffic patterns provide leads on the targeted ports such as 80,25,23 which gives leads to the attack targeted on the services like 'http', 'smtp', 'ftp' or spread of malicious code like 'Bots'. For example, if it is observed that suddenly there is a rise of traffic on the port 25, associated with email service; this may indicate that e-mail-based worms are spreading at a high speed. A sudden traffic rise on the IRC ports may indicate a surge in the 'Botnet activity'. The network traffic flows thus give the exact portrait of the communications happening on the network, irrespective of their state whether a normal or an anomaly. Majority of attacks such as Distributed Denial of Service (DDoS), Worm, Spyware, Botnet detection, malicious scan of any nature etc. at the organization level could thus be detected by analyzing network flow-data traffic. Industry solutions are available to collect and analyze network flow traffic on the gateway routers and switches. Network flow data DO NOT contain any content data and is totally non-intrusive on the network. The organizations may use network flow data for security analysis to detect attacks onto the networks

8.3 Implementation of Security Guidelines issued by Ministry of Home Affairs, Intelligence Bureau, respective Ministries and agencies like IRDA, CERT-IN, MEITY

BESSEGGEN has implemented Security Guidelines and advisories both with respect to cyber and physical security issued by the Ministry of Home Affairs, CERT-In, CERT-D, IRDA, MEITY and other agencies from time to time.

8.4 Manpower Engagement in Cyber Security activities of organization

(a) Screening and Background check

Background verification checks on all employees engaged in implementing and monitoring cyber security and cyber crisis management plan, contractors, and third-party users carried out in accordance

with relevant laws, regulations and ethics, and proportional to the requirements of task and responsibilities, the classification of the information to be accessed, and the perceived risks.
Verification checks take into account all relevant privacy, protection of personal data and/or employment-based legislation, and should, where permitted, include the following:

a) Availability of satisfactory character references, e.g. one business and one personal
b) A check (for completeness and accuracy) of the applicant's curriculum vitae
c) Confirmation of claimed academic and professional qualifications
d) independent identity check (passport or similar document)
e) More detailed checks, such as credit checks or checks of criminal records

Information security management practices based on IRDA and ISO 27001 standard provide guidance with regard to screening and background checks in respect of employees and other personnel. BESSEGGEN consider following best practices.

(b) Roles and responsibilities

Security roles and responsibilities of employees, contractors and third-party users defined and documented in accordance with the BESSEGGEN information security policy. Security roles and responsibilities include the requirement to:

a) Implement and act in accordance with the BESSEGGEN information security policies.
b) Protect assets from unauthorized access, disclosure, modification, destruction or interference.
c) Execute particular security processes or activities.
d) Ensure responsibility is assigned to the individual for actions taken.
e) Report security events or potential events or other security risks to the organization.

Security roles and responsibilities defined and clearly communicated to job candidates during the pre-employment process. Job descriptions used to document security roles and responsibilities. Security roles and responsibilities for individuals not engaged via the BESSEGGEN employment process, e.g. engaged via a third-party organization, should also be clearly defined and communicated.

8.5 Assurance Framework

- **3rd Party Audit – BESSEGGEN** undertakes a comprehensive security audit of the entire organization infrastructure including network and applications by independent CERT empaneled auditing organization to discover the gaps with respect to best security practices and take appropriate corrective actions.
- **Internal Audit –** Periodic internal audit conducted twice a year.
- **VAPT –** Vulnerability Assessment and penetration testing conducted for critical organization infrastructure and applications.
- **Internal testing –** Conducted for any change or new purchase of infrastructure and application in respect of hardware, software, network resources, policies and configurations of systems and subsystems are affected.
- **Mock Drill –** Periodic mock drills conducted to assess their preparedness and resilience in dealing with cyber crises. These drills help BESSEGGEN to learn how to anticipate threats, protect their infrastructure and platform, detect incidents, withstand impacts, recover from attacks and improve their security posture.
  - **Internal Mock Drills –** Conducted by creating an environment (E.g. Staging server, Simulation Environment, Cluster etc.).
  - **External Mock Drill –** In coordination with sectoral CERT-In, IRDA, NCIIPC etc.

8.6 Security Training and Awareness

All employees of BESSEGGEN and, where relevant, contractors and third party users receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function Awareness training commence with a formal induction process designed to introduce the BESSEGGEN security policies and expectations before access to information or services is granted Ongoing training include security requirements, legal responsibilities and business controls, as well as training in the correct use of information processing facilities e.g.

- Latest Technologies and threats
- Implementation of Security Policy
- Physical Security Procedures
- Access Control Procedures
- Use of Licensed Software Packages
- Malicious code and Botnets and their prevention
- Reporting and mitigation of incidents (as in the Format at **Annexure-D, E, F and G)**
- Cyber Crisis Management
- Implementation of Information Security Guidelines

The security awareness, education, and training activities are suitable and relevant to the person's role, responsibilities and skills. Training to enhance awareness is intended to allow individuals to recognize information security problems and incidents, and respond according to the needs of their work role and responsibility in event of violation of Standard Information Security guidelines.

8.7 Coordination and incidents information sharing

BESSEGGEN strive to improve coordination and communication with CERT-In, CERT-D, stakeholders, ministry/department and other designated agencies and will share all information pertaining to cyber security incidents (in the Format at Annexure-D, E, F and G) with CERT-In and other designated agencies. Cyber Security exercises conducted by CERT-in may be used as a tool for improving coordination and information sharing.

8.8 Deployment of Information Security Experts

Given the size of the problem and increasing threats of cyber terrorism, there is a need to deploy more experts in this field. A large number of security experts will be working as and when required on emerging vulnerabilities and effective defenses. Periodic training will be provided to information security experts to update the skills with respect to latest technologies/threats and implementations.

8.8.1 IT Security Best Practices Compliance-Levels of Assurance

In order to assist BESSEGGEN to follow a roadmap for progressively achieving compliance and assurance w.r.t. IT security best practices, different levels of assurance have been conceived. Using these levels of assurance and the methods of verification, BESSEGGEN carry out self-assessment with regard to their present status of compliance assurance and declare the same accordingly. It is expected that these levels of assurance will also help BESSEGGEN in improving the maturity of their IT security management system as well as enhancing predictability and proactive nature of their system. Levels of Assurance are as under-

IT Security best practices Compliance and Assurance -'Levels of Assurance'

Sl. No.	Assurance Level	Description	Methods of verification
1.	**Level 1 - Assurance of systematic approach to IT Security**	BESSEGGEN is aware of **Network and IT security best practices and has defined and documented** its IT security plan, policies and procedures covering people, products, technology and processes. Evidence in the form of appropriate references to the IT security plan, policies and procedures exists.	• Questionnaire based check-list • Remote or on-site desktop assessment of check-list response
2.	**Level 2 - Assurance of compliance to IT security best practices**	BESSEGGEN has **implemented Network and IT security best practices** based on clear understanding of risks, threats & vulnerabilities and the **compliance has been verified by** a self-assessment process or by an independent third-party auditing organization.	• Self-assessment report or independent third-party audit report
3.	**Level 3 - Assurance of an adequate IT security posture** **Level 3+ - Assurance of IT security crisis response & ability to resist cyber attacks**	BESSEGGEN has **conducted Network and IT security posture verification** (by way of security testing of its IT infrastructure involving VA/PT, application security testing, code walkthroughs etc.) by an independent third-party auditing organization. BESSEGGEN has **participated in the cyber security drills** to have its IT security crisis response & ability to resist cyber-attacks tested and verified.	• Security testing of IT infrastructure involving VA/PT, application security testing, code walkthroughs etc. and a report is available for the same ● Share Cyber security drills results with CERT-In
4.	**Level 4 - Assurance of proactive IT security monitoring and mitigation of threats and vulnerabilities** **Level 4+ - Assurance of proactive sharing and mitigation of IT security threats & vulnerabilities.** **Level 4+ + - Assurance of proactive prediction of residual IT security risks & attack paths and mitigation**	BESSEGGEN is in process to **implement mechanisms for proactive Network and IT security monitoring and mitigation** of threats and vulnerabilities. These mechanisms allow for technology-based monitoring and analysis of IT security incidents for proactive preventive actions (Ex. IPS/IDS, SIEM, flow-based analysis etc) BESSEGGEN is planning to **implement mechanisms for proactive sharing and mitigation** of IT security threats & vulnerabilities by way of active collaboration with CERT-In, NCIIPC, and ISACs etc. BESSEGGEN is under review to **implement mechanisms for proactive prediction of residual IT security risks & attack paths** and mitigation of IT security threats and vulnerabilities.	Technology based monitoring and analysis (Ex. IPS/ IDS, SIEM, flow-based analysis etc.) evidenced in terms of governance reports and management feedback Collaboration with CERT-In, NCIIPC, ISACs etc. evidence in terms of communication trail Attack path analysis

9. CYBER CRISIS RECOGNITION, MITIGATION AND MANAGEMENT

9.1 Incident Recognition

Recognition of cyber crisis depends on clearly identifying the cyber incidents within the Insurance sector area of operation. The crisis arising out of cyber-attacks may be categorized and prioritized from level 1 to Level 4. Each subsequent level will follow the preceding one. No level other than level **1** will come in isolation.

Table: Cyber security emergency – Levels of concern

Threat Level	Condition
Level 1 Guarded **Scope: Individual Organization**	Perceptible change/variation in system performance and discovery of critical/non critical vulnerabilities/exploits and attacks that can affect normal operation of network and IT systems of individual organization such as: ● Targeted attacks and espionage activities. ● Identity theft (Phishing, spoofing, social engineering etc.) ● Web defacements and Application-level attacks ● Visible signs of malicious programs (viruses/worms/ Bots/malware/Key loggers/Spyware/etc.) ● Detection of new and advanced malware infections ● Attempts for exploitation of zero-day vulnerabilities ● Denial of service attacks (DoS) ● Distributed Denial of Service (DDoS) and Distributed Reflection Denial of Service (DrDoS) ● Hacking of IT systems such as computers systems, Servers (Mail, Web, Database etc.) and Routers ● Spam
Level 2 Elevated **Scope: Multiple Organizations**	Perceptible change/variation in network/ system performance and abnormal surge in network traffic affecting IT infrastructure of multiple organizations simultaneously due to: ● Targeted attacks and espionage ● Large scale infection of viruses/worms/ Bots/malware/ Keyloggers/Spyware for malicious and espionage activities ● Detection of domain specific malwares like "stuxnet" targeting Industrial Control Systems ● Focused attempts of network scanning and penetration ● DDoS attacks and Distributed Reflection Denial of Service (DrDoS) ● Attacks on Domain Name Servers, Mail Servers, Databases, Routers etc ● Large scale web-application attacks like backdooring and defacement. ● Attacks on Trust infrastructure ● Attack on the IT infrastructure of a Critical Information System ● Infection of Networking Devices
Level 3 Heightened **Scope: State/ Multiple States**	Significant breakdown of supplies or services essential to the life of the citizens including but not limited to financial, Government, transport, energy or communication due to focused cyber-attacks on infrastructure of critical sector and Government across a state or multiple states.
Level 4 Serious **Scope: Entire Nation**	Significant/complete breakdown of supplies or services essential to the life of the citizens including but not limited to financial, Government, national defense, transport, energy or communication due to focused cyber-attacks on infrastructure of critical sectors and Government across the nation.

