# CYBER CRISIS MANAGEMENT PLAN FOR GOVERNMENT OF ASSAM (CCMP)

**DEPARTMENT OF INFORMATION TECHNOLOGY,**

**GOVERNMENT OF ASSAM**

# TABLE OF CONTENTS

# 1. INTRODUCTION

The Cyber Security Policy 2020 of the Government of Assam mandates that State Departments in coordination with Information Technology Department develop, regularly update, maintain, and exercise adaptable cyber incident response plans to address cybersecurity risks to digital information and information infrastructure.

The Cyber Crisis Management Plan (CCMP) provides the strategic framework and guides actions to prepare for, respond to, and begin to coordinate recovery from a cyber incident. It covers different type of cyber crisis, possible targets and related impact, actions and responsibilities of concerned stakeholders, cyber incident response coordination among Departments of State Government, its agencies and Critical Information Infrastructure (CII) organizations to deal with cyber crisis situations.

The motive of Cyber Crisis Management Plan (CCMP) is to provide the State Government with a guideline or foundation for viable handling of Cyber Crisis that may adversely impact Government, Business and Citizen. The Cyber Crisis Management Plan stipulates the actions and processes to be carried out in the event of an attack to safeguard the state government assets and its services.

## 1.1 PURPOSE

- ✓ *To establish the strategic framework and guide actions to prepare for, respond to, and begin to coordinate recovery from a cyber crisis.*
- ✓ *To assist Departments to put in place mechanisms to effectively deal with cyber security crisis and be able to pin point responsibilities and accountabilities.*

# 2. NATURE OF CYBER CRISIS AND CONTINGENCIES

This section identifies different types of threats and crisis that affects specific targets. Impact of such crisis on respective targets and critical business functions and services of the Government of Assam are identified to determine suitable response and mitigation actions.

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

## 2.1 CYBER SECURITY EVENT, INCIDENT AND CRISIS

### *2.1.1 EVENT& INCIDENT*

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

A security incident is defined as an adverse event in an information system and or network that pose 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 system, disruption of data, denial of services/availability, misuse of system resources, computer viruses etc.

### *2.1.2 CYBER SECURITY CRISIS*

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

Incidents are a common thing but managing crisis situations is not an easy task. It requires an organization wide effort that is well integrated, concerted and coordinated. While, most organizations have controls to manage incidents, very few are prepared to deal with crisis like situations and have a well thought out plan.

Very often Government Departments or agencies suffer from cyber security breaches or cyber vulnerabilities due to inadequate cyber security measures, with increasing regulatory and reputational pressure and due to the impacts of cyber breaches, it is increasingly important to prepare the Department/ organization to manage a cyber crisis situation by putting a cyber crisis management plan in place

### *2.1.3 COMPONENTS OF CYBER CRISIS MANAGEMENT PLAN*

Each organization, and the context within which it operates, is unique and there is crisis management strategy thus differs from organization to organization. The CCMP must be developed as per the need and context of the organization Developing a CCMP is not a single person's job, on the contrary, is a collaborative effort across the organization for developing a blue print that Departments can use in a crisis.

**a. CCMP Process to be followed by the Department/s**

i. **Preparation and Readiness:** Involves general preparation and readiness to a broad range of cyber security events. During this phase, roles and responsibilities are defined, procedures defined and tested and employees are trained.

ii. **Detection and Assessment:** Involves monitoring of diverse information sources, discovery of cyber events, reporting from affected departments and an initial assessment of the impact level.

iii. **Business continuity and Recovery:** Includes all response actions required to mitigate impact, containment and eradication, root cause analysis and investigation.

iv. **Post Event Activity:** Covering lessons learned analysis, review of processes and procedures recommending changes to continuously improve the cyber crisis management plan.

| Phase | Objectives |
|---|---|
| Preparation and Readiness | • Define Role and Responsibilities<br>• Document Procedures and Test |

| | |
|---|---|
| | • Train Employees and Staff<br>• Cyber security awareness program |
| Detection and Assessment | • Monitor Information Source,<br>• log management & review,<br>• Pen testing,<br>• Internal/External audit<br>• Detect and Recognize cyber security events |
| Business continuity and Recovery | • Conduct forensic analysis<br>• Containment and Eradication<br>• Restore operation to normal |
| Post Event Activity | • Post-event analysis<br>• Continuous improvement in protective measures |

**b. Structure of Crisis Management Plan for Department/s**

Crisis management is a process designed to prevent or lessen the damage a crisis can inflict on an organization and its stakeholders. As a process crisis management is not just one thing. Departments can divide crisis management into three phases:

a. *Pre-Crisis*
b. *Crisis response*
c. *Post crisis*

The Pre-crisis phase is concerned with prevention and preparation. The Crisis response phase is when management must actually respond to a crisis. The Post crisis phase looks for ways to better prepare for the nest crisis and fulfils commitments made during the crisis phase including follow-up information.

The structure of Crisis Management Plan for countering Cyber crisis has five sections dealing with the following:

i. *Concept of Crisis Management Plan*
ii. *Nature of cyber crisis*
iii. *Incident prevention measures*
iv. *Crisis recognition mitigation and management*
v. *Incident closure and information sharing*

**c. Crisis management & Emergency response**

It is a set of actions aimed at rapid response & remedial measures and recovery & restoration of normalcy in the event of a build-up or emergence of a crisis.

The action includes:

i. *Containment of crisis*

ii. *Communication to all concerned and*
iii. *Coordination of efforts*
iv. *Implementation of mitigation measures*

**d. Categories of Cyber Crisis:**

Targeted cyber-attacks on infrastructure of one or more critical sectors either individually or simultaneously, may result in significant/complete breakdown of services essential to the life of the citizens including but not limited to Finance, Defense, Transport, Energy, Communication or critical sector. These events may lead to National Crisis. Cyber-attack may originate from places within the country or anywhere outside the country. Attack source may spread geographically across the globe.

Cyber-attacks may be triggered on

- *Individual systems*
- *Multiple systems / networks, single or multiple organizations*
- *States and entire Nation*

## 2.2TYPES OF CYBER SECURITY INCIDENTS

Any real or suspected adverse event in relation to 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 activities such as:

- *Attempts (either failed or successful) to gain unauthorized access to a system or its data.*
- *Unwanted disruption or denial of service*
- *The unauthorized use of a system for the processing or storage of data*
- *Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction or consent.*

## 2.3NATURE OF CYBER CRISIS AND CONTINGENCIES

| TYPE OF CRISIS | POSSIBLE TARGETS | RELATED IMPACT |
|---|---|---|
| **1. Target Scanning, Probing and Reconnaissance of** | • Sensitive Government and Critical Information | • Pre-cursor to hacking and focused attack leading to |

| | | |
|---|---|---|
| **Network and IT Infrastructure** | Infrastructure<br><br>• Infrastructure at Data Centres and Network Operation Centres<br><br>○ Routers, Switches, Data-base and DNS Servers<br>○ Web Portals | cyber crisis<br><br>• Total/partial disruption of e-governance and Public services. |
| **2. Large scale defacement and semantic attacks on websites**<br><br>• *Website defacement is when a Defacer breaks into a web server and alters the contents of the hosted website*<br><br>• *Attackers change the content of a web page subtly, so that the alteration is not immediately apparent. As a result, false information is disseminated* | • High profile websites such as CM Portal, Government information dissemination websites of departments, Public utility services such as Power, Police etc.<br><br>• Key economic transaction websites such as Banks/Financial Institutions (FI), Insurance, Online transactions etc. | • Huge embarrassment for the State<br><br>• Total/partial disruption of services/activities<br><br>• Dissemination of false/misleading information<br><br>• Monetary loss, damage of reputation, loss of image etc. |
| **3. Malicious Code attacks (virus /worm / Trojans / Botnets)**<br><br>*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, worms, trojans, Ransomware, Crypto miner, spyware, adware and Bots*<br><br>***3.1 Malware affecting ICS systems***<br><br>*Sophisticated malware such as Stuxnet/Industroyer targeting* | • Large & key state databases such as citizen data base, plan information, tax information network etc.<br><br>• Users<br><br>• Supervisory Control and Data Acquisition systems (SCADA) and Centralized as well as | • Hanging of Complex system<br><br>• Partial or No response from computer system<br><br>• Total/partial corruption of data bases<br><br>• Monetary loss, damage of reputation, loss of image etc.<br><br>• Data Theft, Identity Theft and possible espionage |

| | | |
|---|---|---|
| *industrial Control Systems that are part of networks separated through 'airgap' from regular internet facing networks* | distributed control systems of power, petroleum, transport, refineries etc. and all process industries | • Total/partial disruption services/activities in one or more critical sectors such as energy, transport, telecommunications, emergency services etc. |
| ***3.2 Malware affecting Mobile devices***<br>*Malicious code and malicious applications (apps) affecting operating systems/platforms used for mobile devices such as Android, iOS, Symbian, Window Mobile etc.* | • Mobile devices using affected Operating System and connected computer systems | • Unauthorized disclosure of user's data and contact details |
| ***3.3 Malware affecting IoT devices***<br>*Compromised IoT devices such as cameras, routers, DVRs, wearables, IoT and other embedded technologies, infected with malware like Mirai* | • Sensitive Government and Critical Information Infrastructure<br>• Users | • Total / partial disruption of services / activities in one or more critical sectors such as energy, transport, telecommunications, emergency services etc.<br>• Data theft, possible espionage |
| **4. Attack on Financial sectors and Digital payment ecosystem** | • Digital Payment instruments<br>• IT infrastructure of financial institutions, depositors, Insurance etc.<br>• SWIFT network, ATM switch | • Financial and customer data breach<br>• Financial frauds<br>• Decline in user trust and confidence in digital ecosystem<br>• Loss of reputation |
| **5. Large scale SPAM attack**<br>*Spamming is the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages. SPAM mails may also contain* | • ISP network<br>• Key Government Networks<br>• Large Corporate Network | • Significant slowdown in network performance<br>• Total/partial disruption of E-mail communication services<br>• Severe drain on network |

| | | |
|---|---|---|
| *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.* | | resources<br>• Significant reduction of access to critical network services<br>• Increased possibility of virus/worm infection. |
| **6. Identity Theft Attack**<br>***6.1 Large scale spoofing***<br>*Spoofing is an attack aimed at 'identity theft' in which one person or program successfully masquerades as another falsifying data and thereby gaining an illegitimate advantage*<br>***6.2 Social Engineering***<br>*Art of manipulating people into performing disclosure actions or divulging confidential information*<br>• ***Phishing attacks***<br>*Phishing is an attack aimed at stealing the sensitive personal data that can lead to committing online economic frauds. Phishing attempt to fraudulently acquire sensitive information, such as usernames, passwords, banking details by masquerading as a trustworthy entity in an electronic communication*<br>• ***Vishing attacks***<br>*Vishing is a combination of 'voice' and phishing. It is the practice of using social* | • Senior officials in Government, corporate and key economic installations<br>• Individual users such as senior officials<br>• Network/System/Database Administrators<br>• Key Government organizations and Government service providers | • Increased possibility of identity theft and root privileges compromise leading to penetration into sensitive IT systems and Databases<br>• Loss of sensitive data, monetary loss and loss of image<br>• Loss of sensitive data, monetary loss and loss of image<br>• Financial frauds<br>• Loss of user credentials<br>• Monetary Loss |

| | | |
|---|---|---|
| *engineering over the telephone system, most often using feature facilities by Voice over IP (VoIP), to gain access to private personal and financial information from the public for the purpose of financial reward.*<br><br>• ***SMSihing attacks***<br>*These are phishing attacks launched through SMS service via mobile phones* | | |
| **7. Denial of Service (DoS) attacks and Distributed Denial of Service (DDoS) attacks**<br><br>• *DoS is an attempt to make a computer resource unavailable to its intended users*<br><br>• *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*<br><br>• *DDoS attacks are launched through a Botnet which is a network of compromised computer systems called 'Bots'*<br><br>• *Reflection based Distributed Denial of Service (RDoS) Attack* | • Water Supply<br><br>• Hospital/Ambulance<br><br>• Police<br><br>• Transport<br><br>• Mission critical systems<br><br>• Supervisory control and Data Acquisition (SCADA) System<br><br>• Web-based key economic targets such as banks/FIs, Insurance, online reservations etc.<br><br>• Government Organizations and Web-based key economic targets | • Failed/aborted mission<br><br>• Possible damage to and/or property<br><br>• Total/partial disruption of services for prolong periods<br><br>• Monetary loss damage to reputation, loss of image etc. |
| **8. Domain Name Server (DNS) attacks**<br><br>• *DNS Hijacking refers to* | • Country level domain registry systems (NIXI ".IN" registry)<br><br>• International gateway or | • Total/partial disruption of services for prolong periods<br><br>• Monetary loss damage to |