9.2 Nature and Severity of crisis, Authorities responsible and steps for Mitigation

Severity Level of Crisis	Nature of Crisis	Authorities responsible and Steps for mitigation
Level 1 Response **Scope: Individual Organization**	All Attacks	**Responsibility: Affected Organization (BESSEGGEN INFOTECH LLP)** **Steps to be taken by the Affected Organizations** **General** • Notify incidents to respective Administrative Ministry/Department/Sectoral CERT • Monitor and detect anomalous behavior and degradation of service in network and systems • Take all logs (system, application, security, access, error etc.) of affected systems and data therein and keep them separately for analysis and forensics • Forward a copy of ail the logs of affected systems and network devices, suspicious files, data, traffic. trends wherever applicable to CERT-ln/ NTRO • Consult incident reports or vulnerability reports for specific advisories on the suspected behavior as published by CERT-ln and implement those in the affected networks and systems • Segregate networks (LAN/WAN) and perimeter security devices and systems. Check for configuration vis-Prescribed against each attacks mentioned below • Change all user/root/administrator passwords in all systems and network devices • Install updated software patches on Operating System and all other system software running on computer servers and Personal computers in the network
	Web application Attacks	**Mitigation Steps - Specific to nature of cyber-attacks/crisis** If possible, isolate the affected server from the Internet or disable the affected module in application. • Scan all files for web shells or any malicious footprint. • Take a copy of all the logs at the server and perimeter level (IDS/IPS, firewall) and traffic trends • Identify the type of attack and vulnerability exploited • Patch the vulnerability/ issue by modifying insecure code/configuration by secure code/configuration • Report to CERT-ln with web server logs and dump of the vulnerable web application
	Virus/Worm/Spy ware/Botnet Attacks	• Isolate affected systems/network segments from LAN and Internet • Scan all files in the suspected systems, including emails for viruses • Clean the affected systems with the updated antivirus software • Install updated antivirus/anti-spyware on all systems (servers and Personal Computers) • Take a copy of all the logs at the perimeter level (IDS/IPS, firewall) and traffic trends.

	DoS/DDoS/NTP Based DrDoS attacks	• Identify the type of attack such as flooding of particular types of packets/ requests • Allocate traffic to unaffected available network paths, if possible, to continue the services • 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 • Install updated software patches on all the network devices such as Routers, Firewalls, IDS, IPS and switches
	High Energy RF-based DoS Attacks	• Use a network management solution capable of alerting on a degraded signal noise ratio or the increased noise levels in the airwaves • Identify the other devices due to which RF interference occurs and physically remove them • Deploy IPS/IDS to detect rouge access points
	DNS Attacks	• Check for version updates at the DNS server and install latest software patches • Implement spoofing countermeasures • Use Unicast Reverse Path Forwarding to mitigate problems that are caused by malformed or forged IP source addresses • Adopt source IP address verification • Implement DNSSec • Check for effectiveness of filtering rules in the routers, firewall and IPS and reconfigure if required • Check the logs of these devices for source of attack
	Attack attempts/scans on Servers, Routers, Firewall etc.	• Keep watch on phishing sites • Alert customers regarding the known phishing sites • Encourage customers to use anti-phishing enabled browsers • Shutdown phishing sites in coordination with concerned ISP and CERT-In • Deploy hot standby mail servers in physically separated networks and places which can be made operational when the main server is attacked • Disable all other ports and services on mail servers • Enforce strong password policy and encourage users to change passwords periodically
	Phishing Attacks	• Check for signs of infection in computer systems in general • Isolate infected systems from all networks immediately

	Mail Server Attacks Attacks on Critical Infrastructure	• Report the incident to the local IR Team/ CERT-In at the earliest. Consult relevant advisories of CERT-In and follow specific measures suggested therein • Take a forensic image and send to local IR Team/CERT-In • Clean the affected systems with the updated antivirus software • Install updated antivirus/anti-spyware on all systems (servers and Personal Computers) • Examine the vectors of propagation of worms - Removal media, network shares and other sneaker net systems • Examine Critical systems of Industrial process for abnormal functionality • Examine network traffic towards malicious domains/websites/hosts that are identified as Command & Control • Review the security controls and processes to ensure isolation of critical networks from other infrastructure • Follow guidelines mentioned under Section 5.1 in respect of dealing with air gap for isolation of control systems from other networks **On report of the incident, CERT-in would take following supportive actions** • Analyze the information/logs received from affected organizations • Check for latest patches/updates from various sources including vendors (as per format in Annexure-B &C) • Consult the vendors and other sources (as per format in Annexure-B &C) to help the organizations in resolving the problems • Document the vulnerability information and disseminate • In case of phishing attacks, take appropriate action to block the phishing sites by interfacing with concerned organizations, ISPs and international CERTs • In case of Botnet attacks, locate Command & Control server and initiate action to disable the same in coordination with ISPs **On report of the incident, NTRO would take following supportive actions** • Carryout all response activities in respect of Law Enforcement and Security agencies, Space, Atomic Energy, Defense Research, Defense Production and their critical infrastructure

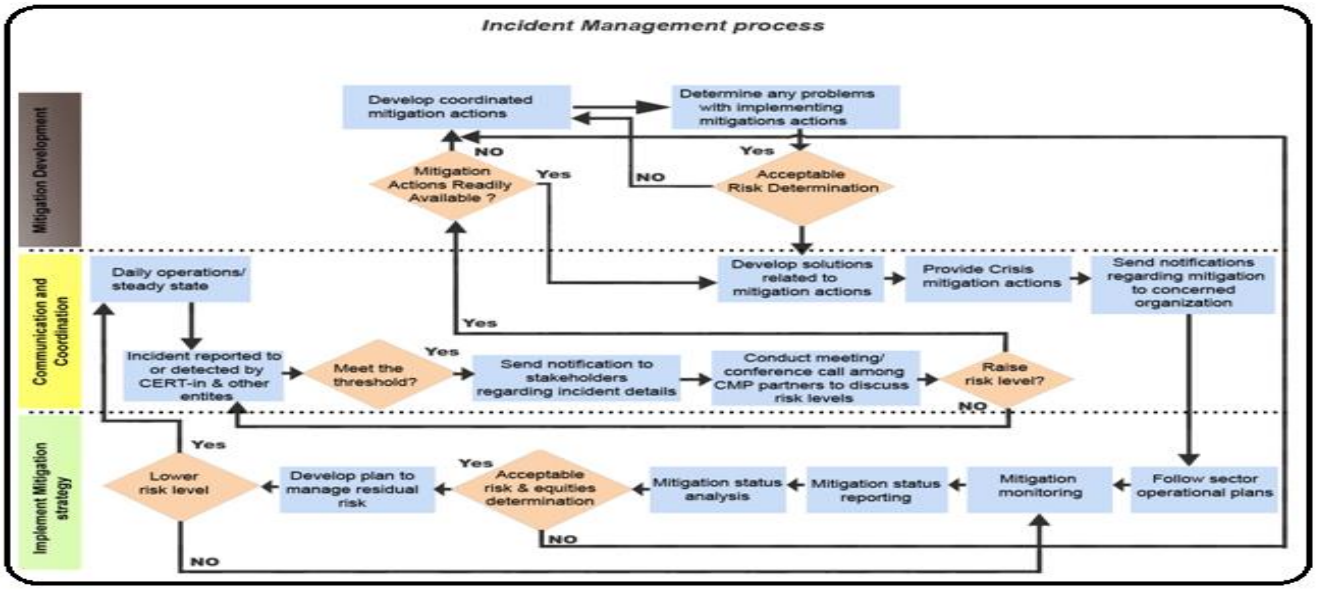
9.3 Planning and Preparation for Incident Handling

Proper and advanced planning ensures the response activities are known, coordinated and systematically carried out. It also facilitates the organization and its functional department concerned to make appropriate and effective decisions in tackling cyber security incidents, and in turn minimizes the possible damages caused. The plan includes strengthening of cyber security protection, making appropriate response to the incident, recovery of the system and other follow up activities. Major activities involved in planning and preparation are as follows:

The following flowchart depicts the broad incident management process and related actions

Sr. No.	Item	Details

1	Cyber Security Incident Handling Plan	Plan for Security Incident Handling – this document takes care of this requirement
2	Reporting Procedure	Design and prepare for the reporting mechanism(s) Publish the report mechanism(s) to all staff
3	Escalation Procedure	Gather contact information for all personnel to be contacted / involved, both internal and external. Publish the escalation procedure to all personnel involved.
4	Security Incident Response Procedure	Prepare security incident response procedure - This document takes care of this requirement. Publish the security incident response procedure to all personnel involved.
5	Training and Education	Provide training to operation and support staff on knowledge in handling security incidents. This can be done as part of the induction process for any recruit in the functional group. Ensure staff are familiar with the incident response process.
6	Incident Monitoring Measure	Monitor and measure various parameters related to incidents and ensure that these are reviewed as part of regular functional group meetings.



9.4 Incident Handling Team Structure

1. Notification Team

An incident can be reported by anyone; however, it is typically reported by one of the following persons/ groups involved in managing and monitoring resources/ services:

- IT Infrastructure [particularly Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) / Router Monitoring Team]
- Network & System Support (NSS) Engineers
- Administration (Physical Security) Team
- Internal / External Audit Team

- Associates

Responsibility

An Associate / team discovering the incident is responsible for communicating the same to the Service Desk Team immediately. Incidents must be assigned the appropriate severity level by the associate / team at the time of reporting the incident.

2. The Service Desk Team

The Service Desk is the place in BESSEGGEN where all security incidents are to be registered by issuing a service ticket. Efficient and effective reaction to security incidents demands a formal method of working that can be supported by software tools.
Incidents that cannot be resolved immediately by the Service Desk are to be assigned to the concerned functional group for that location. A resolution or work-around should be established as quickly as possible in order to restore service to users with minimum disruption to their work. After resolution of the cause of the incident and restoration of service, the incident is closed.
Throughout an incident life cycle, it is important that the service ticket is maintained. Even in cases where the incident is reported by a phone call / email, the ticket must be raised by the service support team member. This allows any member of the support team to provide an up-to-date progress report.

3. Cyber Crisis Detection and Prevention

Cyber crisis detection and prevention is ensured 24 hours a day via the Administration, Human Resource and Information Security staff together with all involved project delivery staff. All these services would cooperate towards the prevention and handling of a cyber crisis. It is the concerned associate on duty who is responsible for alerting the Crisis Management Cell (CMC) of an imminent serious crisis.

4. Level I Incident Resolution Team

Each location of the organization (BESSEGGEN) has an identified list of personnel who will be part of the respective Level I Incident Resolution team.

Responsibilities

- Identify the correctness of the severity level
- Contain, Eradicate and Recover
- Seek necessary resources and support from the corresponding Level II Incident Resolution Team
- Provide regular updates to corresponding Level II Incident Resolution Team and the Crisis Management Cell (CMC) regarding progress of the incident handling process
- Escalate to the corresponding Level II Incident Resolution Team, if unable to resolve within the prescribed time frame/reasonable time frame.

5. Level II Incident Resolution Team

The team involves CISO, his team, Admin, HR functional groups. This team should have full authority to undertake any actions or decisions necessary to contain, eradicate and recover the situation.

Responsibilities

- Provide support to the Level I Incident Resolution Team to facilitate prompt containment, eradication and recovery of the affected entity
- Communicate to all responsible parties and stakeholders like Project Managers and Onsite Account Managers including customer's contact (if warranted in the agreement) and Crisis Management Cell (CMC) within the organization.
- Maintain contact with CERT-In and the respective nodal agency.
- Supervise and coordinate all security incident handlings for the functional group at the particular location.
- Facilitate experience and information sharing on security incidents to CMC, CERT-In and respective nodal agencies.

9.5 Media Management

The media forms a vital link between those responding to crisis situations and the outside world. Besides this, the media also can help in educating all concerns about crisis prevention and preparedness. It is recognized that unbiased and comprehensive media coverage can effectively aid the crisis response & resolution process and also enhance public confidence in the ability of organizations to respond to crises. Accordingly, media management is a crucial issue in terms of pre-incidents as well as post-incident information flow. In order to make best possible use of this vital link, it is necessary that the media is given clear information and regular updates to enable them to perceive the right picture and proportion of the crisis. In this context, it is also necessary for BESSEGGEN responding to cyber security incidents to identify a responsible person of suitable level that has access to correct & updated information and is adequately trained for proper & consistent communication and avoid contradiction at all times.

9.6 Post Incident Activity

After successful mitigation and recovery from incident, the following need to be undertaken (before closing the incident) for future reference/precaution:

- Perform a postmortem analysis of the incident as well as the incident response adopted at the organization and CERT-In level
- Evaluate and perform assessment of the attack from the technical point of view in order to fine-tune and optimize the eradication mechanism
- Document lessons learnt from the incident and prepare incident report, including infrastructure protection improvements from the postmortem process
- Share incident report with CERT-In for future precaution and mitigation of similar attacks
- All critical organizations to implement infrastructure protection improvements resulting from postmortem reviews or other protection improvement mechanisms
- A thorough cyber-Audit by CERT-In empaneled agencies.

Appendix – I

Important Security Controls for Effective Cyber Security and Continuous Security Policy Compliance

"Establishing a prioritized baseline of information security measures and controls that can be continuously monitored through automated mechanisms."

Securing our Nation against cyber-attacks has become one of the highest priorities. To achieve this objective, networks, systems, and the operations teams that support them must vigorously defend against external attacks. Furthermore, for those external attacks that are successful, defenses must be capable of thwarting, detecting, and responding to follow-on attacks on internal networks as attackers spread inside a compromised network.

Security Controls for Effective Cyber Security and Continuous Security Policy Compliance

- Inventory and Control of Hardware Assets
- Inventory and Control of Software Assets
- Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
- Continuous Vulnerability Management
- Controlled Use of Administrative Privileges
- Maintenance, Monitoring and Analysis of Audit Logs
- Email and Web Browser Protections
- Malware Defenses
- Limitation and Control of Network Ports, Protocols, and Services
- Data Recovery Capabilities
- Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- Boundary Defense
- Data Protection
- Controlled Access Based on the Need to Know
- Wireless Access Control
- Account Monitoring and Control
- Implement a security Awareness and Training Program
- Application Software Security
- Incident Response and Management
- Penetration Tests and Red Team Exercises

In general, BESSEGGEN examines all control areas against their current status and develops a BESSEGGEN specific plan to implement the controls.

Insider Threats vs. Outsider Threats

A quick review of the critical controls may lead some readers to think that they are heavily focused on outsider threats and may, therefore, not fully deal with insider attacks. In reality, the insider threat is well covered in these controls in two ways. First, specific controls such as network segmentation, control of administrative rights, enforcement of need to know, data leakage protection, and effective incident response all directly address the key ways that insider threats can be mitigated. Second, the insider and outsider threats are merging as outsiders are more and more easily penetrating the security perimeters and becoming "insiders." All of the controls that limit unauthorized access within the BESSEGGEN work effectively to mitigate both insider and outsider threats. It is important to note that these controls are meant to deal with multiple kinds of computer attackers, including but not limited to malicious internal employees and contractors, independent individual external actors, organized crime groups, terrorists, and nation state actors, as well as mixes of these different threats.

Furthermore, these controls are not limited to blocking only the initial compromise of systems, but also address detecting already-compromised machines, and preventing or disrupting attacker's actions. The defenses identified through these controls deal with decreasing the initial attack surface through improving architectures and hardening security, identifying already-compromised machines to address long-term threats inside BESSEGGEN network, controlling so-called 'super user' privileges on systems, and disrupting attackers' command-and-control of implanted malicious code. Figure 1 illustrates the scope of different kinds of attacker activities that these controls are designed to help thwart.

The rings represent the actions computer attackers may take against target machines. These actions include initially compromising a machine to establish a foothold by exploiting one or more vulnerabilities (i.e., "Getting in"). Attackers can then maintain long-term access on a system, often by creating accounts, subverting existing accounts, or altering the software on the machine to include backdoors and rootkits (i.e., "Staying In"). Attackers with access to machines can also cause damage, which could include stealing, altering, or destroying information; impairing the system's functionality to jeopardize its business effectiveness or mission; or using it as a jump-off point for compromise of other systems in the environment (i.e. "Acting"). Where these rings overlap, attackers have even more ability to compromise sensitive information or cause damage. Outside of each set of rings in the figure, various defensive strategies are presented, which are covered throughout the controls described in this document. Defenses in any of the rings helps to limit the abilities of attackers, but improved defenses are required across all three rings and their intersections. It is important to note that the guidelines are designed to help improve defenses across each of these rings, rather than on merely preventing initial compromise.

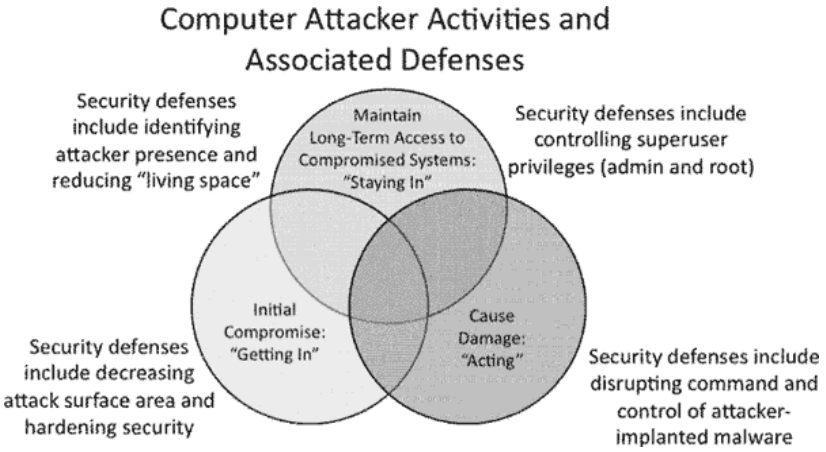


Figure 1: Computer Attacker Activities and Associated Defenses

Periodic and Continuous Testing of Controls

Each control included in this document describes a series of tests that BESSEGGEN conducts on a periodic or, in some cases, continual basis to ensure that appropriate defenses are in place. One of the goals of the tests described in this document is to provide as much automation of testing as possible. By leveraging standardization efforts these automated test suites and scripts can be highly shareable between organizations, consistent to a large extent, and easily used by auditors for validation. However, at various phases of the tests, human testers are needed to set up tests or evaluate results in a fashion that cannot be automated. The testers associated with measuring such controls must be trusted individuals, as the test may require them to access sensitive network devices/systems or data in the course of their tests. Without appropriate authorization, background checks, and possibly clearance, such tests may be impossible. Such tests will also be supervised or reviewed by appropriate agency officials well versed in the parameters of lawful monitoring and analysis of information technology systems.

DESCRIPTION OF CONTROLS

Control 1: Inventory and Control of Hardware Assets

Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

Attackers are continuously scanning the address space of target organizations, waiting for new and possibly unprotected systems to be attached to the network. They are particularly interested in devices which come and go off of the enterprise's network such as laptops or Bring-Your-Own-Devices (BYOD) which might be out of synch with security updates or might already be compromised. Even devices that are not visible from the Internet can be used by attackers who have already gained internal access and are hunting for internal pivot points or victims. Additional systems that connect to the enterprise's network (e.g., demonstration systems, temporary test systems, guest networks) also be managed carefully and/or isolated in order to prevent adversarial access from affecting the security of enterprise operations.

This Control requires both technical and procedural actions, united in a process that accounts for and manages the inventory of hardware and all associated information throughout its life cycle. It links to business governance by establishing information/asset owners who are responsible for each component of a business process that includes information, software, and hardware. BESSEGGEN uses large-scale, comprehensive enterprise products to maintain IT asset inventories.