| | | |
|---|---|---|
| *modification of DNS records with the intention of redirecting the victim to malicious domains/IPs*<br><br>• *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*<br><br>• *DNS cache poisoning involves corrupting the DNS server's cache with fake values causing the name server to return an incorrect result. This may result in traffic being diverted to malicious systems* | ISP/Large corporate server systems<br><br>• E-commerce<br><br>• Business and banking application<br><br>• Individual users/home routers<br><br>• E-Governance<br><br>• Government Organizations | reputation, loss of image etc. |
| **9. Application Level Attacks**<br><br>*Exploitation of inherent vulnerabilities in the code of application software such as web/mail/databases* | • e-Governance<br><br>• e-Commerce<br><br>• Business and Banking Applications | • Data manipulation which may result in huge economic fallouts including monetary as well as business loss<br><br>• Disruption of services<br><br>• Loss of sensitive data and loss of image and trust |
| **10. Attacks on Trusted infrastructure**<br><br>*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* | • SSL Servers<br><br>• Certifying Authorities<br><br>• Authentication infrastructures<br><br>• Secure Communication Protocols and Systems<br><br>• Public Key Infrastructure | • Blocking of Handshaking resulting in disruption of financial and authentication services<br><br>• Large scale man-in-the middle attacks resulting in disclosure of sensitive data and user information<br><br>• Redirection of users to fake websites with dubious authentication |

| | | |
|---|---|---|
| *trust of users and misuse of authentication mechanism*<br>• *Denial of Service attacks*<br>• *Rogue certificates* | | • Signing malicious code to make it appear as legitimate<br>• Large scale cyber espionage |
| **11. Compound Attacks**<br>*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.* | • Public utility services<br>• Fire<br>• Water supply<br>• Hospitals/Ambulance<br>• Police<br>• Transport<br>• Web based economic targets<br>• Large & key databases<br>• Mission Critical systems<br>• International gateway/ISPs | • Total/partial disruption of services/activities<br>• Significant slowdown in disaster/emergency response capabilities that can magnify the impact of a physical attack<br>• Huge economic fallouts<br>• Damage to reputation, loss of image etc. |
| **12. Routing Attacks**<br>*Routers are the controllers of any network, they connect different network to internet. Routers works on Layer 3 device and it works on logical IP address. Routing disruption could lead to unavailability of network, websites, Internet.*<br>***BGP (Border Gateway Protocols)***<br>*BGP is primary exterior routing protocol used to route traffic between different autonomous system.*<br>*BGP Route Hijacking: The attacker announces the more specific prefixes of intended target network to reroute traffic itself. Once successful, the hijacker could then perform Man-in-the-middle attacks, eavesdropping, modify or block the traffic.*<br>***DoS***<br>*BGP Denial of Service, A* | • ISP gateways/Routers<br>• ISP Networks<br>• Large Corporate Networks.<br>• Wifi Routers<br>• Business & Banking Networks<br>• Sensitive Government and Critical Information Infrastructure<br>• E Commerce Networks | • Total/Partial disruption of Internet.<br>• Illegal diversion of Internet traffic.<br>• Loss of Sensitive personal data.<br>• Breakdown of online activities.<br>• Monetary Loss, damage of reputation, loss of Image<br>• Huge economic fallouts including monetary as well as business loss.<br>• Disruption of Critical Websites.<br>• Complete outage on corporate data center. |

| | | |
|---|---|---|
| *compromised router in the network sends malicious BGP traffic to another router. The target router stops processingvalid BGP updates due to excessive loads.* | | |
| **13. RF(Radio Frequency) Attacks**<br><br>*Physical devices like Antennas to direct focused beam which can be modulated from a distance to cause RF jamming of communication systems including wireless networks leading to attacks such as Denial of Service.* | • Satellite Network Communication System<br><br>• Mobile networks.<br><br>• Wireless Networks Wi-Fi, Wi-MAX<br><br>• | • Total disruption in the Wireless, Mobile and Satellite Networks.<br><br>• Connectivity between Phones, PC through Bluetooth could be disturbed.<br><br>• RF jamming tools may use very high energy sufficient to break down the electronics and make it to malfunction totally |
| **14. Client-Side attacks**<br><br>*Client-side vulnerable software like MS Office, Abode reader, Java browser plugins etc, Sophisticated tool kit with various exploits available for compromising client system.Attacks targeting social network platform for malicious activities such as identity theft, fake social accounts, fake news, command & control of Botnets.* | • Individual Users<br><br>• Corporate<br><br>• Political Leader | • Data Leakage<br><br>• Use system as bot or launch pad for launching further attacks.<br><br>• Loss of sensitive personal data, loss of image and trust. |
| **15. Threats due to Emerging technologies (IoT, Big Data, Artificial Intelligence)**<br><br>*The extraordinary capabilities of these emerging technologies have extended and endowed cyberspace with capabilities beyond the hyper-connectivity of the* | • Government Organizations<br><br>• Critical Sector Organizations<br><br>• Corporate Sector<br><br>• Cloud service providers<br><br>• Start-up contributing | • Cyber espionage<br><br>• Attack on critical Infrastructure<br><br>• Disclosure of sensitive information. |

| | | |
|---|---|---|
| *Internet itself.*<br>*The expanded network infrastructure and increased number of connected devices introduce more vulnerabilities to intrusions. Furthermore, the enormous volumes of data processed and shared among the vast numbers of Internet-connected nodes become increasingly likely targets of exploitation and distortion.* | | |

## 2.4RANSOMWARE

Ransomware is malware that employs encryption to hold a victim's information at ransom. A ransom is then demanded to provide access. Ransomware is often designed to spread across a network and target database and file servers, and can thus quickly paralyze an entire organization.

It is recommended that backing up important data is the single most effective way of recovering from a ransomware infection. however. backup files should be appropriately protected and stored offline or out-of-band, so they can't be targeted by attackers.

***Do's and Don'ts for the Departments***

- *Disconnect and isolate your system.*
- *Maintain a regular backup of the system.*
- *Keep your software up to date to avoid security bugs in outdated software.*
- *Make use of threat intelligence.*
- *Use strong passwords.*
- *Monitor the network and devices for any suspicious activity.*
- *If a lot is at stake, disable remote services.*
- *Encrypt everything possible.*
- *Many ransomware variants take advantage of (RDP) port 3389 and Server Message Block (SMB) port 445. Need to provide sufficient access on need to know basis if not using, need to disable the service.*
- *If it comes to that, avoid paying the ransom at all costs.*
- *An Intrusion Detection System (IDS) looks for malicious activity by comparing network traffic logs to signatures that detect known malicious activity*

***IT Department, Government of Assam, Assam Police, Cert-In etc. should be informed immediately once such attacks are identified by the Department in its machine***

**Ransomware Detection and Analysis**

1. Determine the systems were impacted, and immediately isolate them.

    - If several systems or subnets appear impacted, take the network offline at the switch level. It may not be feasible to disconnect individual systems during an incident.

    - If taking the network temporarily offline is not immediately possible, locate the network (e.g., Ethernet) cable and unplug affected devices from the network or remove them from Wi-Fi to contain the infection.

    - After an initial compromise, malicious actors may monitor organization's activity or communications to understand if their actions have been detected. Be sure to isolate systems in acoordinated manner and use out-of-band communication methods like phone calls or other means to avoid tipping off attackers that they have been discovered and that mitigation actions are being undertaken.

    - Note: Step 2 will prevent you from maintaining ransomware infection artifacts and potential evidence stored in volatile memory. It should be carried out only if it is not possible to temporarily shut down the network or disconnect affected hosts from the network using other means.

2. Only in the event are unable to disconnect devices from the network, power them down to avoid further spread of the ransomware infection.

3. Triage impacted systems for restoration and recovery.Identify and prioritize critical systems for restoration, and confirm the nature of data housed on impacted systems.Prioritize restoration and recovery based on a predefined critical asset list that includes information systems critical for health and safety, revenue generation, or other critical services,as well as systems they depend on.

4. Using the contact information, engage internal and external teams and stakeholders with an understanding of what they can provide to help you mitigate, respond to, and recover fromthe incident. Share the information have at your disposal to receive the most timely and relevant assistance. Keep management and senior leaders informed via regular updates as the situation develops. Relevant stakeholders may include your IT department, CERT-in, and departmental or elected leaders.

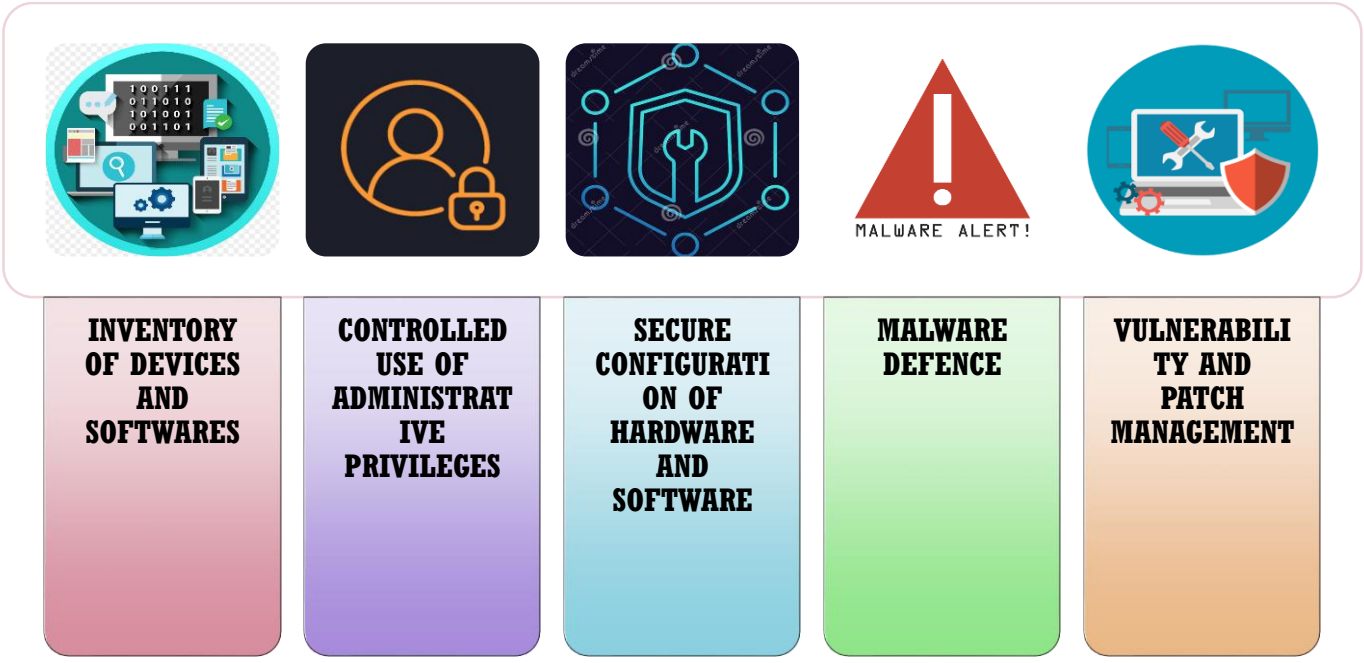
5. Take a system image and memory capture of a sample of affected devices (e.g., workstations and servers). Additionally, collect any relevant logs as well as samples of any "precursor" malware binaries and associated observables or indicators of compromise (e.g., suspected command and control IP addresses, suspicious registry entries, or other relevant files detected). Take care to preserve evidence that is highly volatile in nature—or limited in retention—to prevent loss or tampering (e.g., system memory, Windows Security logs, data in firewall log buffers).