Critical Control 2: Inventory and Control of Software Assets

Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution. Attackers continuously scan target organizations looking for vulnerable versions of software that can be remotely exploited. Some attackers also distribute hostile web pages, document files, media files, and other content via their own web pages or otherwise trustworthy third-party sites. When unsuspecting victims access this content with a vulnerable browser or other client-side program, attackers compromise their machines, often installing backdoor programs and bots that give the attacker long-term control of the system. Managed control of all software also plays a critical role in planning and executing system backup, incident response, and recovery. Whitelisting is implemented using a combination of commercial whitelisting tools, policies or application execution tools that come with antivirus suites and popular operating systems. The best of these tools provides an inventory check of hundreds of common applications used in enterprises, pulling information about the patch level of each installed program to ensure that it is the latest version and leveraging standardized application names, such as those found in the common platform enumeration specification.

Critical Control 3: Continuous Vulnerability Management

Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers. An effective vulnerability assessment and remediation program must be able to prevent the exploitation of vulnerabilities by detecting and remediating vulnerabilities in covered devices in a timely fashion. Proactively managing vulnerabilities on covered devices will reduce or eliminate the potential for exploitation and save on the resources otherwise needed to respond to incidents after exploitation has occurred. BESSEGGEN has defined roles and responsibilities associated with vulnerability detection and remediation.

Critical Control 4: Controlled Use of Administrative Privileges

The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications. The misuse of administrative privileges is a primary method for attackers to spread inside a target enterprise. Two very common attacker techniques take advantage of uncontrolled administrative privileges. In the first, a workstation user running as a privileged user is fooled into opening a malicious email attachment, downloading and opening a file from a malicious website, or simply surfing to a website hosting attacker content that can automatically exploit browsers. The file or exploit contains executable code that runs on the victim's machine either automatically or by tricking the user into executing the attacker's content. The second common technique used by attackers is elevation of privileges by guessing or cracking a password for an administrative user to gain access to a target machine. If administrative privileges are loosely and widely distributed, or identical to passwords used on less critical systems, the attacker has a much easier time gaining full control of systems, because there are many more accounts that can act as avenues for the attacker to compromise administrative privileges.

Critical Control 5: Secure Configurations for Hardware and Software on Routers, Switches, WLC's, AP's, Laptops, Workstations, and Servers

Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings. Prevent attackers

from exploiting services and settings that allow easy access through networks and browsers: Build a secure image that is used for all new systems deployed to the enterprise, host these standard images on secure storage servers, regularly validate and update these configurations, and track system images in a configuration management system. All remote administration of servers, workstation, network devices, and similar equipment done over secure channels. Protocols such as telnet, virtual network computing (VNC), remote desktop protocol (RDP), or other protocols that do not natively support strong encryption used if they are performed over a secondary encryption channel, such as secure sockets layer (SSL) or Internet protocol security (IPSEC).

Critical Control 6: Maintenance, Monitoring and Analysis of Audit Logs

Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack. Most free and commercial operating systems, network services, and firewall technologies offer logging capabilities. Such logging should be activated, with logs sent to centralized logging servers. Firewalls, proxies, and remote access systems (VPN, dial-up, etc.) should all be configured for verbose logging, storing all the information available for logging in the event a follow-up investigation is required. Furthermore, operating systems, especially those of servers, should be configured to create access control logs when a user attempts to access resources without the appropriate privileges. To evaluate whether such logging is in place, an organization should periodically scan through its logs and compare them with the asset inventory in order to ensure that each managed item actively connected to the network is periodically generating logs. Analytical programs such as SIEM solutions for reviewing logs can provide value, but the capabilities employed to analyze audit logs are quite extensive, even including, importantly, just a cursory examination by a person. Actual correlation tools can make audit logs far more useful for subsequent manual inspection. Such tools can be quite helpful in identifying subtle attacks. However, these tools are neither a panacea nor a replacement for skilled information security personnel and system administrators. Even with automated log analysis tools, human expertise and intuition are often required to identify and understand attacks.

Critical Control 7: Email and Web Browser Protections

Minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems. Web browsers and email clients are very common points of entry and attack because of their technical complexity, flexibility, and their direct interaction with users and with the other systems and websites. Content can be crafted to entice or spoof users into taking actions that greatly increase risk and allow introduction of malicious code, loss of valuable data, and other attacks. Since these applications are the main means for users to interact with untrusted environments, these are potential targets for both code exploitation and social engineering.

Critical Control 8: Malware Defenses

Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action. Malware defenses must be able to operate in this dynamic environment through large-scale automation, rapid updating, and integration with processes like incident response. They must also be deployed at multiple possible points of attack to detect, stop the movement of, or control the execution of malicious software. Enterprise endpoint security suites provide administrative features to verify that all defenses are active and current on every managed system. To ensure anti-virus signatures are up-to-date, organizations use automation. They use the built-in administrative features of enterprise endpoint security suites to verify that anti-virus, antispyware, and host-based IDS features are active on every managed system. They run automated assessments daily and review the results to find and mitigate systems that have deactivated such protections, as well as systems that do not have the latest malware definitions.

Critical Control 9: Limitation and Control of Network Ports, Protocols, and Services

Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers. Attackers search for remotely accessible network services that are vulnerable to exploitation. Common examples include poorly configured web servers, mail servers, file and print services, and Domain Name System (DNS) servers installed by default on a variety of different device types, often without a business need for the given service. Port scanning tools are used to determine which services are listening on the network for a range of target systems. In addition to determining which ports are open, effective port scanners can be configured to identify the version of the protocol and service listening on each discovered port. This list of services and their versions are compared against an inventory of services required by the organization for each server and workstation in an asset management system. Recently added features in these port scanners are being used to determine the changes in services offered by scanned machines on the network since the previous scan, helping security personnel identify differences over time.

Critical Control 10: Data Recovery Capabilities

The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it. When attackers compromise machines, they often make significant changes to configurations and software. Sometimes attackers also make subtle alterations of data stored on compromised machines, potentially jeopardizing organizational effectiveness with polluted information. When the attackers are discovered, it can be extremely difficult for organizations without a trustworthy data recovery capability to remove all aspects of the attacker's presence on the machine.

Critical Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches

Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings. Attackers take advantage of network devices becoming less securely configured over time as users demand exceptions for specific business needs. Sometimes the exceptions are deployed and then left undone when they are no longer applicable to the business needs. In some cases, the security risk of the exception is neither properly analyzed nor measured against the associated business need and can change over time. Attackers search for vulnerable default settings, gaps or inconsistencies in firewall rule sets, routers, and switches and use those holes to penetrate defenses. They exploit flaws in these devices to gain access to networks, redirect traffic on a network, and intercept information while in transmission. Through such actions, the attacker gains access to sensitive data, alters important information, or even uses a compromised machine to pose as another trusted system on the network.

Critical Control 12: Boundary Defense

Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data. Attackers focus on exploiting systems that they can reach across the internet, including not only DMZ systems but also workstations and laptop computers that pull content from the Internet through network boundaries. To control the flow of traffic through network borders and police content by looking for attacks and evidence of compromised machines, boundary defenses should be multi-layered, relying on firewalls, proxies, DMZ perimeter networks, and network-based IPS and IDS. It is also critical to filter both inbound and outbound traffic. It should be noted that boundary lines between internal and external networks are diminishing as a result of increased interconnectivity within and between organizations as well as the rapid rise in deployment of wireless technologies. These blurring lines

sometimes allow attackers to gain access inside networks while bypassing boundary systems. However, even with this blurring of boundaries, effective security deployments still rely on carefully configured boundary defenses that separate networks with different threat levels, sets of users, data and levels of control. And despite the blurring of internal and external networks, effective multi-layered defenses of perimeter networks help lower the number of successful attacks, allowing security personnel to focus on attackers who have devised methods to bypass boundary restrictions.

Critical Control 13: Data Protection

The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information. It is important that an organization understand what its sensitive information is, where it resides, and who needs access to it. To derive sensitivity levels, organizations need to put together a list of the key types of data and the overall importance to the organization. This analysis would be used to create an overall data classification scheme for the organization. Organizations should define labels, such as “Sensitive,” “Business Confidential,” and “Public,” and classify their data according to those labels. Once the private information has been identified, it can then be further subdivided based on the impact it would have to the organization if it were compromised. Once the sensitivity of the data has been identified, create a data inventory or mapping that identifies business applications and the servers that house those applications. The network then needs to be segmented so that systems of the same sensitivity level are on the same network and segmented from systems with different trust levels. If possible, firewalls need to control access to each segment.

Critical Control 14: Controlled Access Based on the Need to Know

The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, and systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification. Commercial tools are available to support enterprise management of encryption and key management within an enterprise and include the ability to support implementation of encryption controls within cloud and mobile environments. Definition of life cycle processes and roles and responsibilities associated with key management should be undertaken by each organization. Commercial Data loss prevention (DLP) solutions are available to look for exfiltration attempts and detect other suspicious activities associated with a protected network holding sensitive information. Organizations deploying such tools should carefully inspect their logs and follow up on any discovered attempts, even those that are successfully blocked, to transmit sensitive information out of the organization without authorization.

Critical Control 15: Wireless Access Control

Effective organizations run commercial wireless scanning, detection, and discovery tools as well as commercial wireless intrusion detection systems. Major thefts of data have been initiated by attackers who have gained wireless access to organizations from outside the physical building, bypassing organizations’ security perimeters by connecting wirelessly to access points inside the organization. Effective organizations run commercial wireless scanning, detection, and discovery tools as well as commercial wireless intrusion detection systems. Additionally, the security team should periodically capture wireless traffic from within the borders of a facility and use free and commercial analysis tools to determine whether the wireless traffic was transmitted using weaker protocols or encryption than the organization mandates. When devices relying on weak wireless security settings are identified, they should be found within the organization’s asset inventory and either reconfigured more securely or denied access to the

organization network. Additionally, the security team should employ remote management tools on the wired network to pull information about the wireless capabilities and devices connected to manage systems.

Critical Control 16: Account Monitoring and Control

Actively manage the life cycle of system and application accounts - their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them. Although most operating systems include capabilities for logging information about account usage, these features are sometimes disabled by default. Even when such features are present and active, they often do not provide fine-grained detail about access to the system by default. Security personnel can configure systems to record more detailed information about account access, and use home-grown scripts or third-party log analysis tools to analyze this information and profile user access of various systems. Accounts must also be tracked very closely. Any account that is dormant must be disabled and eventually removed from the system. All active accounts must be traced back to authorized users of the system, and they should utilize multi-factor authentication. Users must also be logged out of the system after a period of inactivity to minimize the possibility of an attacker using their system to extract information from the organization.

Critical Control 17: Implement a Security Awareness and Training Program

For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs. An effective enterprise-wide training program should take a holistic approach and consider policy and technology at the same time as the training of people. Policies should be designed with technical measurement and enforcement and they should be reinforced by training to fill gaps in understanding; technical controls can be implemented to protect systems and data and minimize the opportunity for people to make mistakes. With technical controls in place, training can focus on concepts and skills that cannot be managed technically.

Critical Control 18: Application Software Security

Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses. Attacks often take advantage of vulnerabilities found in web-based and other application software. Vulnerabilities can be present for many reasons, including coding mistakes, logic errors, incomplete requirements, and failure to test for unusual or unexpected conditions. Examples of specific errors include: the failure to check the size of user input; failure to filter out unneeded but potentially malicious character sequences from input streams; failure to initialize and clear variables; and poor memory management allowing flaws in one part of the software to affect unrelated (and more security critical) portions.

Critical Control 19: Incident Response and Management

Protect the organization’s information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker’s presence, and restoring the integrity of the network and systems. After defining detailed incident response procedures, the incident response team should engage in periodic scenario-based training,

working through a series of attack scenarios fine-tuned to the threats and vulnerabilities the organization faces. These scenarios help ensure that team members understand their role on the incident response team and also help prepare them to handle incidents. It is inevitable that exercise and training scenarios will identify gaps in plans and processes, and unexpected dependencies.

Critical Control 20: Penetration Tests and Red Team Exercises

Test the overall strength of an organization's defense (the technology, the processes, and the people) by simulating the objectives and actions of an attacker. A successful defensive posture requires a comprehensive program of effective policies and governance, strong technical defenses, and appropriate action by people. Penetration testing starts with the identification and assessment of vulnerabilities that can be identified in the enterprise. Red Team exercises take a comprehensive approach at the full spectrum of organization policies, processes, and defenses in order to improve organizational readiness, improve training for defensive practitioners, and inspect current performance levels. Independent Red Teams can provide valuable and objective insights about the existence of vulnerabilities and the efficacy of defenses and mitigating controls already in place and even of those planned for future Implementation. Penetration tests and Red Team tests are performed:

- as a "dramatic" demonstration of an attack, usually to convince decision makers Of their enterprise's vulnerability;
- as a means to test the correct operation of enterprise defenses ("verification"); and to test that the enterprise has built the right defenses in the first place ("validation").

Appendix – II

Guidelines on Cyber Crisis Management and Security of Critical Infrastructure

1.0 Introduction

Critical networks contain Network devices, computers and applications that perform key functions in providing essential services and commodities. As such, they are part of the nation's critical infrastructure and require protection from a variety of threats that exist in cyberspace today. By allowing remote collection and analysis of data and control of equipment, critical networks provide great efficiency and are widely used. However, this makes critical networks potentially vulnerable to disruption of service, process redirection, or manipulation of operational data that could result in public safety concerns and/or serious disruptions to the nation's critical infrastructure.

2.0 Guidelines to improve security of critical networks

The guidelines prescribed in the following sections are intended to ensure that interruptions or manipulations of critical functions/services in critical sector organizations are brief, infrequent, and manageable and cause least possible damage. The following steps focus on specific actions to be taken to improve the security of critical networks:

2.1 Identify all connections to critical networks.

Conduct a thorough risk analysis to assess the risk and necessity of each connection to the critical network. Develop a comprehensive understanding of all connections to the critical network, and how well these connections are protected. Identify and evaluate the following types of connections:

- Internal local area and wide area networks, including business networks
- The Internet and networking devices
- Wireless network devices, including satellite uplinks
- Modem or dial-up connections
- Connections to customers, business partners, vendors or regulatory agencies

2.2 Disconnect unnecessary connections to the critical network.

To ensure the highest degree of security of critical systems, isolate the critical network from other network connections to as great a degree as possible. Any connection to another network introduces security risks, particularly if the connection creates a pathway from or to the Internet. Although direct connections with other networks may allow important information to be passed efficiently and conveniently, insecure connections are simply not worth the risk; isolation of the critical network must be a primary goal to provide needed protection. Consider 'Air-Gap' for sensitive networks, following a risk assessment. Strategies such as utilization of "demilitarized zones" (DMZs) and data warehousing can facilitate the secure transfer of data from the critical network to business networks. However, they must be designed and implemented properly to avoid introduction of additional risk through improper configuration.

2.3 Evaluate and strengthen the security of any remaining connections to the critical network.

Conduct penetration testing or vulnerability analysis of any remaining connections to the critical network to evaluate the protection posture associated with these pathways. Use this information in conjunction with risk management processes to develop a robust protection strategy for any pathways to the critical network. Since the critical network is only as secure as its weakest connecting point, it is essential to deploy firewalls, intrusion detection systems (IDSs), and other appropriate security measures at each point of entry. Configure firewall rules to prohibit access from and to the critical network, and be as specific as possible when permitting approved connections. For example, an Independent System Operator (ISO) should not be granted "blanket" network access simply because there is a need for a connection to certain

components of the critical system. Strategically place IDSs at each entry point to alert security personnel of potential breaches of network security. Organization management must understand and accept responsibility for risks associated with any connection to the critical network.

2.4 Harden critical networks by removing or disabling unnecessary services.

Critical control servers built on commercial or open-source operating systems can be exposed to attack through default network services. To the greatest degree possible, remove or disable unused services and network daemons to reduce the risk of direct attack. This is particularly important when critical networks are interconnected with other networks. Do not permit a service or feature on a critical network unless a thorough risk assessment of the consequences of allowing the service/feature shows that the benefits of the service/feature far outweigh the potential for vulnerability exploitation. Examples of services to remove from critical networks include automated meter reading/remote billing systems, email services, and Internet access. An example of a feature to disable is remote maintenance. Numerous secure configuration guidelines for both commercial and open-source operating systems are available in the public domain. Additionally, work closely with critical vendors to identify secure configurations and coordinate any and all changes to operational systems to ensure that removing or disabling services does not cause downtime, interruption of service, or loss of support.

2.5 Do not rely on proprietary protocols to protect your system.

Some critical systems use unique, proprietary protocols for communications between field devices and servers. Often the security of critical systems is based solely on the secrecy of these protocols. Unfortunately, obscure protocols provide very little “real” security. Do not rely on proprietary protocols or factory default configuration settings to protect your system. Additionally, it may be demanded from vendors to disclose any backdoors or vendor interfaces to your critical systems, and expect them to provide systems that are capable of being secured.

2.6 Implement the security features provided by device and system vendors.

Older critical systems (most systems in use) have no security features whatsoever. Critical system owners must insist that their system vendor implement security features in the form of product patches or upgrades. Some newer critical devices are shipped with basic security features, but these are usually disabled to ensure ease of installation. Analyze each critical device to determine whether security features are present. Additionally, factory default security settings (such as in computer network firewalls) are often set to provide maximum usability, but minimal security. Set all security features to provide the maximum level of security. Allow settings below maximum security only after a thorough risk assessment of the consequences of reducing the security level.

2.7 Establish strong controls over any medium that is used as a backdoor into the critical network.

Where backdoors or vendor connections do exist in critical systems, strong authentication must be implemented to ensure secure communications. Modems, wireless, and wired networks used for communications and maintenance represent a significant vulnerability to the critical network and remote sites. Successful “war dialing” or “war driving” attacks could allow an attacker to bypass all other controls and have direct access to the critical network or resources. To minimize the risk of such attacks, disable inbound access and replace it with some type of call back system.

2.8 Implementation of control for Data flow

A data diode is a piece of hardware that physically enforces a one-way flow of data. As one-way data transfer systems, data diodes are used as cybersecurity tools to isolate and protect networks from external cyber threats and prevent penetration from any external sources. A data diode sits at the edge of the network security perimeter; relying on its physical hardware components to mitigate all cyber threats against the network while simultaneously allowing the transfer of data out of the network in a highly controlled, deterministic manner. Data diodes create a physical barrier between networks and hence can be used for one-way communication channels from secure network to the insecure network protecting highly sensitive data and networks of critical infrastructure.

2.9 Implement internal and external intrusion detection systems, incident response systems and establish 24-hour-a-day incident monitoring.

To be able to effectively respond to cyber-attacks, establish an intrusion detection strategy that includes alerting network administrators of malicious network activity originating from internal or external sources. Intrusion detection system monitoring is essential 24 hours a day. Additionally, incident response procedures must be in place to allow an effective response to any attack. To complement network monitoring, enable logging on all systems and audit system logs daily to detect suspicious activity as soon as possible.

2.10 Perform technical audits of critical devices and networks, and any other connected networks, to identify security concerns.

Technical audits of critical devices and networks are critical to ongoing security effectiveness. Many commercial and open-source security tools are available that allow system administrators to conduct audits of their systems/networks to identify active services, patch level, and common vulnerabilities. The use of these tools will not solve systemic problems, but will eliminate the “paths of least resistance” that an attacker could exploit. Analyse identified vulnerabilities to determine their significance, and take corrective actions as appropriate. Track corrective actions and analyse this information to identify trends. Additionally, retest systems after corrective actions have been taken to ensure that vulnerabilities were actually eliminated. Scan non-production environments actively to identify and address potential problems.

2.11 Conduct physical security surveys and assess all remote sites connected to the critical network to evaluate their security.

Any location that has a connection to the critical network is a target, especially unmanned or unguarded remote sites. Conduct a physical security survey and inventory access points at each facility that has a connection to the critical system. Identify and assess any source of information including remote telephone/computer network/fiber optic cables that could be tapped; radio and microwave links that are exploitable; computer terminals that could be accessed; and wireless local area network access points. Identify and eliminate single points of failure. The security of the site must be adequate to detect or prevent unauthorized access. Do not allow “live” network access points at remote, unguarded sites simply for convenience.

2.12 Establish critical “Red Teams” to identify and evaluate possible attack scenarios.

Establish a "Red Team (this term refers to teams that conduct security evaluation exercises in an unannounced manner)" to identify potential attack scenarios and evaluate potential system vulnerabilities. Use a variety of people who can provide insight into weaknesses of the overall network, critical systems, physical systems, and security controls. People who work on the system every day have great insight into the vulnerabilities of your critical network and should be consulted when identifying potential attack scenarios and possible consequences. Also, ensure that the risk from a malicious insider is fully evaluated, given that this represents one of the greatest threats to an organization. Feed information resulting from the "Red Team" evaluation into risk management processes to assess the information and establish appropriate protection strategies.

The following steps focus on management actions to establish an effective cyber security program:

2.13 Clearly define cyber security roles, responsibilities, and authorities for managers, system administrators, and users.