6. Consult law enforcement regarding possible decryptors available.

7. Conduct extended analysis to identify outside-in and inside-out persistence mechanisms. Outside-in persistence may include authenticated access to external systems via rogue accounts, backdoors on perimeter systems, exploitation of external vulnerabilities, etc. Inside-out persistence may include malware implants on the internal network or a variety of living-off-the-land style modifications (e.g., use of commercial penetration testing tools like Cobalt Strike; use of PsTools suite, including PsExec, to remotely install and control malware and gather information regarding—or perform remote management of—Windows systems; use ofPowerShell scripts).Identification may involve deployment of endpoint detection and response solutions, audits of local and domain accounts, examination of data found in centralized logging systems, or deeper forensic analysis of specific systems once movement within the environment has been mapped out.

## 3. BUILDING CYBER SECURITY CAPABILITIES

All organizations should develop culture of cyber security among themselves in every aspect of their functionality. The Cyber Security Must Haves indicates the basic cyber security fundamentals applicable to all the organizations. By developing these Must Haves, organizations can defend against the most common form of basic cyber attacks originating from the internet.




### 3.1 PRIMARY CONTROLS

#### *3.1.1INVENTORY OF DEVICES AND SOFTWARE*

- All Departments & its subordinate organizations shall mandatorily maintain inventory of all hardware and software assets procured over the years.
- Maintain an asset inventory of all systems connected to the network and the network devices themselves.
- The asset inventory must also include data on whether the device is portable.

- Develop an inventory of information assets that identifies their critical information and maps critical information to the hardware assets (including servers, workstations, and laptops) on which it is located.

- Organizations and individual responsible for each information asset should be identified, recorded, and tracked.

- Ensure that network inventory monitoring tools are operational and continuously monitoring, keeping the asset inventory up to date on a real-time basis, looking for deviations from the expected inventory of assets on the network, and alerting security and/or operations personnel when deviations are discovered.

- Secure the asset inventory database and related systems. Limit access to these systems to authorized personnel only, and carefully log all such access.

- Use Network Access Control technology to authenticate and authorize devices before allowing them on the network.

- Devise a list of authorized software that is required for each type of system, including servers, workstations, and laptops of various kinds and uses.

- Organizations shall not allow pirated and unknown software for installation in their official system and also follow due protocols whenever hardware needs to be disposed due to end of life of the product or change of the product for newer version.

- Deploy application white listing technology that allows systems to run only approved software and prevents execution of all other software on the system, based on an automatically generated list of valid software from a representative sample machine.

### *3.1.2 CONTROLLED USE OF ADMINISTRATIVE PRIVILEDGES*

- The Department through its Information Steering Committee shall decide the administrative privileges for their ICT System, for application/software, devices and network etc.

- Access to the resources should be provided on need to know basis.

- Required privileges granted role wise must be documented and work out mechanism for monitoring the logs of administrative privilege.

- Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to a difficult-to-guess value.

- Passwords for all systems should be stored in a well-hashed or encrypted format

- Ensure that administrator accounts are used only for system administration activities, and not for reading e-mail, composing documents, or surfing the Internet.

- Require that administrators establish unique, different passwords for their administrator and non-administrative accounts.

- Access to a machine (either remotely or locally) should be blocked for administrator-level accounts.

- If services are outsourced to third parties, language should be included in the contracts to ensure that they properly protect and control administrative access. It should be validated that they are not sharing passwords and have accountability to hold administrators liable for their actions.

- Segregate administrator accounts based on defined roles.

- Configure systems to issue a log entry and alert when an account is added to or removed.

- Inventory all administrative accounts and validate that each person with administrative privileges on desktops, laptops, and servers is authorized.

- Audit the use of administrative privileged functions and monitor for anomalous behavior.

- Configure all administrative-level accounts to require regular password changes on a frequent interval of no longer than 180 days.

- Ensure that all service accounts have long and difficult-to-guess passwords that are changed on a periodic basis at a frequent interval of no longer than annually.

- Configure operating systems so that passwords cannot be re-used.

- All administrative access must use two-factor authentication where possible.

### *3.1.3 SECURE CONFIGURATIONS FOR HARDWARE AND SOFTWARE*

- Implement and manage secure configuration of hardware and software installed within network.
- Implement strict configuration rules and change control/approval process.
- Patching and updates of firmware and software must be ensured.
- Secure configuration control reduces the attack surface by only operating services and functionalities which are required by organizations in secure fashion.
- Default configurations of hardware and software must be changed for ensuring security.
- Allow what is necessary and remove/block unnecessary ports & services.
- Run a stable version of software and make sure it is fully patched. Remove outdated or older software from the system.
- All remote administration of servers, workstation, network devices, and similar equipment should be done over secure channels.
- Strict configuration management should be followed, building a secure image that is used to build all new systems that are deployed.
- Systems should be hardened, including underlying operating system and the applications installed on the system.
- Ensure contracts to buy systems include that the systems are configured securely out of the box using standardized images.
- The master images must be stored on securely configured servers, with integrity checking tools and change management to ensure that only authorized changes to the images are possible.
- Utilize file integrity checking tools on at least a weekly basis to ensure that critical system files (including sensitive system and application executables, libraries, and configurations) have not been altered.

### *3.1.4 MALWARE DEFENCE*

- Employ automated tools to continuously monitor workstations, servers, and mobile devices for active, up-to-date anti-malware protection with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality.

- Employ anti-malware software and signature auto update features or have administrators manually push updates to all machines on a daily basis.

- Configure systems so that they conduct an automated anti-malware scan of removable media when it is inserted.

- All attachments entering an e-mail gateway should be scanned and blocked if they contain malicious code or, where appropriate, file types unneeded for the business.

- All malware detection events should be sent to anti-malware event log servers and reviewed frequently.

- Configure laptops, workstations, and servers so that they will not auto-run content from USB tokens (i.e., "thumb drives"), USB hard drives, CDs/DVDs, Firewire devices, external serial advanced technology attachment devices, mounted network shares, or other removable media.

- Deploy network access control tools to verify security configuration and patch-level compliance before granting access to a network.

### *3.1.5 VULNERABILITY AND PATCH MANAGEMENT*

- Run automated vulnerability scanning tools against all systems on the network at least quarterly. Any vulnerability identified should be remediated in a timely manner, with critical vulnerabilities fixed or temporarily mitigated within 48 hours.

- Critical patches must be evaluated in a test environment before being pushed into production.

- Compare the results from back-to-back vulnerability scans to verify that vulnerabilities were addressed either by patching, implementing a compensating control, or documenting and accepting a reasonable business risk.

- During a vulnerability scan, compare services (ports) that are listening on each machine against a list of authorized services.

- Event logs should be correlated with information from vulnerability scans.

- Deploy automated patch management tools and software update tools for operating system and third-party software on all systems.

- Ensure that all vulnerability scanning is performed in authenticated mode either with agents running locally on each end system to analyze the security configuration or with remote scanners that are given administrative rights on the system being tested.

## 3.2 SUB CONTROLS ALIGNED WITH PRIMARY CONTROLS

### *3.2.1 INVENTORY OF DEVICES AND SOFTWARE*

**INVENTORY OF DEVICE**

Developing, documenting, and maintaining a current inventory of all systems including user system, network device, Router, Switch, Firewall, printers, camera, any biometric device etc.

**INVENTORY OF SOFTWARE**

Creating & Maintaining an inventory of all applications that are active/inactive for the department, all the purchased software that used by department along with details of license.This would be helpful for AMC management and proper authentication & authorization.

**INVENTORY OF VIRTUAL ASSET**

The virtual asset service providers, virtual asset exchange providers and custodian wallet providers (as defined by Ministry of Finance from time to time) shall mandatorily maintain all information obtained as part of Know Your Customer (KYC) and records of financial transactions for a period of five years so as to ensure cyber security in the area of payments and financial markets for citizens while protecting their data,

fundamental rights and economic freedom in view of the growth of virtual assets. For more information on notification and guidelines, kindly refer @The Reserve Bank of India (RBI) Directions 2016 /Securities and Exchange Board of India (SEBI) circular dated April 24, 2020 / Department of Telecom (DoT) notice September 21, 2021 mandated procedures as amended from time to time.

### *3.2.2 CONTROLLED USE OF ADMINISTRATIVE PRIVILEGES*

**STRONG AUTHENTICATION**

Verifying the identity of users, devices, or other entities through rigorous means (e.g. multi-factor authentication/ biometric authentication) before granting access.

**SECURE ADMINISTRATION**

Performing administrative tasks in a secure manner, using secure protocols. HTTPS instead of HTTP, SSH instead of telnet, FTPS, Secure IPsec tunnel etc.

**LEAST PRIVILEGE, ZERO TRUST & NEED TO KNOW**

The principle of least privilege specifies that individuals or processes are granted only the privileges they need to perform their assigned tasks or functions, but no more than the required access. Admin privilege must be assigned the individual who must need the access to perform his/her duty. Designing the security architecture such that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.

No one/ no device could be trusted until unless they proved who/what they are and once identified they must be given access depending on what they need to know, need to work basis.

### *3.2.3 SECURE CONFIGURATIONS FOR HARDWARE AND SOFTWARE*

***BACKUP AND RECOVERY***

Keeping copies of configuration and data, as needed, to allow for the quick restoration of service in the event of malicious incidents, system failures, or corruption.

**CONTROL OF UNUSED PORTS, SERVICES, DEFAULT CONFIGURATION ON DEVICE:**

Unused ports/services must be disabled on the web server, unused ports must be shut down on network devices. Default configuration must be modified, default credential must be deleted.

**TIME SYNCHRONIZATION**

Coordinating clocks on all systems (e.g. servers, workstations, network devices) to enable accurate comparison of timestamps between systems. This is very important for auditing and accounting and as well as in case of Incident Management.

**EMAIL & WEB BROWSER PROTECTION**

Ensuring that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor. Uninstall or disable any unauthorized browser or email client plugins or add-on applications. Ensuring that only authorized scripting languages are able to run in all web browsers and email clients. Enforcing network-based URL filters that limit a system's ability to connect to websites not approved by the organization.

**DATA PROTECTION**

Data must be kept in secure while in use, in transits and in rest. CIA (Confidentiality, Integrity, Availability) triad must keep in mid while protecting the data. Also personal data must be kept in private and only agreed disclosure of such data may be disclosed with proper consent.

**WIRELESS ACCESS CONTROL**

Wireless users must be authenticated through LEAP/PEAP protocol for Organization users and assigned them to work defined VLAN once they authenticated. Guest users must be assigned to a guest VLAN with very limited access.

**ACCOUNT MANAGEMENT**

Account management is key for Security posture, as people stay longer in organization, their access getting increased day by day as they would be added in multiple groups depending on their task and activities. So time to time it should be mandatory to review

the access and remove unnecessary access. Also access must be revoked as soon as someone leave the organization.

**RESILIENCE**

Ensuring that systems, services, and protections maintain acceptable performance under adverse conditions. Monitoring and maintenance must be proper with coordination.

### *3.2.4 MALWARE DEFENCE*

**MALWARE DEFENSE**

Block malicious code from tampering with system settings or contents, capturing sensitive data, or spreading: Use automated anti-virus and anti-spyware software to continuously monitor and protect workstations, servers, and mobile devices.

**ENTERPRISE THREAT INTELLIGENCE**

Obtaining threat intelligence from private and government sources and implementing mitigations for the identified risks arising from APT(Advance persistent Threat), malware, virus, worms, SQL injection, XSS script, Zero day exploit, DNS tunneling, Business email compromise, Secure quantum communications, Cyber autonomy and automation, Internet of things (IoT) and cyber physical security etc.

**INCIDENT MANAGEMENT**

An incident management process shall be established, documented, implemented and maintained by the Departments and shall include security Incident and weakness identification, reporting, recording, analysis, response, recovery and mitigation procedures. Roles and responsibilities of all the stakeholders of the incident management process shall be defined.

Incident management team shall be established to take all incident related decisions. A communication channel shall be set up with internal parties and external organizations

**PENETRATION TEST AND SYSTEM AUDIT**

The IT infrastructure should be subject to configuration review (vulnerability assessment/penetration tests) against different cyber threat, attacks on a periodic basis. Regular scheduled assessments, such as internal and external vulnerability scans should be conducted for the IT Infrastructure including but not limited to software,

applications, server, network, database, operating system, wireless devices, and other network equipment.