Organization personnel need to understand the specific expectations associated with protecting information technology resources through the definition of clear and logical roles and responsibilities. In addition, key personnel need to be given sufficient authority to carry out their assigned responsibilities. Too often, good cyber security is left up to the initiative of the individual, which usually leads to inconsistent implementations and ineffective security. Establish cyber security organizational structures that define roles and responsibilities and clearly identify how cyber security issues are escalated and who is notified in an emergency.

2.14 Document network architecture and identify systems that serve critical functions or contain sensitive information that require additional levels of protection.

Develop and document robust information security architecture as part of a process to establish an effective protection strategy. It is essential that organizations design their networks with security in mind and continue to have a strong understanding of their network architecture throughout its lifecycle. Of particular importance, an in-depth understanding of the functions that the systems perform and the sensitivity of the stored information is required. Without this understanding, risk cannot be properly assessed and protection strategies may not be sufficient. Documenting the information security architecture and its components is critical to understanding the overall protection strategy, and identifying single points of failure.

2.15 Establish a rigorous, ongoing risk management process

A thorough understanding of the risks to network computing resources from denial-of-service attacks and the vulnerability of sensitive information to compromise is essential to an effective cyber security program. Risk assessments form the technical basis of this understanding and are critical to formulating effective strategies to mitigate vulnerabilities and preserve the integrity of computing resources. Initially, perform a baseline risk analysis based on a current threat assessment to use for developing a network protection strategy. Due to rapidly changing technology and the emergence of new threats on a daily basis, an ongoing risk assessment process is also needed so that routine changes can be made to the protection strategy to ensure it remains effective. Fundamental to risk management is identification of residual risk with a network protection strategy in place and acceptance of that risk by management. (Refer ISO 27005) Legacy technologies are extremely vulnerable to attack from cyber criminals because many of these outdated systems are no longer supported by the manufacturer, a single unpatched vulnerability can enable

attackers to access all applications, middleware, and databases running on the server platform. Risk awareness related to legacy technologies need to be maintained and appropriate control should be implemented to reduce the risk. If possible, legacy technologies need to be replaced with the latest technologies to prevent the risk.

2.15.1 Vendor Risk Management

Vendor risk management (VRM) is a comprehensive plan for identifying and decreasing potential business uncertainties and legal liabilities regarding the hiring of 3rd party vendors for information technology (IT) products and services.

Best Practices for Effective Vendor Risk Management:

- Proper planning and due diligence need to be taken for vendor risk identification and mitigation.
- A robust vendor governance program to be developed to assess critical, high, moderate, and low risk vendors through surveys and assessments.
- Vendor performance needs to be monitored on a regular basis to be continually aware of a vendor's capability to comply with contractual obligations. Vendor KPIs and KRIs should be clearly defined in line with applicable laws, regulations, and standards.
- The organizational hierarchy involved in vendor governance need to be defined.
- Procure through Trusted Vendors only as per CEA Guidelines for Trusted Vendors.

2.15.2 Service Level Agreement (SLA)

A Service Level Agreement (SLA) is the service contract component between a service provider and organization. An SLA provides specific and measurable aspects related to service offerings. SLAs are an integral part of an IT/ Network vendor contract. An SLA pulls together information on all of the contracted services and their agreed-upon expected reliability into a single document. They clearly state metrics, responsibilities and expectations so that, in the event of issues with the service, neither party can plead ignorance. It ensures both sides have the same understanding of requirements. Any significant contract without an associated SLA (reviewed by legal counsel) is open to deliberate or inadvertent misinterpretation. The SLA protects both parties in the agreement.

2.15.3 Supply Chain Risk Management

Supply chain risk management (SCRM) is the coordinated efforts of an organization to help identify, monitor, detect and mitigate threats to supply chain continuity and profitability.
The best practices to manage supply chain risks are:

- Include security requirements in every RFP and contract.
- "Right to Audit" on vendor/supplier should be reserved by the organization and same should be included in the RFP/Contract.
- Trusted source during supply, operation and maintenance phase for products and services need to be ensured
- The cyber security posture of supplier organization needs to be ensured
- After finalization of a work contract, involvement of vendors should be there on-site to address any vulnerabilities and security gaps in the supplied products / services.

- Secure Software Lifecycle Development Programs and training for all engineers in the life cycle should be organized.
- Rigorous controls on access by service vendors should be imposed through proper authorization.
- Legacy support for end-of-life products and platforms

2.16 Establish a network protection strategy based on the principle of defense-in-depth.

A fundamental principle that must be part of any network protection strategy is defense-in-depth. Defense-in-depth must be considered early in the design phase of the development process, and must be an integral consideration in all technical decision-making associated with the network. Utilize technical and administrative controls to mitigate threats from identified risks to as great a degree as possible at all levels of the network. Single points of failure must be avoided, and cyber security defense must be layered to limit and contain the impact of any security incidents. Additionally, each layer must be protected against other systems at the same layer. For example, to protect against the insider threat, restrict users to access only those resources necessary to perform their job functions.

2.17 Clearly identify cyber security requirements.

Organizations and companies need structured security programs with mandated requirements to establish expectations and allow personnel to be held accountable. Formalized policies and procedures are typically used to establish and institutionalize a cyber-security program. A formal program is essential for establishing a consistent, standards-based approach to cyber security throughout an organization and eliminates sole dependence on individual initiative. Policies and procedures also inform employees of their specific cyber security responsibilities and the consequences of failing to meet those responsibilities. They also provide guidance regarding actions to be taken during a cyber-security incident and promote efficient and effective actions during a time of cyber crisis. As part of identifying cyber security requirements, include user agreements and notification and warning banners. Establish requirements to minimize the threat from malicious insiders, including the need for conducting background checks and limiting network privileges to those absolutely necessary.

2.18 Establish effective configuration management processes.

A fundamental management process needed to maintain a secure network is configuration management. Configuration management needs to cover both hardware configurations and software configurations. Changes to hardware or software can easily introduce vulnerabilities that undermine network security. Processes are required to evaluate and control any change to ensure that the network remains secure. Configuration management begins with well-tested and documented security baselines for your various systems.

2.19 Conduct routine self-assessments.

Robust performance evaluation processes are needed to provide organizations with feedback on the effectiveness of cyber security policy and technical implementation. A sign of a mature organization is one that is able to self-identify issues, conduct root cause analyses, and implement effective corrective actions that address individual and systemic problems. Self-assessment processes that are normally part of an effective cyber security program include routine scanning for vulnerabilities, automated auditing of the network, and self-assessments of organizational and individual performance.

2.20 Establish system backups and disaster recovery plans.

Establish a disaster recovery plan that allows for rapid recovery from any emergency (including a cyber-attack). System backups are an essential part of any plan and allow rapid reconstruction of the network. Routinely exercise disaster recovery plans to ensure that they work and that personnel are familiar with them. Make appropriate changes to disaster recovery plans based on lessons learned from exercises.

2.21 Senior organizational leadership should establish expectations for cyber security performance and hold individuals accountable for their performance.

Effective cyber security performance requires commitment and leadership from senior managers in the organization. It is essential that senior management establish an expectation for strong cyber security and communicate this to their subordinate managers throughout the organization. It is also essential that senior organizational leadership establish a structure for implementation of a cyber-security program. This structure will promote consistent implementation and the ability to sustain a strong cyber security program. It is then important for individuals to be held accountable for their performance as it relates to cyber security. This includes managers, system administrators, technicians, and users/operators.

2.22 Establish policies and conduct training to minimize the likelihood that organizational personnel will inadvertently disclose sensitive information regarding critical system design, operations, or security controls.

Release data related to the critical network only on a strict, need-to-know basis, and only to persons explicitly authorized to receive such information. “Social engineering,” the gathering of information about a computer or computer network via questions to naive users, is often the first step in a malicious attack on computer networks. The more information revealed about a computer or computer network, the more vulnerable the computer/network is. Never divulge data related to a critical network, including the names and contact information about the system operators/administrators, computer operating systems, and/or physical and logical locations of computers and network systems over telephones or to personnel unless they are explicitly authorized to receive such information. Any requests for information by unknown persons need to be sent to a central network security location for verification and fulfilment. People can be a weak link in an otherwise secure network. Conduct training and information awareness campaigns to ensure that personnel remain diligent in guarding sensitive network information, particularly their passwords.

3.0 Guidelines on Cyber Crisis Management plan for critical networks

3.1 Strategic issues in cyber crisis management and business continuity

- Implementation of appropriate measures to reduce the likelihood of incidents occurring and/or reduce the potential effects of those incidents
- Taking due account of the resilience and mitigation measures
- Providing continuity for critical services during and following an incident
- Taking into account those activities that have not been identified as critical.

The effectiveness of above actions depends on a range of factors such as:

- The maximum tolerable period of disruption of a critical activity
- The costs of implementing a strategy and
- Consequences of inaction

3.2 Effective cyber crisis management and business continuity strategies also cover the following:

3.2.1 People

Organizations should identify appropriate strategies for maintaining core skills and knowledge. This analysis should go beyond employees to contractors and other stakeholders who possess extensive specialist skills and knowledge. Strategies to protect or provide those skills might include:

- Documentation of the way in which critical activities are performed
- Multi-skill training of staff and contractors
- Separation of core skills to reduce the concentration of risk
- Use of third parties
- Succession planning and
- Knowledge retention and management

3.2.2 Premises Organizations should devise a strategy for reducing impact of unavailability of its normal work site(s). This may include one or more of the following:

- Alternative premises (locations) within the organization including displacement of other activities
- Alternative sites provided by other organizations
- Alternative premises provided by third party specialists
- Working from home or at remote sites
- Other agreed suitable premises and
- Use of an alternative workforce in an established site

3.2.3 Technology

Technology strategies depend on the nature of the technology employed and its relationship with critical activities, but will typically be one or a combination of the following:

- Provision made within the organization
- Services delivered to the organization and
- Services provided externally by a third party
- Technology strategies may include:
- Geographical spread of technology
- Holding older equipment as emergency replacement or spares and ‘
- Additional risk mitigation for unique or long lead time equipment

Network services require complex continuity strategies. In such cases, consideration should be given to:

- Recovery time objectives (RTO) & Recovery point objectives (RPO) for systems and applications that support the key activities identified in the business impact analysis
- Location and distance between technology sites
- Number of technology sites
- Remote access
- Use of un-staffed sites as opposed to staffed sites

- Telecom connectivity and redundant routing
- The nature of fail-over (whether manual intervention is required to activate alternative IT provision or it can be done automatically)
- Third party connectivity and external links

3.2.4 Information

Information strategies should be such as to ensure that information vital to the organization's operation is protected and recoverable according to the time frames prescribed with the business impact analysis. These strategies should include information in both hard copy formats and electronic formats. Any information required for enabling the delivery of organization's critical activities should have appropriate:

- Confidentiality
- Integrity
- Availability and
- Currency

Appendix – III

Sample Business Impact Analysis (BIA)

Business Impact Analysis (BIA) as applied to a small organization / field office In this example, an agency maintains a small field office with a local area network (LAN) that supports about 50 users. The office relies on the LAN and its components for standard automated processes, such as developing and using

spreadsheets, word processing, and electronic mail (e-mail). The office also maintains a customized database application that supports Inventory, a key resource management process. The network manager is responsible for developing a network contingency plan and begins with the business impact analysis (BIA). The network includes the following components:

- Authentication/network operating system server
- Database server (supports customized Inventory database application)
- File server (stores general, non-Inventory files)
- Application server (supports office automation software)
- Networked printer
- Routers
- Switches
- WLC's
- AP's
- E-mail server and application
- 50 desktop computers
- Five hubs.