Frequency of conducting vulnerability assessment shall depend upon the criticality of the Information Asset (application, software, database, operating system, network devices and wireless networks). All Internet facing applications shall undergo vulnerability assessments before deployment in the production environment.

**DEFENSE IN DEPTH**

Defense in depth must be exercised through multiple layers as applicable, as an example Web application firewall for deep packet inspection for code validation, Layer 3 firewall, VPN concentration services, IPS/IDS, proxy services, router. Switch should have proper ACL/limit Mac address per port, so this would ensure multiple level of security checks.

**VPN server**

Data center providers, Cloud service provider, VPN provider must ensure accurate information of customers, members, assets (assigned IP, System, hiring, on boarding etc) . Providers must do due diligence, due care and take complete accountability and must maintain the below mentioned data for five years.

a. Validated names of subscribers/customers hiring the services
b. Period of hire including dates
c. IPs allotted to / being used by the members
d. Email address and IP address and time stamp used at the time of registration / on-boarding
e. Purpose for hiring services
f. Validated address and contact numbers
g. Ownership pattern of the subscribers / customers hiring services

### *3.2.5VULNERABILITY AND PATCH MANAGEMENT*

**APPLICATION SECURITY**

Software applications are complex and can be vulnerable to a wide variety of security issues. Possible issues range from bad code and security misconfigurations to authorization failure. SecDevOps is a new movement that merges security, development, and operations so that they work together to achieve a common goal by making improvements in their processes, tooling and team collaborations. SDLC cycle or OWASP guidelines should be followed in all the stages of Software development, testing, deployment etc. Software versioning is a must for any changes affected.

**CONFIGURATION MANAGEMENT**

Implementing a formal plan for documenting, managing changes to the environment, and monitoring for deviations, preferably automated. Revision control would be helpful to rollback in previously working condition in case of system anomalies.

**PATCH MANAGEMENT**

Identifying, acquiring, installing, and verifying patches for products and systems. Before installing the patches in production, test must be done in test servers. CVE report shall be checked periodically and supplier must be made accountable for effective patch management.

**CENTRAL LOG MANAGEMENT WITH ANALYSIS**

Collecting, storing, and analyzing the logs, where the collection and storage are designed to facilitate data fusion and the security analysis aids in discovery and response to malicious activity. Central log management system must be kept in place to collect logs from all the device and web application traffic.

**AUDITING AND ACCOUNTING**

Capturing business records, including logs and making them available for auditing and accounting as required. Design of the auditing system should take insider threat into consideration, including separation of duties violation tracking, such that insider abuse or misuse can be detected.

**POLICY ENFORCEMENT**

Consistently applying security protections and other policies, procedures, guidelines are independent of the communication mechanism, forwarding path, or endpoints used.

**SECURITY AWARENESS TRAINING PROGRAM**

Security awareness training and certification must kept mandatory to complete, Training program must be useful for user and that must be acceptable for use. Reward/Bonus must be given for successful completion.

## 4. ROLES AND RESPONSIBILITIES

### STATE CRISIS MANAGEMENT COMMITTEE

**Chairperson:** Chief Secretary Government of Assam

**Members:**

- *Senior most Secretary, IT Department, Government of Assam, Member Convener*
- *Senior most Secretary, Home & Political Department, Government of Assam*
- *DGP, Assam Police, Government of Assam*
- *Representative from NCIIPC / CERT-In, GoI.*

### DEPARTMENT/ORGANISATIONAL LEVEL

**Chairperson:** Senior most Secretary of the Department

**Members:**

- *Chief Information Security Officer (CISO) of the Department.*
- *Nodal officer or Head of the IT Project of the Department.*
- *Financial Advisor to the Department.*
- *Technical in-charges (System, Network and Database Administrator etc.).*

| SL No | Description of Control | Roles and Responsibilities |
|---|---|---|
| 1 | Reporting Structure | Each Department should utilize an organization chart that depicts the reporting structure of information security Team structure when assigning specific responsibilities for the security of IT systems and data. Each Department shall maintain documentation regarding specific roles and responsibilities relating to information security. |
| 2 | Information Security Program | Each Department shall establish, document, implement, and maintain its IT security program appropriate to its business and technology environment in compliance with this Standard. In addition, because resources that can reasonably be committed to protecting IT systems are limited, each Department must implement its information security program in a manner commensurate with sensitivity and risk. |
| 3 | CISO | CISO is responsible for the security of the Department's IT systems and data.<br>Responsibilities include the following: |

**Cyber security Actionable**: All service providers, intermediaries, data centres, body corporate and Government organisations must perform time to time recommended activity from cert.in .

It is now been mandated to report any cyber security incident to Cert.in within six hours of Incident detected and it is for across the entire department, organisation, PSU, service providers, data center etc.

**SPOC contact details**: Department/Organisation should nominate CISO who shall act as a Single point of contact (SPOC) for co-ordinating all cyber security related activities and provide the contact details to the IT department for onwards submission to Cert-in as well. The IT department has already sent the notification to nominate and provide the contact details of CISO. That CISO would be the point of contact to Cert.in on behalf of the department.

CISO must ensure to collect and share all SPOC details for their underlying organisation, Cloud service provider, ISP, Intermediaries, data center etc.

**Information Asset Tracking:** Data center providers, Cloud service provider, VPN provider must ensure accurate information of customers, members, assets (assigned IP, System, hiring, on boarding etc) . Providers must do due diligence, due care and take complete accountability and must maintain the data for five years.

- **If any department/PSU/other entities of Government of Assam are utilising the cloud service from any data centres other than AMTRON data Centre, SDC, NIC or taking network services from various ISPs should enforce Cert-in recommendation with respective services providers accordingly.**

- Ensure that Department information security program is maintained, that is sufficient to protect the Department's IT systems, and that is documented and effectively communicated.
- Review and approve the Department's Business Impact Analyses (BIAs), Risk Assessments (RAs), and Continuity of Operations Plan (COOP), to include an IT Disaster Recovery Plan, if applicable.
- Ensure compliance is maintained with the current version of the IT Security Audit Standard This compliance must include.
- Ensure a program of information security safeguards is established.

| | | |
|---|---|---|
| | | • Ensure an information security awareness and training program is established.<br>• Provide the resources to enable employees to carry out their responsibilities for securing IT systems and data.<br>• Verify and validate that all Department IT systems and data are classified for sensitivity.<br>• Implement and maintain the appropriate balance of preventative, detective and corrective controls for Department IT systems commensurate with data sensitivity, risk and systems criticality. |
| 4 | System Owner/Data Owner Department Nodal Officer | The System Owner is the Department Nodal Officer IT responsible for having an IT system operated and maintained. With respect to IT security, the System Owner's responsibilities include the following:<br>• Require that the IT system users complete any system unique security training prior to, or as soon as practicable after, receiving access to the system, and no less than annually, thereafter.<br>• Manage system risk and developing any additional information security policies and procedures required to protect the system in a manner commensurate with risk.<br>• Maintain compliance with requirements specified by Data Owners for the handling of data processed by the system.<br>• Department/Organisation must preserve audit trail log centrally in their server for minimum six month duration. |
| | | The Data Owner is the Department Nodal Officer IT responsible for the policy and practice decisions regarding data, and is responsible for the following:<br>• Evaluate and classify sensitivity of the data.<br>• Define protection requirements for the data based on the sensitivity of the data, any legal or regulatory requirements, and business needs.<br>• Communicate data protection requirements to the System Owner.<br>• Define requirements for access to the data. |
| 5 | System Administrator | The System Administrator is an analyst, engineer, or consultant who implements, manages, and/or operates a system or systems at the direction of the System Owner, Data Owner, and/or Data Custodian. The System Administrator assists Department management in the day-to-day administration of Department IT systems, and implements security controls and other requirements of the Department information security program on IT systems for which the System Administrator has been assigned responsibility. |
| 6 | IT System Users | All users of IT systems including employees and contractors are responsible for the following:<br>• Reading and complying with information security program requirements. |

| | | |
|---|---|---|
| | | • Reporting breaches of IT security, actual or suspected, to their Department management<br>• Taking reasonable and prudent steps to protect the security of IT systems and data to which they have access. |
| 7 | Database & Backup administrator | • Secure off-site storage for backup media. Secure off-site storage for backup media.<br>• Store off-site backup media in an off-site location that is geographically, separate and distinct from the primary location.<br>• Performance of backups only by authorized personnel.<br>• Review of backup logs after the completion of each backup job to verify successful completion.<br>• Approval of backup schedules of a system by the System Owner.<br>• Approval of emergency backup and operations restoration plans by the System Owner.<br>• Protection of any backup media that is sent off site (physically or electronically), or shipped by the<br>• Retention of the data handled by an IT system in accordance with the Department's records retention policy.<br>• Document and exercise a strategy for testing that IT system and data backups are functioning as expected and the data is present in a usable form. |
| 8 | Network & Security Administrator | • Identify, document, and apply more restrictive security configurations for sensitive Department IT systems, as necessary.<br>• Maintain records that document the application of baseline security configurations.<br>• Monitor systems for security baselines and policy compliance.<br>• Review and revise all security configuration standards annually, or more frequently, as needed.<br>• Reapply all security configurations to Department-owned IT systems, as appropriate, when the IT system undergoes a material change, such as an operating system upgrade.<br>• Require periodic operating system level vulnerability scanning of sensitive IT systems in a frequency commensurate with sensitivity and risk, to assess whether security configurations are in place and if they are functioning effectively.<br>• **Time Synchronization:** All service providers, intermediaries, data centres, body corporate and Government organisations shall connect to the Network Time Protocol (NTP) Server of National Informatics Centre (NIC) or National Physical Laboratory (NPL) or with NTP servers traceable to these NTP servers, for synchronisation of all their ICT systems clocks. |

| | | |
|---|---|---|
| | | • Modify individual IT system configurations or baseline security configuration standards, as appropriate, to improve their effectiveness based on the results of vulnerability scanning.<br>• Apply all software publisher security updates to the associated software products.<br>• All security updates must be applied as soon as possible after appropriate testing, not to exceed 90 days for implementation.<br>• Prohibit the use of software products that the software publisher has designated as End-of-Life (i.e., software publisher no longer provides security patches for the software product).<br>• Prohibit all IT system users from intentionally developing or experimenting with malicious programs (e.g., viruses, worms, spyware, keystroke loggers, phishing software, Trojan horses, etc.).<br>• Prohibit all IT system users from knowingly propagating malicious programs including opening attachments from unknown sources.<br>• Provide malicious program detection, protection, eradication, logging, and reporting capabilities."<br>• Provide malicious code protection mechanisms via multiple IT systems and for all IT system users preferably deploying malicious code detection products from multiple vendors on various platforms<br>• Provide the ability for automatic download of definition files for malicious code protection programs whenever new files become available, and propagate the new files to all devices protected by the malicious code protection program.<br>• Require all forms of malicious code protection to start automatically upon system boot.<br>• Provide network designs that allow malicious code to be detected and removed or quarantined before it can enter and infect a production device.<br>• Prohibit the use of common use workstations and desktops (e.g., training rooms) to create distribution media. |
| 9 | Software Programmer/Developer | ***Incorporate IT security requirements in each phase of the life cycle, as well as for each modification proposed for the IT application system in each stage of its life cycle.***<br><br>**<u>Project Initiation</u>**<br>• Perform an initial risk analysis based on the known requirements and the business objectives to provide high-level security guidelines for the system development phase.<br>• Classify the types of data (see IT System and Data Sensitivity Classification) that the IT system will process and the sensitivity of the proposed IT system. |

| | | |
|---|---|---|
| | | • Assess the need for collection and maintenance of sensitive data before incorporating such collection and maintenance in IT system requirements. Identify, develop, and document IT security requirements for the IT system during the Project Definition phase. |
| | | **ApplicationDevelopment**<br>• Authentication - Application-based authentication and authorization shall be performed for access to data that is available through the application but is not considered publicly accessible.<br>• Session Management - Any user sessions created by an application shall support an automatic inactivity timeout function.<br>• Data storage shall be separated either logically or physically, from the application interface (i.e., design two or three tier architectures where possible).<br>• Input Validation - All application input shall be validated irrespective of source. Input validation should always consider both expected and unexpected input, and not block input based on arbitrary criteria.<br>• Default Deny - Application access control shall implement a default deny policy, with access explicitly granted<br>• Principle of Least Privilege - All processing shall be performed with the least set of privileges required.<br>• Quality Assurance - Internal testing shall include at least one of the following: penetration testing, fuzz testing,<br>• or a source code auditing technique. Third party source code auditing and/or penetration testing should be conducted commensurate with sensitivity and risk."<br>• Configure applications to clear the cached data and temporary files upon exit or logoff of the system. |
| | | **Production and Maintenance**<br>• Production applications shall be hosted on servers compliant with latest security requirement.<br>• Internet-facing applications classified as sensitive shall have periodic vulnerability scans run against the applications and supporting server infrastructure, and always when any significant change to the environment or application has been made. Any remotely exploitable vulnerability shall be remediated immediately. Other vulnerabilities should be remediated without undue delay. |

## 5.CYBER CRISIS RECOGNITION, MITIGATION & MANAGEMENT

## 5.1CRISIS RECOGNITION

A cyber state of alert will be determined using indicators that rank the severity of the threat and the likelihood of their materialization. A declaration of a cyber state of alert that corresponds to the magnitude will help to reduce the likelihood of damage to vital cyber assets including physical assists.