The Contingency Planning Coordinator begins the BIA process by identifying the network stakeholders. In this case, the coordinator identifies and consults with the following individuals:

- Inventory process manager
- Sampling of network users
- System administrators for each network server.

Based on subsequent discussions, the coordinator learns the following information:

- The Inventory system is critical to the parent agency's master resource management operations; the system provides updated data to the larger system at the end of each business day. If the system were unavailable for more than 1 working day (8 hours), significant business impacts would result at the parent agency. Inventory requires a minimum of five personnel with desktop computers and access to the system database to process data. Also, five personnel to provide and maintain network services to clients.
- Other non-Inventory processes may be considered non-critical and could be allowed to lapse for up to 10 days.
- The ORGANISATION/ RNOC HOD's and Inventory manager indicate that e-mail is an essential service; however, staff can operate effectively without e-mail access for up to 3 days.
- Staff could function without access to the spreadsheet application for up to 15 working days without affecting business processes significantly.
- Word processing access would need to be restored within 5 working days; however, individuals could use manual processes for up to 10 days if the required forms were available in hard-copy format.
- Outputs from the day's Inventory system records normally are printed daily; the data to be printed may be stored on any desktop computer used by the Inventory system staff. In an emergency, the Inventory system output could be transmitted electronically via e-mail for up to 3 days before significantly affecting business operations. Other printing functions would not be considered essential and could be unavailable for up to 10 days with no impact on business functions.

Based on the information gathered in discussions with stakeholders, the Contingency Planning Coordinator follows the three-step BIA process to identify critical network/ information technology (IT) resources, identify outage impacts and allowable outage times, and develop recovery priorities.

Identify Critical IT Resources

The manager identifies the following resources as critical, meaning that they support critical business processes:

- Authentication/network operating system server (required for users to have LAN access)
- Database server (required to process the Inventory system)
- E-mail server and application
- Five desktop computers (to support five Inventory users)
- One hub (to support five Inventory users)
- Routers
- Switches
- WLC's
- AP's
- Network cabling
- Electric power
- Heating, ventilation, and air conditioning (HVAC)
- Physical security
- Facility.

Identify Outage Impacts and Allowable Outage Times

Next, the manager determines outage impacts and allowable outage times for the critical resources:

Resource	**Outage Impact**	**Allowable Outage Time**
Authentication server	Users could not access Inventory system	8 hours
Tier 1 & 2 Routers and Switches	Users could not access Inventory system	8 hours
E-mail server	Users could not send e-mail	2 days
5 desktop computers	Users could not access Inventory system	8 hours
Hub	Users could not access Inventory system	8 hours
Network cabling	Users could not access Inventory system	8 hours
Electric power	Users could not access Inventory system	8 hours
Printer	Users could not produce Inventory reports	4 days

Develop Recovery Priorities

Using the table completed in the previous step, the Contingency Planning Coordinator develops recovery priorities for the system resources. The manager uses a simple high-, medium-, low-scale to prioritize the resources. High priorities are based on the need to restore critical resources within their allowable outage times; medium and low priorities reflect the requirement to restore full operational capabilities over a

longer recovery period.

Resource	**Recovery Priority**
Authentication server	High
Tier 1& 2 Routers and Switches	High
Desktop computers	High
Hub	High
Network cabling	High
Electric power	High
E-mail server	Medium
Printer	Medium
Remaining desktop computers (45)	Low
Remaining hubs (4)	Low

Having completed the BIA, the Contingency Planning Coordinator may use the recovery priority information above to develop strategies that enable all system resources to be recovered within their respective allowable outage times and in a prioritized manner.
A template for completing the BIA is provided below.

Business Impact Analysis (BIA) Template

This sample template is designed to assist the user in performing a BIA on an IT system. The BIA is an essential step in developing the IT contingency plan. The template is meant only as a basic guide and may not apply to all systems. The user may modify this template or the general BIA approach as required to best accommodate the specific system.

Preliminary System Information Organization:	Date BIA Completed:
System Name:	BIA POC:
System Manager Point of Contact (POC):	
System Description: {Discussion of the system purpose and architecture, including system diagrams}	
A. Identify System POCs	**Role**
Internal POC {Identify the individuals, positions, or offices within your organization that depend on or support the system; also specify their relationship to the system}	
• Xxxx	• xxxx

• xxxx • xxxx =	• xxxx • xxxx
External POC {Identify the individuals, positions, or offices outside your organization that depend on or support the system; also specify their relationship to the system}	
• xxxx • xxxx • xxxx	• xxxx • xxxx • xxxx
B. Identify System Resources {Identify the specific hardware, software, and other resources that comprise the system; include quantity and type}	
Hardware • xxxx • xxxx • xxxx	
Software • xxxx • xxxx	

Appendix –IV

Information Security Management System (ISMS)

(a) Information Security and Management

Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities. Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met.

An Information Security Management System (ISMS) is a systematic approach to managing sensitive information of an organization (Discom) so that it remains secure. The adoption of an information security management system is a strategic decision for an organization. It encompasses people, processes and IT systems.

(b) Information Security Standards

International Organization for Standardization (ISO) has published the following standards to enable organizations to establish and implement ISMS effectively:

ISO 27001 - Information Security Management Systems - Requirements
ISO 27002 - Code of Practice for Information Security Management

These standards codify industry experience and security best practices, and are applicable to all types of organizations, irrespective of their size or business.

(c) National Cyber security Policy, 2013

In light of the growth of IT sector in the country, the National Cyber Security Policy of India 2013 was announced by Indian Government in 2013 yet its actual implementation is still missing. As a result, fields like e-governance and e-commerce are still risky and may require cyber insurance in the near future. Its important features include:

- To build secure and resilient cyber space
- Creating a secure cyber ecosystem, generate trust in IT transactions.
- Creation of National Critical Information Infrastructure Protection Center (NCIIPC)
- Indigenous technological solutions
- Testing of ICT products and certifying them/ Validated products etc.

Countering cybercrimes is a coordinated effort on the part of several agencies in the Ministry of Home Affairs and in the Ministry of Electronics and Information Technology. The law enforcement agencies such as the CBI, IB, state police organizations and other specialized organizations such as Indian Computer Emergency Response Team (CERT-In) are the main organizations to tackle cybercrimes.

Appendix –V

Cyber Resilience Control matrix

Component	Protect	Detect	Contain	Recover
Identity	●Controlled access based on need-to- know ●Enforce Strong password policy ●Multi factor authentication ●Usage of Digital Certificates	●Maintenance and Analysis of complete security events and audit logs ●Privilege escalation monitoring and alerting	●Minimize the invalid logon counts ●Revocation of digital certificate ●Change access control on all devices ●Continuous account monitoring and deactivating the dormant accounts	●Offline recovery procedures for logging into accounts ● Alternative Indicators
System Processes	●Effective Security Patch Updating Mechanism on applications etc. ●Following Best Security practices during Software Development Lifecycle ●Secure configuration ●Malware defenses	●Forensic Memory Analysis ●File integrity checking ●Malware Analysis	●Policy based restrictions on process actions ●Reconfiguration of settings ●Usage of Sandbox Security Mechanism	●Assured Data Back-ups ●Clustering ●Recovery Time Objectives (RTO) & Recovery Point Objectives (RPO) for system and support ●Manual /automated takeover to activate alternative IT provision ●Use of Unstaffed sites as opposed to staffed sites
Hardware and Software Platform	●Asset Inventory (asset classification and management) ●Supply chain protections ●Regular review of configuration files: OS/middleware ●Boot process integrity check	●Continuous vulnerability testing and remediation ●Tamper detection mechanism ●Platform Security Assessment (Review of System architecture/Operating system configuration/Security management controls/System configuration)	●Remote Wipe on failed logins ●Code Integrity Checks to help prevent malicious code from being injected into system files or into the kernel at load/run time	●Baseline remote image deployment ●Usage of Virtual environment ●Assured Back-up and replication ●Replacing compromised files with clean versions

Data	● Database access control: Regular review of access privileges to users of the database/use of biometric technology ● Data Encryption while in-process, handling, storage or transit) ● Data Masking (for sensitive information) ●	● Monitoring Data flow to detect data leakage ● Forensic disk imaging and analysis ● Monitoring remote access ● Database integrity Checking	● Application restrictions monitoring ● Data Leakage Prevention (system designed to detect potential data leakage while in-process, handling, storage or transit ● Access Control on Database	● Assured Data Back-ups and physical segregation of back-up ● Storage replication Mirroring/Cloning ● Database reprocessing (Going back to a known point of database activity before the problem occurred and reprocessing work from that point forward)
Network	● Limitation and control of ports, protocols and services ● Wireless Device Control ● Following Best Practices for secure configuration of network devices	● Centralized network log analysis for wired & wireless networks ● Honey-net ● Network Scanning and Analysis	● Isolation of trusted networks from untrusted networks. ● Denial of service offload to ISP and cloud ● Reconfiguration of impacted network devices ● Modify access control (all user/root/administrator passwords) in all systems and network devices	● Alternate network routing ● Alternative cloud communications ● Usage of devices in cluster mode/load balancing mode

Annexure – A

CRISIS MANAGEMENT GROUP (CMG)

1 Computer Emergency Response Team India (CERT –IN)

The Organization Cyber Crisis Management Group CMG can report any Cyber Security Incidents/ Cyber Attacks / Cyber Breach or any adverse activity or unwanted behavior which they may feel as an incident to CERT-In.