### CYBER SECURITY EMERGENCY- LEVELS OF CONCERN

| Threat Level | Severity | Scope | Condition |
|---|---|---|---|
| **Level 1** | **Guarded** | ***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:<br>• *Targeted attacks and espionage activities.*<br>• *Identity theft (Phishing, spoofing, social engineering etc.)*<br>• *Web defacements and Application level attacks*<br>• *Visible signs of malicious programs (virus/worms/Bots/malware/Spyware/etc.)*<br>• *Detection of new and advanced malware infections*<br>• *Attempts to exploitation of zero-day vulnerabilities*<br>• *Denial of Service attacks (DoS)*<br>• *Distributed Denial of Service (DDoS)and Distributed reflection Denial of Service (DrDoS)*<br>• *Hacking of IT' systems such as computer systems, Servers (Mail, Web, database etc.) and Routers*<br>• *Spam* |
| **Level 2** | **Elevated** | ***Multiple Organizations*** | Perceptible change/variation in network/system performance and abnormal surge in network traffic affecting IT infrastructure of multiple organizations simultaneously due to:<br>• *Targeted attacks and espionage activities*<br>• *Large scale infection of* |

| | | | |
|---|---|---|---|
| | | | *viruses/worm/Bots/malware/keylogger/Spyware etc. for malicious and espionage activities*<br>• *Detection of domain specific malwares like "Stuxnet' targeting Industrial Control Systems*<br>• *Focused attempts of network scanning and penetration*<br>• *DDoS attacks and Distributed Reflection Denial of Service (DDoS)*<br>• *Attacks on Domain name Servers, mail Servers, Databases, Routers etc.*<br>• *Large scale web-application attacks like backdooring and defacement*<br>• *Attacks on trust infrastructure*<br>• *Attacks on IT infrastructure of a Critical Information System*<br>• *Infection of computer systems and/or Programmable Logic Controllers (PLCs)*<br>• *Abnormal functioning of SCADA/industrial Control Systems.* |
| **Level 3** | **Heightened** | ***State/Multiple States*** | Significant break down of supplies or services essential to the life of the citizens including but not limited to Government, financial, transport, energy, or communication due to focused cyber-attacks on infrastructure of critical sector and Government across a state/multiple states. |
| **Level 4** | **Serious** | ***Entire Nation*** | Significant/complete breakdown of supplies or services essential to 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 sector and Government across the nation. |

## 5.2CYBER CRISIS REPORTINGAUTHORITY

As far as possible it is incumbent upon all the Departments to document every step of a cyber security incident and its mitigation measures. Such documentation involves action that is taken, such as the reporting of the incident, the collecting of evidence, conversations with users, system owners and others, etc.

State Departments should always make it a point to report cyber security incidents to the Cyber Emergency Response Team, CERT-In. Reporting to the CERT-In is vital in determining whether the incident is isolated or not and allows to keep track of threat trends in India.

Department nominated CISO would be ultimately responsible for Identification & Reporting the CRISIS in proper format with logs.

1. *Organization contact details*
2. *The type of the incident*
3. *The date & time of the incident*
4. *Is the incident ongoing?*
5. *How did organization notice this incident?*
6. *What's the impact of the incident?*
7. *Have organization already taken actions or measures? If so, which ones?*
8. *Do organization have logs or other useful data?*
9. *Share the logs, evidence to CERT-Infor further investigation*
10. *What is the organization expectation from CERT-In?*

## 5.3 ACTIONS TO BE UNDERTAKEN BY CERT-IN

*On report of the incident, CERT-In would take the following supportive actions*

- ✓ Analyze the information/logs received from affected organization
- ✓ Check for latest patches/updates from various sources including vendors
- ✓ Consult vendors and others sources to help the organization in resolving the problem
- ✓ Document the vulnerability information and disseminate
- ✓ In case of Phishing attacks, take appropriate actions to block the phishing site 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
- ✓ In case of DoS/DDoS attacks, contact the concerned CERTs or ISPs from where the attacks are originating for blocking
- ✓ Analyze ongoing attack/traffic and seek assistance from Vendors and other CERTs if required
- ✓ Work closely with affected organizations, ISPs and other agencies to provide all necessary help to mitigate the incident
- ✓ Advice appropriate measures to isolate systems/networks at organizations/regions

## 5.4 REPORTING OF A SECURITY INCIDENT

System Administrators can report an 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

**Security Incident Reporting Form**

| **Form to report Incidents to CERT-In** | | | |
|---|---|---|---|
| For official use only: | | Incident Tracking Number:**CERT-In-xxxxxx** | |
| 1.ContactInformationforthisIncident: | | | |
| Name: | Organization: | Title: | |
| Phone/ Fax No: | Mobile: | Email: | |
| **Address:** | | | |
| 2.Sector(Please tick the appropriate choices) | | | |
| Government<br>Financial<br>Power | Transportation<br>Manufacturing<br>Health | Telecommunications<br>Academia Petroleum | InfoTech<br>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'smission? (Yes/No).Details. | | | | |
| | | | | |
| 6.InformationofAffected System: | | | | |
| IP Address: | Computer/ Host Name: | Operating System (incl.Ver./release No.) | Last Patched/Updated | Hardware Vendor/Model |
| 7.TypeofIncident: | | | | |
| Phishing<br>Network scanning /Probing Break-in/Root Compromise<br>Virus/Malicious Code<br>Website Defacement<br>System Misuse | | SpamBot/Botnet<br>EmailSpoofing<br>Denial of Service(DoS)<br>Distributed<br>Denial of Service(DDoS)<br>UserAccount Compromise | | Website Intrusion Social Engineering<br>Technical Vulnerability<br>IPS poofing<br>Other_____ |
| 8.Description of Incident: | | | | |
| | | | | |
| 9.Unusualbehavior/symptoms(Tick the symptoms) | | | | |
| • System crashes<br>• 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<br>• Unexplained elevation or use of privileges Operation of a program or sniffer device to capture network traffic;<br>• An indicated last time of usage of a user account that does not correspond to the actual last time of usage for that user<br>• A system alarm or similar indication from an intrusion detection tool<br>• Altered home pages, which are usually the | | | | • Anomalies Suspicious probes Suspicious browsing New files<br>• Changes in file lengths or dates Attempts to write to system Data modification or deletion Denialof service<br>• Door knob rattling Unusual time of usage Unusual usage patterns Unusual log file entries<br>• Presence of new set uid or set gid files Changes in system directories and files Presence of cracking utilities |

| | |
|---|---|
| intentional target for visibility, or other pages on theWeb server | • Activity during non-working hours or holidays<br>• Other(Please specify) |

| 10.Hasthisproblembeenexperiencedearlier?Ifyes,details. | | | |
|---|---|---|---|
| | | | |
| 12.Agencies notified? | | | |
| Law Enforcement | Private Agency | Affected Product Vendor | Other_____ |
| 11.Whenand How was the incident detected: | | | |
| | | | |
| 13.Additional Information:(Include any other details noticed ,relevant to the Security Incident.) | | | |
| Whether log be ing submitted | | Mode of submission: | |

**OPTIONALINFORMATION**

| 14.IPAddressofApparent or Suspected Source: | |
|---|---|
| Source IP address: | Other information available: |

| 15.SecurityInfrastructureinplace: | | | | |
|---|---|---|---|---|
| | 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.HowManyHost(s)are Affected | | |
|---|---|---|
| 1to 10 | 10to 100 | Morethan100 |
| 17.Actionstakento 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:+91-11-24368546or email at: incident@cert-in.org.in | | |

## 5.5 CYBER CRISIS COMMUNICATION STRATEGY

The State Government departments should develop a strategy for public relations and a plan for communication with stakeholders upon a crisis.

A communication strategy could be expected to address the following requirements:

i. *Media communications shall be handled by only Senior Most Officer of the Department to avoid misinformation.*

ii. *Points of contact and communication decision makers need shall be defined as per the provision of the Cyber Security Policy of the State.*

iii. *Continuously notify affected or impacted stakeholders on containment and progress efforts*

Communication of the crisis is crucial. The processes, plans, and methods of sharing information on the crisis with relevant stakeholders need to be ready to handle incoming requests. What is known regarding the cyber crisis should be proactively

shared transparently with the public and with stakeholders. The organization's response to the cyber-attack and intentions of what should be done can easily trigger negative reactions on the web, social media sites, these conversations should be monitored and addressed.

An organized, structured response with clearly articulated chronological events timeline with various vendors and technology partners, not only enables a better response but also prepares for regulatory inquiries, litigation in the future.

## 5.6 CYBER CRISIS NATURE & MITIGATION

| Severity level of Cyber crisis | Nature of cyber crisis | Steps for mitigation |
|---|---|---|
| **Level 1 Response**<br><br>**Scope: Individual Organization** | ***All attacks*** | • *Notify incidents to respective administrative Department*<br>• *Monitor and detect anomalous behavior and degradation of service in network and systems*<br>• *Take all logs (system, application, security, access, error etc.) of affected systems and data therein and keep them separately for analysis and forensics*<br>• *Forward a copy of all the logs of affected systems and network devices, suspicious files, data, traffic trends wherever applicable to CERT-In*<br>• *Consult incident reports or vulnerability reports for specific advisories on the suspicious behavior as published by CERT-In and implement those in the affected networks and systems*<br>• *Segregate networks (LAN/WAN) and perimeter security devices and systems*<br>• *Change all user/root/administrator passwords in all systems and network devices*<br>• *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*** | • *If possible, isolate affected server from Internet or disable the affected module in application*<br>• *Scan all files for any malicious footprint*<br>• *Take a copy of all logs at the server and perimeter level (IDS/IPS, firewall) and traffic trends*<br>• *Identify the type of attack and vulnerability exploited* |

| | | |
|---|---|---|
| | | • *Patch the vulnerability/ issue by modifying insecure code/configuration by secure code/configuration*<br>• *Report to CERT-In with web server logs and dump of the vulnerable web application* |
| | ***Virus / Worm / Spyware / Botnet attacks*** | • *Isolate affected systems/network segments from LAN and Internet*<br>• *Scan all files in the suspected systems, including emails for viruses*<br>• *Clean the affected systems with the updated antivirus software*<br>• *Install updated Antivirus/ anti-Spyware on all systems* |
| | ***DoS/DDoS attacks/ NTP based DrDoS attacks*** | • *Take a copy of all the logs at perimeter level (IDS/IPS, firewall) and traffic trends*<br>• *Identify the type of attack such as flooding of particular types of packets/requests*<br>• *Allocate traffic to unaffected available network paths, if possible*<br>• *Apply appropriate rate limiting strategies at the local perimeter and if necessary, consult ISP*<br>• *Implement Egress and Ingress filtering to block spoofed packets*<br>• *Use appropriate DoS prevention tools*<br>• *Install updated software patches on all 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 noise signal ratio or increased noise levels in the airwaves.*<br>• *Identify the other devices due to which the RF interference occurs and physically remove them*<br>• *Deploy IPS/IDS to detect rogue access points* |
| | ***DNS Attack*** | • *Check the version updates at the DNS server and install latest software patches*<br>• *Implement spoofing countermeasures*<br>• *Use Unicast Reverse Path Forwarding to mitigate problems that are caused by malformed or forged IP source addresses*<br>• *Adopt source IP address verification*<br>• *Implement DNSSec* |
| | ***Attack attempts / scan on Servers, Routers,*** | • *Check for effectiveness of filtering rules in the routers, firewall and IPS and reconfigure if required*<br>• *Check the logs of these devices for source of attack* |

| | | |
|---|---|---|
| | ***Firewall etc.*** | |
| | ***Phishing attacks*** | • *Keep watch on phishing sites*<br>• *Alert customers regarding the phishing sites*<br>• *Encourage customers to use anti-phishing enable browsers*<br>• *Shutdown phishing sites in coordination with concerned ISP and CERT-In* |
| | ***Mail Server attacks*** | • *Deploy hot standby mail servers in physically separated networks and places which can be made operational when the main server is attacked*<br>• *Disable all other ports and services on mail servers*<br>• *Enforce strong password policy and encourage users to change passwords periodically* |
| | ***Attacks on Critical Infrastructure and associated SCADA/Industrial Control Systems, through sophisticated malware such as Stuxnet/Duqu/ Nitro/Flame*** | • *Check the signs of infection in computer systems in general*<br>• *Isolate the infected system from all networks immediately*<br>• *Report the incident to CERT-In at the earliest. Consult relevant advisories of CERT-In and follow specific measures suggested therein.*<br>• *Take forensic image and send to CERT-In*<br>• *Clean the affected system with the updated antivirus software*<br>• *Install updated Antivirus/Anti-spyware on all systems*<br>• *Examine the vectors of propagation of worms- Removal media, network shares and other sneakernet systems*<br>• *Examine the critical SCADA/ Industrial Control Systems/PLCs for abnormal functionality*<br>• *Examine network traffic towards malicious domains/websites/hosts that are identified as Command & Control*<br>• *Review the security controls and processes to ensure isolation of critical networks from other infrastructure* |
| | ***Attack on IoT/IIoT devices*** | • *Check for signs of infection or compromise in IoT/IIoT devices*<br>• *Coordinated vulnerability mitigation*<br>• *Isolate infected devices from all networks immediately*<br>• *Report the incident to CERT-In at the earliest. Consult relevant advisories of CERT-In and follow specific measures suggested therein.*<br>• *Take forensic image and send to CERT-In*<br>• *Update the affected systems with relevant patch/workaround* |

| | | |
|---|---|---|
| | ***Supply Chain Attacks/ Vendor Risk management*** | • *Isolate affected systems/products from network*<br>• *Coordinated vulnerability mitigation*<br>• *Identification of workaround*<br>• *Impact analysis*<br>• *Review SLAs, policies and controls*<br>• *Reporting of incidents to relevant agencies* |
| **Level 2 Response**<br><br>**Scope: Multiple Organizations** | ***All Attacks*** | • *Notify incidents to respective administrative Department*<br>• *Monitor and detect anomalous behavior and degradation of service in network and systems*<br>• *Take all logs (system, application, security, access, error etc.) of affected systems and data therein and keep them separately for analysis and forensics*<br>• *Forward a copy of all the logs of affected systems and network devices, suspicious files, data, traffic trends wherever applicable to CERT-In*<br>• *Consult incident reports or vulnerability reports for specific advisories on the suspicious behavior as published by CERT-In and implement those in the affected networks and systems*<br>• *Segregate networks (LAN/WAN) and perimeter security devices and systems*<br>• *Change all user/root/administrator passwords in all systems and network devices* |
| | ***Web Applications*** | • *If possible, isolate affected server from Internet or disable the affected module in application*<br>• *Scan all files for any malicious footprint*<br>• *Take a copy of all logs at the server and perimeter level (IDS/IPS, firewall) and traffic trends*<br>• *Identify the type of attack and vulnerability exploited*<br>• *Patch the vulnerability/ issue by modifying insecure code/configuration by secure code/configuration*<br>• *Report to CERT-In with web server logs and dump of the vulnerable web application* |
| | ***Virus / Worm / Spyware / Botnet attacks*** | • *Isolate affected systems/network segments from LAN and Internet*<br>• *Scan all files in the suspected systems, including emails for viruses*<br>• *Clean the affected systems with the updated antivirus software*<br>• *Install updated Antivirus/ anti-Spyware on all systems*<br>• *Block the infection/attack vectors through IPS/Firewall* |

| | | |
|---|---|---|
| | ***DoS/DDoS attacks/ NTP based DrDoS attacks*** | • *Shift critical services to alternate channels*<br>• *Incase of IP based attacks, shift hosting of affected services to different ISPs*<br>• *Apply appropriate rate limiting strategies at the local perimeter and if necessary, consult ISP*<br>• *Implement Egress and Ingress filtering to block spoofed packets*<br>• *Use appropriate DoS prevention tools*<br>• *Take a copy of all the logs at perimeter level (IDS/IPS, firewall) and traffic trends*<br>• *Install updated patches on the network devices* |
| | ***High energy RF-based DoS attacks*** | • *Use a network management solution capable of alerting on a degraded noise signal ratio or increased noise levels in the airwaves.*<br>• *Identify the other devices due to which the RF interference occurs and physically remove them*<br>• *Relocate the Access Points in case of Wireless Network* |
| | ***DNS Attack*** | • *Change the preferred DNS server*<br>• *Implement source address validation through ingress filtering (Implement IETF BCP 38/RFC 2827)*<br>• *Use Unicast Reverse Path Forwarding to mitigate problems that are caused by malformed or forged IP source addresses*<br>• *Run separate DELEGATED and RESOLVING name servers*<br>• *Disable Recursion on DNS server authoritative for the zone*<br>• *Restrict zone transfers to slave name servers and other authorized software*<br>• *Block invalid DNS messages to an authoritative name server at the network edge. This includes blocking large IP packets directed to an authoritative name server*<br>• *Version updates and install latest patches*<br>• *Implement split DNS architecture*<br>• *Implement anycast technology on DNS server* |
| | ***Attack attempts / scan on Servers, Routers, Firewall etc.*** | • *Check for effectiveness of filtering rules in the routers, firewall and IPS and reconfigure if required*<br>• *Check the logs of these devices for source of attack*<br>• *Check for version updates/patches and install latest patches for routers, firewall and IPS* |

| | | |
|---|---|---|
| | ***Mail Server attacks*** | • *Activate hot standby mail servers mail traffic appropriately* |
| | ***Advanced targeted Attacks*** | • *Identify the target entities and sensitize them about the targeted attacks*<br>• *Isolate systems found to be connecting to suspicious domains/hosts after preserving volatile data and create forensic images for further analysis*<br>• *Based on analysis of incident apply appropriate security controls such as patching the targeted application, updating antivirus signatures to detect the crafted malware and detecting connections to call back domains/hosts through perimeter devices*<br>• *Regularly monitor events and traffic at host/network level to detect malicious activities and report any suspicious activities to CERT-In* |
| | ***Attacks on Critical Infrastructure and associated SCADA / Industrial Control Systems, through sophisticated malware*** | • *Check the signs of infection in computer systems in general*<br>• *Isolate the infected system from all networks immediately*<br>• *Report the incident to CERT-In at the earliest. Consult relevant advisories of CERT-In and follow specific measures suggested therein.*<br>• *Take forensic image and send to CERT-In*<br>• *Clean the affected system with the updated antivirus software*<br>• *Install updated Antivirus/Anti-spyware on all systems*<br>• *Examine the vectors of propagation of worms- Removal media, network shares and other sneakernet systems*<br>• *Examine the critical SCADA/ Industrial Control Systems/PLCs for abnormal functionality*<br>• *Examine network traffic towards malicious domains/websites/hosts that are identified as Command & Control*<br>• *Review the security controls and processes to ensure isolation of critical networks from other infrastructure* |
| | ***Compromise of trust infrastructure – Certifying Authority, authentication mechanism, compromise of*** | • *Immediately report the incident to CERT-In*<br>• *Revoke the compromised keys*<br>• *Announce revocation notification at the earliest*<br>• *Review network/system security posture*<br>• *Deploy appropriate mechanism to check and certify correctness of cryptographic functions*<br>• *Generate fresh keys/certificates* |

| | | |
|---|---|---|
| | ***key management*** | • *Conduct appropriate awareness campaigns to notify all users* |
| | ***Attack on IoT/IIoT devices*** | • *Check for signs of infection or compromise in IoT/IIoT devices*<br>• *Coordinated vulnerability mitigation*<br>• *Isolate infected devices from all networks immediately*<br>• *Report the incident to CERT-In at the earliest. Consult relevant advisories of CERT-In and follow specific measures suggested therein.*<br>• *Take forensic image and send to CERT-In*<br>• *Update the affected systems with relevant patch/workaround* |
| | ***Supply Chain Attacks/ Vendor Risk management*** | • *Isolate affected systems/products from network*<br>• *Coordinated vulnerability mitigation*<br>• *Identification of workaround*<br>• *Impact analysis*<br>• *Review SLAs, policies and controls*<br>• *Reporting of incidents to relevant agencies* |
| **Level 3 Response**<br><br>**Scope: Multiple States** | ***All Attacks*** | • *Notify incident to respective Departments*<br>• *Implement the Contingency Plan*<br>• *Deploy onsite response team on 24x7 basis*<br>• *Limit the access to systems and networks from outside in consultation with concerned ISPs*<br>• *Enable hot stand-by systems/servers with alternate traffic paths*<br>• *Take all logs (system, application, security, access, error etc.) of affected systems and data therein and keep them separately for analysis and forensics*<br>• *Forward a copy of all the logs of affected systems and network devices, suspicious files, data, traffic trends wherever applicable to CERT-In*<br>• *Consult incident reports or vulnerability reports for specific advisories on the suspicious behavior as published by CERT-In and implement those in the affected networks and systems*<br>• *Carry out file integrity checks on all the systems*<br>• *Restore systems from trusted back-ups and validate the systems and networks before connecting to Internet*<br>• *Change all user/root/administrator passwords in all systems and network devices* |
| **Level 4 Response** | ***All Attacks*** | • *Notify incidents to Apex Committee*<br>• *Request meeting of Apex Committee*<br>• *Affected Department carry out the steps indicated in Level-3* |

| | | |
|---|---|---|
| **Scope:**<br>**Entire Nation** | | • *Implement the directives of Apex Committee*<br>• *Implement specific advisories and instructions issued by CERT-In and other designated agencies* |

## 6. PHYSICAL SECURITY

Physical security is the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to an enterprise, agency or institution. At its core, physical security is about keeping theICT assets &facilities and people safe from real-world threats. It includes physical deterrence, detection of intruders, and responding to those threats. Physical attacks could be breaking into a secure data center, sneaking into restricted areas of a building, or using terminals they have no business accessing. Attackers could steal or damage important IT assets such as servers or storage media, gain access to important terminals for mission critical applications, steal information via USB, or upload malware onto your systems.Rigorous controls at the outermost perimeter should be able to keep out external threats, while internal measures around access should be able to reduce the likelihood of internal attackers while it could be from environmental events, the term is usually applied to keeping people – whether external actors or potential insider threats – from accessing areas or assets they shouldn't.

1) **Protection against Dumpster Diving**: It's one of the few completely legal ways in which others can steal sensitive information if you're not careful. The legality and relative ease of it make it inherently dangerous. So, to protect against it, organization can start by making sure that nobody can walk into their premise and simply steal. Ensure that all important documents are shredded, and still remain secure. In case of usage of a remote shredding service, make sure they have chain of custody controls in place that allow you to track ownership of the sensitive document at any point.

2) **Site Access Control**: Especially in an area where sensitive data is handled and stored like data center, that becomes a crucial place. Standard access control. Policy to physical site is a must. Only authorized person should be allowed to access to such location by the Department. ICTS infrastructure related to critical devices like network, firewall, switch, printer location information shouldn't made available to public. Tailgating must not be allowed under any circumstances.

3) **Employee Awareness Training:** Employee training on physical security aspects is a must and Departments shall ensure that regular training are conducted as per assigned accountabilities.

4) **Securing Backups:** Importance of data backups for your business. Physical backups are an important part of business continuity to prevent data loss in the face of outages, disasters, and more. Backup devices should be also be kept with standard security measures.