They may use the following channels to report the incident.

E-mail: incident@cert-in.org.in

Helpdesk: +91-1800-11-4949

Fax: +91-1800-11-6969

2 Name of CISO: Vibhu Garg

3 Name of Officers for CMG:

CRISIS MANAGEMENT TEAM			
NAME	**DEPT**	**ROLE**	**Contact**
Karun Singla		Partner	
Ankit Pruthi		Partner	
Vibhu Garg		CISO	

Annexure B

Key Vendor Contact Details

Vendor	Contact Person	Contact Number/Mobile	Off Business Hours Contact
<Software Solution Provide >			
<Hardware Solution Provider>			
<LAN Solution Provider>			
<WAN Solution Provider>			
Firewall and Antivirus			

Annexure C

IT Vendor Escalation Matrix

Vendor Name	Service Proving For	Escalation 1	Escalation 2	Escalation 3

Annexure D
Incident Management Process

Incident Response

Activity	Authority/ Responsibility
The personnel who detected the incident shall immediately bring it to the notice of the Crisis Management Group. (CMG)	Users & CMG
The CMG shall intimate the facts and impacts of incident to CISO using the Incident Reporting Form (Refer to Annexure-E, F)	CMG
The CMG shall, in consultation with the concerned Head of Department, analyze the impact of the incident, then document and send it to the CISO using the Incident Management Form (Refer to Annexure-H)	CMG
The CMG Team shall maintain the log of all incidents. By using Incident tracker (Refer Annexure-G)	CMG
The CMG Team shall categorize all incidents based on the nature of each incident. The CMG may take assistance from domain experts to classify the incidents.	CMG
The CISO, in consultation with IT Team shall prepare the corrective action plan for the Incident and present it to Crisis Management Group (CMG) for approval.	CISO & CMG

Level of Escalation

Activity	Authority/ Responsibility
Level One Escalation Level One is the initial level for all incidents. The contact must be available 24x7x365 and therefore represents a role rather than an individual. The contacts at this level must have the ability to call to action engineers and to escalate to management as required, to resolve all categories and severity of incidents. All reports must be sent to the CISO every week.	User & CMG
Level Two Escalation Level Two represents senior management with authority to take actions that fall outside the standard operating policies of the concerned organizations. Escalation to Level Two is appropriate in cases where Level-One interactions have been unsuccessful in resolving an operational issue within the stipulated time schedule.	CMG

Annexure-E

Incident Reporting Form

Form to report Incidents to CERT-In			
For official use only:		Incident Tracking Number: **CERTIn-xxxxxx**	
1. Contact Information for this Incident:			
Name:	Organization:	Title:	
Phone / Fax No:	Mobile:	Email:	
Address:			
2. Sector : (Please tick the appropriate choices)			
Government Financial Power	Transportation Manufacturing Health	Telecommunications Academia Petroleum Insurance	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:	Operating System (incl. 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 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	Anomalies 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.

12. Agencies notified?			
Law Enforcement	Private Agency	Affected Product Vendor	Other

11. 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 checked	Log Files examined System(s) disconnected form 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		

Contact Details of CERT-In

If the purpose of communication is a cyber-security incident report contact CERT-In Incident Response Help Desk

Email: incident@cert-in.org.in

Phone: +91-11-24368572

Toll Free Phone: +91-1800-11-4949

Toll Free Fax: +91-1800-11-6969

If the purpose of your communication is vulnerability report, security alerts, or any other technical questions/feedback related to cyber security, contact CERT-In Information Desk.

Email: info@cert-in.org.in

PGP Key Details:

User ID: info@cert-in.org.in
advisory@cert-in.org.in
subscribe@cert-in.org.in

Phone: +91-11-24368572

Toll Free Phone: +91-1800-11-4949

Toll Free Fax: +91-1800-11-6969

Email: csk@cert-in.org.in

PGP Key Details:

Phone: +91-11-24368572

Toll Free Phone: +91-1800-11-4949

Toll Free Fax: +91-1800-11-6969

Postal Address:

Indian Computer Emergency Response Team (CERT-In) Ministry of Electronics and Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India

+91-11-24368572
+91-1800-11-6969

Annexure-F:

Incident Response Form

From:

To:

Incident Ref #:			Incident Date: Incident Time:	
No #	Location	Date of reporting	Details	Risk and Impact Analysis
Location / Office:			Date of reporting from the Location / Office:	
Facts of the incident:				
Discussed with IT Team:				
Cause of the Incident:				

Corrective Action plan for Incident management (with time schedule):					
#	Corrective Action	Responsibility	Start Date	Date of Completion	Cost incurred

Preventive Action Plan:			
#	Actions Required	Test Results	List of Departments Informed

Signature: IT Head/ Designated Authority	Date:

Annexure-G:
Incident Tracker

Incident Tracker								
Issue No.	**Incident Reporti-ng Date**	**Problem Description**	**Problem identificati-on**	**Problem Resoluti-on**	**Status**	**Issue Resolv-ed date**	**Challenges faced**	**Remarks**

Annexure-H
Incident Management Form

Name of Reportee	
Date of Filing Incident	
Record Number	
Filed by CISO	
Type of Incident - Physical Incident (P) - Logical Incident (L)	

Scope of Incident - What did happen? - Which asset(s) have been compromised? - What is the damage done?	
Time of Incident - When was it detected? - When was it reported? - When action was taken?	
Authorities (Name, Designation, Dept, Signature) - Reportee - Manager of Reportee, if applicable - CISO (acknowledgment and follow up)	
Analysis & Compliance - What was the root cause of the incident? - What are the lessons learned? - What are the actions taken?	

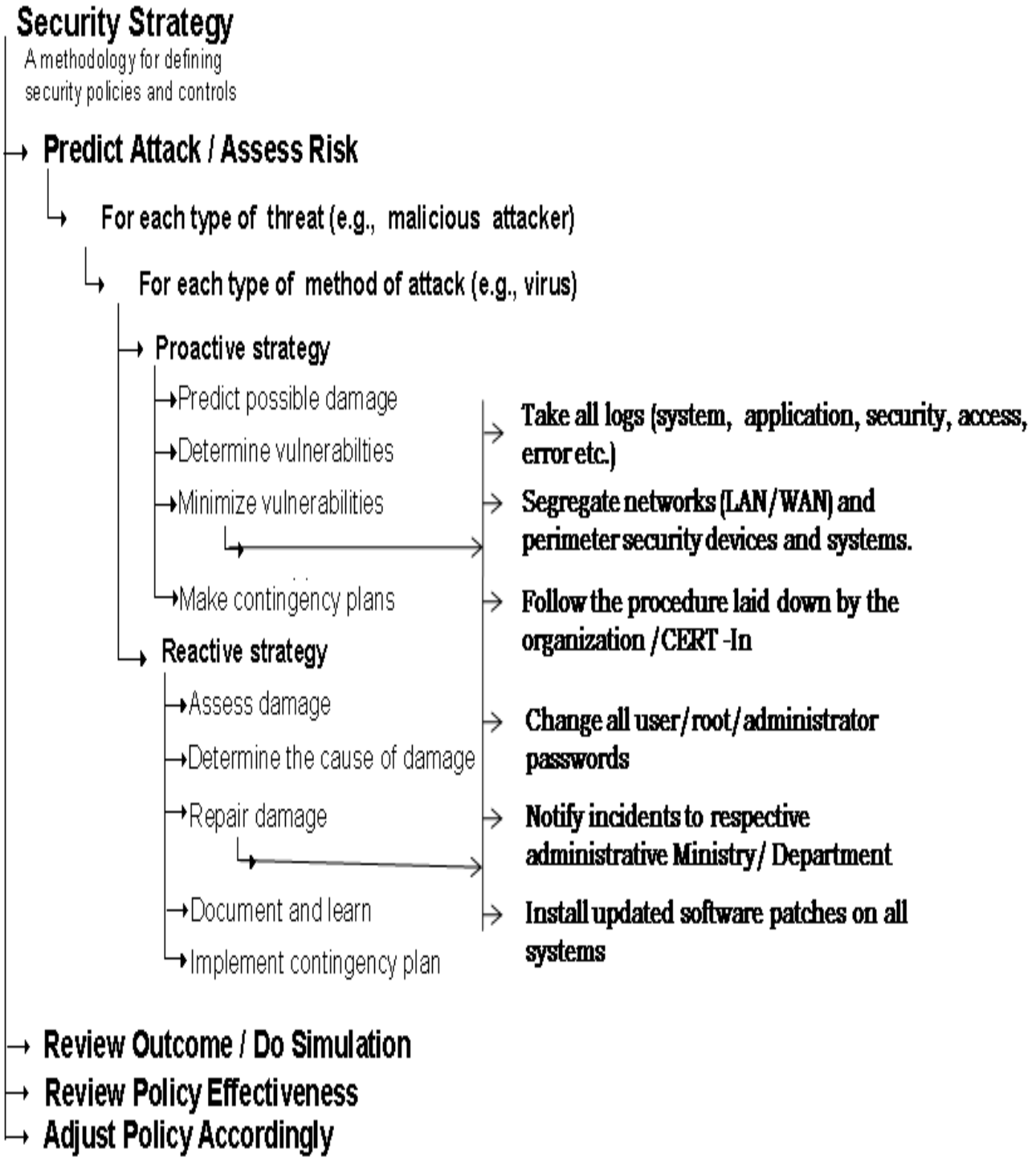
Date **Signature**
CISO

Annexure I
Control Room Details of IT/Security Departments

Primary Contact (BESSEGGEN INFOTECH LLP NOC)		
Name		
Alternate Contact		
Contact Details		

Annexure J

FLOW DIAGRAM FOR IDENTIFICATION OF THREATS AND ACTION REQUIRED BY UTILITIES


Security Strategy
A methodology for defining security policies and controls
Predict Attack / Assess Risk
For each type of threat (e.g., malicious attacker)
For each type of method of attack (e.g., virus)
Proactive strategy
Predict possible damage
Determine vulnerabilties
Minimize vulnerabilities
Make contingency plans
Take all logs (system, application, security, access, error etc.)
Segregate networks (LAN/WAN) and perimeter security devices and systems.
Follow the procedure laid down by the organization /CERT -In
Reactive strategy
Assess damage
Determine the cause of damage
Repair damage
Document and learn
Implement contingency plan
Change all user/root/administrator passwords
Notify incidents to respective administrative Ministry/ Department
Install updated software patches on all systems
Review Outcome / Do Simulation
Review Policy Effectiveness
Adjust Policy Accordingly