5) **Accounting for Lost or Stolen Device:** As devices become more mobile, the potential for them being stolen becomes more frequent. Encourage employees to work only organization owned device. Incase loss of any device need to be taken seriously and remote wipe off mechanism must be implemented.

6) **Secure Network-Enabled Printers:** Network printers are convenient. They allow anyone in the office to get connected, without the need of extra wiring. Unfortunately, they are also a security risk. Many of them, through default settings, offer open wifi access, allowing anyone to get in and open vulnerabilities in the process. To prevent hacked the network printer, inventory network devices and only connect those to the internet that actually need to be. If only people in office use the printer, remote access will not be necessary. Adding passwords to the connection can also help.

7) **Implementing Video surveillance Systems:** A video surveillance system wherever required for shall be deployed to secure the ICT Infra from physical damage and theft.

8) **Securing Windows& Doors:** Physical entry points like Door and Windows os should be thoroughly checked for any vulnerabilities where ICT assets are deployed.

9) **Building Secure Guest WiFi:** Guest WiFi must be having very limited access, it should not allow external users access to organization network, which they can exploit to sometimes devastating consequences. Guest Wifi must be placed a separate vlan which doesn't have any communication to organization other vlan except Internet.

10) **Physical safety for Datacenter/IT Asset:** Always try to build the datacenter/IT asset with safety measures for minimum disruption from earthquake and flood type of geographic catastrophic situation.

## 7. RECOMMENDATIONS BEST USED POLICY

| | |
|---|---|
| **Information Security Policy and implementation of Best Practices** | The critical sectors should necessarily implement Information Security Management System (ISMS) Best Practices as per ISO 27001. The following steps should be taken into account while implementing the ISMS<br>• *Clearly identify the three components namely process, technology and mitigation of incidents*<br>• *Undertake comprehensive Risk Assessment of Information Technology/Network assts*<br>• *Implement appropriate security control measures such those defined in ISO 270001 which include Service Level Agreements with various service providers.* |
| **Disaster Recovery Plan (DRP)** | Establish Disaster Recovery (DR) plans with adequate redundancy to take over operation in case of the need |
| **Security of Information Infrastructure, network and Applications** | Security devices may be installed in 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 should be checked at the time of installation as well at the time of significant changes for the needed functionalities and security features.<br>• *The security mechanism should include appropriate devices and methods to log and monitor the events to detect network scanning, probing and reconnaissance, flooding attempts on IT infrastructure.*<br>• *The remote monitoring and maintenance of the security devices should be strictly restricted to authorized persons only.*<br>• *The software at network, system and application level should be regularly upgraded*<br>Application Security best practices includes:<br>• *Implementation of application security controls for both web and mobile applications* |

| | |
|---|---|
| | • *Secure application development should be enhanced by applying security checkpoints and techniques at early stages of development as well as throughout software development life cycle (SDLC)special emphasis should be applied to the coding phase of development. Security mechanisms that should be used include threat modelling, risk analysis, static analysis, digital signature, among others*<br>• *Comprehensive security assessments of applications should be performed before final deployment of application and after any major changes or upgrades to the system*<br>• *Application design and development should ensure compliance of policy and regulations as applicable.* |
| **Network Traffic Scanning** | The network traffic scanning technique provides visibility into the state of network and identifies deviations from baselines that may indicate normal or suspicious behavior. The traffic patterns provide leads on 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 rise on the port 25, associate with e-mail service; this may indicate that e-mail based worm is spreading at a high speed. A sudden traffic rise on the IRC ports may indicate surge in the 'Botnet activity'. The network traffic flows thus give the exact portrait of the communication 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 the network flow-data traffic. Industry solutions are available to collect and analyze network flow traffic on the gateway routers and switches.<br><br>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. |
| **Isolation of critical** | The critical networks should be isolated from other production |

| | |
|---|---|
| **networks** | networks connected over intranet/internet. No transfer of data from intranet/internet-based network to a critical network or vice versa be allowed. In case required, it should be under strict control and thoroughly screened. There are malicious codes specifically designed to target critical infrastructure systems by means of spreading through systems connected over internet. Risk assessment and regular monitoring of critical networks is essential for security of critical infrastructure. |
| **Vendor Risk Management (VRM)** | Vendor Risk Management 9VRM) is a comprehensive plan for identifying and decreasing potential uncertainties and legal liabilities regarding hiring of third-party vendors for information technology products and services. The use of third-party vendors presents several other risks, the most prominent of which are legal, operational and reputational<br>• *Proper planning and due diligence need to be taken for vendor risk identification and mitigation*<br>• *A robust vendor governance program to be developed to access critical, high, moderate and low risk vendors through surveys and assessments*<br>• *Vendor performance need to be monitored on 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.*<br>• *The organizational hierarchy involved in vendor governance need to be defined* |
| **Audit and Assurance** | • *Organizations should undertake comprehensive security audit of the entire IT infrastructure networks and applications by independent auditing organizations to discover the gaps with respect to the best security practices and take appropriate corrective actions.*<br>• *The audit of system should be undertaken at least once in a year also as and when significant addition or alteration is respect of hardware, software, network resources, policies and configurations of systems and sub systems are affected.* |
| **Security Training and Awareness** | All employees of the organization and where relevant contractors and third-party users should receive appropriate |

| | |
|---|---|
| | awareness training. Ongoing training should include security requirements, legal responsibilities and business controls as well as training in correct use of information processing facilities e.g.<br>• *Latest Technologies and threats*<br>• *Physical Security Procedures*<br>• *Access Control Procedures*<br>• *Use of License Software Packages*<br>• *Malicious code and Botnets and their prevention*<br>• *Reporting and mitigation of incidents*<br>• *Cyber Crisis Management*<br><br>*The security awareness and training activities should be 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.* |

## 8. CYBER RESILIENCE CONTROL MATRIX

### Identity

- Controlled access based on need-to-know
- Enforce Strong
- Maintenance and Analysis of complete security events and audit logs
- Minimize the invalid logon counts
- Revocation of digital certificate
- Offline recovery procedures for logging into

### Password policy

- Multi factor authentication
- Usage of Digital Certificates
- Privilege escalation monitoring and alerting
- Change access contra on all devices
- Continuous account monitoring and deactivating the dormant accounts

### System Process

- Effective Security Patch Updating Mechanism on applications etc.
- 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) 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)
- 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
- 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

## 9. CRISIS RESPONSE – FIRST HOUR, ZERO HOUR, ZERO DAY

The incident response actions during the first hour is to contain the damage and notify appropriate authorities about the incident and ensure continuity of essential activities and services of the Department.

The following guideline defines the actions to be taken within the affected Department during the first hour of incident. The guideline also facilitates detailed incident analysis and determination of recovery and response actions and possible escalation within and outside the Department.

| SYMPTOMS / ALERTS | SOURCE OF DETECTION | RESPONSE ACTION | RESPONSIBILITY |
|---|---|---|---|
| **COMMON SYMPTOMS** | | | |
| • **Non availability of computer systems (failure to start)** | • User | • Boot with alternate OS/ recovery media<br>• Check the booting process for specific errors<br>• Report to System Administrator | • User<br>• System Administrator |
| • **Frequent system crashes**<br>• **Unexplained poor system performance**<br>• **Presence of new file**<br>• **Presence of unknown processes**<br>• **Changes in file size or dates** | • User | • Scan system with updated Antivirus & Anti-Spyware<br>• Report to System Administrator | • User<br>• System Administrator |
| • **New suspicious user accounts** | • User | • Report to System Administrator | • System Administrator |

| | | | |
|---|---|---|---|
| • **Failed or successful social engineering attempts** | • User<br>• System Administrator | • Collect all details such as email content, header etc. and examine<br>• Alert other users | • System Administrator |
| • **Failed login attempts by unauthorized users** | • Technical Tools<br>• Supervisory review of logs | • Determine the timing, sources of activities<br>• Trace the attack sources from logs of systems/directory server | • System Administrator |
| • **Unusual time of usage**<br>• **Unauthorized user accounts** | • Supervisory review of logs | • Correlate with physical access by users<br>• Correlate with perimeter devices to find external intrusion | • System Administrator<br>• Network Administrator |
| • **Virus / Worm Infection / lockdown of resources by unauthorized encryption** | • User<br>• System Administrator | • Disconnect system from network<br>• Boot with different OS and scan with Antivirus & Anti-Spyware<br>• Antivirus & Anti-Spyware should be regularly updated | • User<br>• System Administrator |
| • **Suspicious probes** | • Technical tools (IDS/IPS/Firewall) | • Close the ports and services which are not required<br>• Send the logs to Incident response team for examination | • Network Administrator |
| • **Abnormal surge in traffic (inbound/ outbound)** | • Technical tools<br>• Network behavior analysis<br>• Router | • Trace the specific service/protocol<br>• Detect the source of generation of abnormal traffic<br>• Correlate with alerts from CERT-In | • Network Administrator |

| | | | |
|---|---|---|---|
| • **Any cyber security incident must be informed to CERT-in within six hours of Incident detected.** | • CERT-in Incident Reporting Form | • Necessary supporting logs. | • CISO |
| **EXTERNAL ALERTS** | | | |
| • **Alert for new vulnerability** | • CERT-In | • Apply appropriate patches/updates<br>• Implement suggested workarounds for zero-day vulnerability | • System Administrator |
| • **Alert on propagation of malicious code** | • CERT-In | • Update the Antivirus signatures<br>• Follow the counter measures suggested in the specific advisory | • System Administrator |
| • **Alert indicating attack sources** | • CERT-In<br>• Security Agencies | • Block the attack sources notified by CERT-In and other agencies | • Network Administrator |
| **WEBSITE DEFACEMENT AND SEMANTIC ATTACKS** | | | |
| • **Detection of defacement / intrusion of websites** | • Users<br>• Website Administrators<br>• External Agencies | • Disconnect the webserver hosting defacement/compromised website<br>• Examine the compromised system/website for specific unauthorized changes<br>• Restore the website content, shift and run website from different trusted system by making appropriate DNS changes at the new system<br>• Collect relevant logs of | • Website Administrator<br>• Network Administrator |

| | | | |
|---|---|---|---|
| | | server and application and submit to IR team of Department/organization<br>• Report the incident along with logs to CERT-In | |
| • **Unexplained poor system performance**<br>• **Presence of suspicious process / files on system**<br>• **Suspicious / un-authorized changes to system files, configuration files (e.g. Hosts files)**<br>• **Unauthorized encryption of the systems / files**<br>• **Surge in traffic of ports / services used by malware**<br>• **Connections to suspicious remote systems**<br>• **Unusual ports open** | • Users<br>• System Administrator<br>• Alerts from Antivirus, NIDS<br>• External Agencies | • Disconnect infected systems from network<br>• Scan with updated Antivirus and Anti-spyware<br>• Recover from clean backup<br>• Apply appropriate counter measures in consultation with local incident response team/ CERT-In | • System Administrator |
| **SPAM ATTACKS** | | | |
| • **Abnormal surge in SMTP traffic**<br>• **Bandwidth congestion**<br>• **Slow response of mail servers** | • Users<br>• Network Administrators<br>• Network behavior Analysis | • Check the mail servers for open relays and disable<br>• Close ports not required in the Mail server<br>• Identify possible sources of SPAM from email headers and invoke blacklists such as SBL, XBL, and PBL<br>• If attack persists report to local Incident Response | • Network Administrator<br>• Mail Server Administrator |

| | | | |
|---|---|---|---|
| | | Team/ CERT-In | |
| **ATTACK ON ICS AND IoT/IIoT DEVICES** | | | |
| • **Backdoor detection**<br>• **Abnormal functions**<br>• **Data exfiltration**<br>• **Alerts in monitoring & detection systems** | • Service Consumers<br>• OT Team<br>• IT Team<br>• External Agencies | • Check signs of infection or compromise in IoT/IIoT devices or ICS environment including HMI & Business network<br>• Identify vulnerability exploited<br>• Isolate infected devices from all networks immediately<br>• Report the incident to local IR team/CERT-In at the earliest. Consult and follow relevant advisories of CERT-In.<br>• Take forensic image and send to local IR team/CERT-In<br>• Update the affected systems with the relevant patch / workaround | • IT and OT team |
| **ATTACKS ON MAIL SERVERS** | | | |
| • **Non availability of mail accounts**<br>• **Compromised mail accounts** | • Users<br>• Mail Server Administrators | ***Mail server compromise:***<br>• Disconnect mail server<br>• Activate standby mail server<br>• Check logs of mail server and identify attack source<br>• Send the logs to Incident response team/ CERT-In<br>***User account compromise:***<br>• Reset the password<br>• Enforce strong passwords<br>• Enforce email best practices | • Mail Server Administrator |
| **IDENTITY THEFT ATTACKS THROUGH SPOOFING** | | | |
| • **Detection of suspicious network** | • Alert on IPS/IDS<br>• Email headers | • Examine the mail header and find the actual origin of email | • Network Administrator |

| | | | |
|---|---|---|---|
| **connections**<br>• **Detection of Packets with suspicious source address**<br>• **Emails from masqueraded account name** | | • Notify and alert users<br>• To counter spoofing, implement Egress and Ingress filtering at perimeter (Router)<br>• Enforce email authentication<br>• Report to local Incident Response Team/CERT-In<br>• | |
| **PHISHING ATTACKS** | | | |
| • **Report of phishing email / website** | • Users<br>• Anti-phishing / fraud detection services<br>• CERT-In / External agencies | • Report to local Incident Response Team/CERT-In<br>• Report phishing URL to phishing filters<br>• Send phishing emails and details of phishing website to CERT-In | • Users<br>• Designated Persons |
| **DENIAL OF SERVICE (DoS) ATTACKS** | | | |
| • **Non - Availability of services such as website, email, etc.**<br>• **System crashes**<br>• **Bandwidth congestion**<br>• **Surge in traffic** | • Users<br>• Website Administrator | • Identify the type of attack such as flooding of particular types of packets / requests (TCP SYN, ICMP etc.) by examining logs of Router/IPS/IDS/Firewall<br>• Identify the attack sources<br>• Block the attack sources at Router / packet filtering device<br>• Check Router configuration and implement Egress and Ingress filtering to block spoofed packets<br>• Disable the non-essential ports / services<br>• Report to local Incident Response Team/CERT-In | • |
| **DISTRIBUTED DENIAL OF SERVICE (DoS) ATTACKS** | | | |
| • **Non-Availability of services such** | • Network Administrator<br>• Alerts of IPS / IDS / Firewalls | • Identify the type of attack such as flooding of particular types of packets/requests by | • Network Administrator |

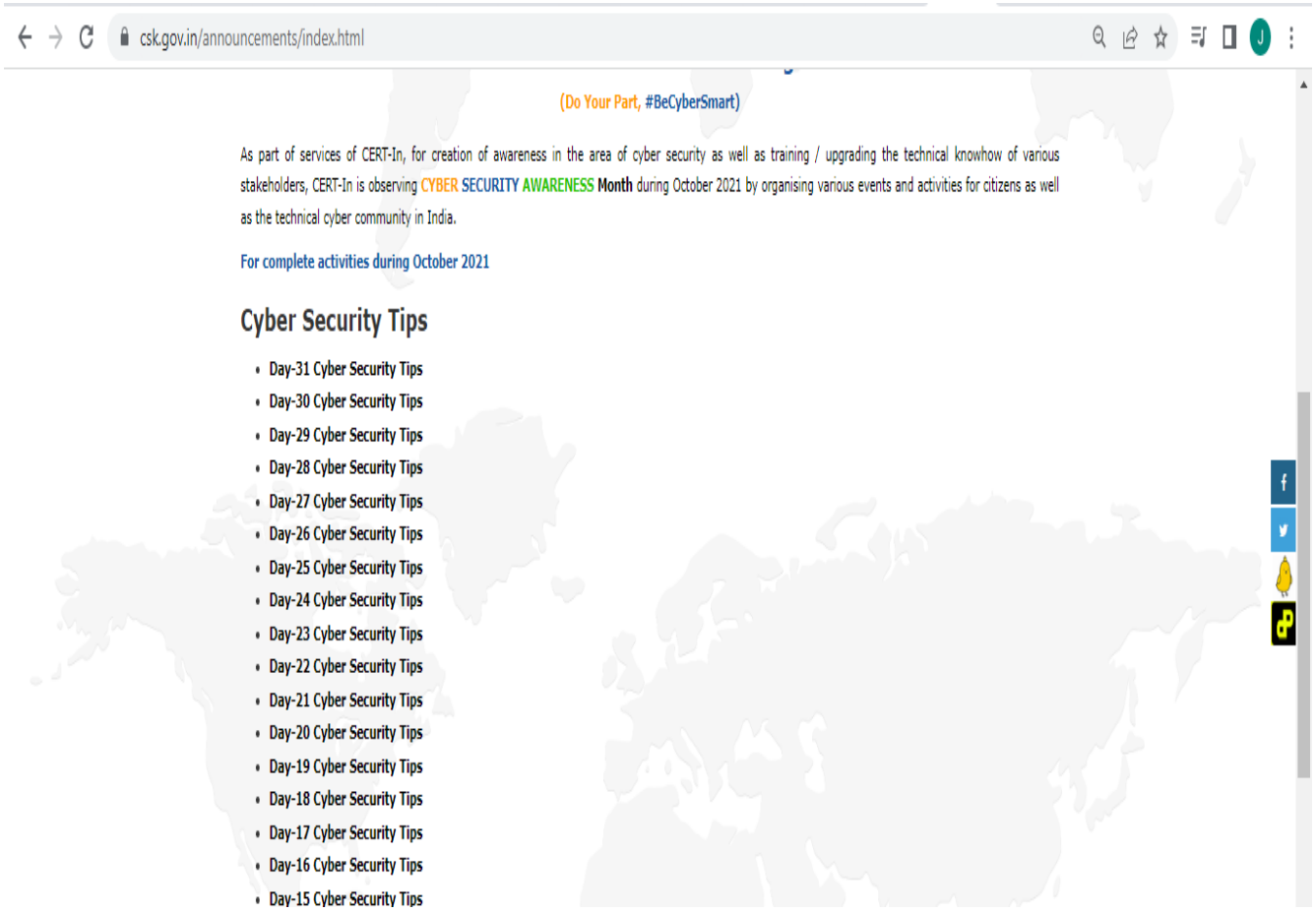
| | | | |
|---|---|---|---|
| **as websites, email etc.**<br>• **System crashes**<br>• **Bandwidth congestion**<br>• **Surge in traffic** | • Network Behaviour Analysis<br>• CERT-In | examining logs of Router/IPS/IDS/Firewall<br>• Apply appropriate rate limiting strategies at the local perimeter and if necessary, consult ISP<br>• Implement Egress and Ingress filtering to block spoofed packets<br>• Use appropriate DoS prevention tools<br>• If problem persists, shift web/mail services hosting to alternate Internet Protocol (IP) addresses.<br>• Report to local Incident Response Team/CERT-In with relevant logs | |
| **DoS ATTACKS ON DNS SERVER** | | | |
| • **Slow response or non - availability of web / mail services** | • User<br>• Network Administrator | • Change the primary DNS Server<br>• Implement source address validation through Ingress filtering (Implement IEFT BCP 38/RFC 2827)<br>• Use Unicast Reverse Path Forwarding to mitigate problems that are caused by malformed or forged IP source addresses<br>• Run separate DELEGATED and RESOLVING name servers<br>• Disable Recursion of DNS server authoritative for the zone<br>• Restrict zone transfer to Secondary name servers only<br>• Block invalid DNS messages to an authoritative name server at the network | • Network Administrator |

| | | | |
|---|---|---|---|
| | | edge. This includes blocking large IP packets directed to an authoritative name server.<br>• Report to local Incident Response Team/CERT-In | |
| **DNS CACHE POISIONING ATTACKS** | | | |
| • **Redirection of legitimate web / mail traffic to suspicious websites / mail servers** | • User<br>• Network Administration | • Purge cache<br>• Restart DNS server<br>• Replace DNS records with content from trusted backup<br>• Examine DNS forwarding traffic to identify rogue DNS server and block<br>• Restrict rights of configuration changes to Administrator only<br>• At client side, delete any additional entries in HOST file<br>• Report to local Incident Response Team/CERT-In | • Network Administrator |
| **APPLICATION LEVEL ATTACKS** | | | |
| • **Unauthorized changes to Data**<br>• **Suspicious user activity**<br>• **Elevation of privilege of user accounts**<br>• **Presence of malicious links/content** | • Web/Database Administrator<br>• Application logs | • Disable suspected user accounts<br>• Reduce the interactive features and run with minimum essential features<br>• Restore data from trusted backup<br>• Identify attack sources from application logs and block<br>• Enforce Input validation<br>• Apply latest patches / updates<br>• Report to local Incident Response Team/CERT-In | • Web Administrator<br>• Database Administrator |
| **ROUTER LEVEL ATTACKS** | | | |
| • **Unexplained packet loss** | • Users<br>• Network Administrator | • Replace the router with securely configured standby router with | • Network Administrator |

| | | | |
|---|---|---|---|
| • **Non-availability of gateway/ internet services** | • Review of Router configurations | Egress and Ingress filtering<br>• Check the logs and configuration files of compromised router to identify attacks<br>• Replace the configuration files with trusted backup<br>• Apply appropriate patches / updates<br>• Block the attack source<br>• Report to local Incident Response Team/Service Provider/CERT-In | |
| **HIGH ENERGY RF BASED DENIAL OF SERVICES ATTACKS** | | | |
| • **Non-availability of wireless connectivity**<br>• **Degraded Signal to Noise Ratio**<br>• **Increased Noise Levels in the airwaves** | • Users<br>• Network Administrator<br>• Alerts on IDS/IPS | • Identify the other devices due to which RF interference occurs and physically remove them<br>• Detect rouge access points and remove them<br>• If attack persists, switch critical functions to wired networks<br>• Report to local Incident Response Team/CERT-In | • Network Administrator |
| **TARGETED SCANNING, PROBING AND RECONNAISSANCE OF NETWORKS AND IT INFRASTRUCTURE** | | | |
| • **Huge amount of IPS/IDS alerts**<br>• **High volume dropped packets by Firewalls**<br>• **Surge in specific traffic** | • Users<br>• Network Administrator<br>• Logs of relevant devices | • Identify the type of scans/probes by examining logs of Router/IDS/IPS/Firewall<br>• Identify the sources of scans<br>• Block the sources of scanning<br>• Report the incidents with relevant logs to CERT-In | • Network Administrator |

Department/Organisation may refer website  Cyber Swachhta Pakhwada 2022 of CERT.in and make efforts to increase awareness and avoid human error that leading vulnerabilities and cyber threat.

https://www.csk.gov.in/announcements/index.html



**Annexure**

## Format for providing Point of Contact (PoC) information by Service providers, intermediaries, data centres, body corporate and Government organisations to CERT-In

The Information relating to the Point of Contact shall be sent to CERT-In via email (info@cert-in.org.in) in the format specified below and shall be updated from time to time:

| | |
|---|---|
| Name | |
| Designation | |
| Organisation Name | |
| Office Address | |
| Email ID | |
| Mobile No. | |
| Office Phone | |
| Office Fax | |

## ACRONYMS &ABBREVIATION

| | |
|---|---|
| **APT** | ***Advance Persistent Threat*** |
| **CCMP** | ***Cyber Crisis Management Plan*** |
| **CERT-In** | ***Computer Emergency Response Team – India*** |
| **CIA** | ***Confidentiality, Integrity, Availability*** |
| **CII** | ***Critical Information infrastructure*** |
| **CISO** | ***Chief Information Security Officer*** |
| **DDoS** | ***Distributed Denial of Service*** |
| **DNS** | ***Domain Name System*** |
| **DoS** | ***Denial of Service*** |
| **DR** | ***Disaster Recovery*** |
| **DrDoS** | ***Distributed Reflection Denial of Service*** |
| **DVR** | ***Digital Video Recorder*** |
| **FTP** | ***File Transfer Protocol*** |
| **HTTP** | ***Hypertext Transfer Protocol*** |
| **HTTPS** | ***Hypertext Transfer Protocol Secure*** |
| **ICT** | ***Information Communication Technology*** |
| **ICS** | ***Industrial Control System*** |
| **IDS** | ***Intrusion Detection System*** |
| **IETF** | ***Internet Engineering Task Force*** |
| **IP** | ***Internet Protocol*** |
| **IPS** | ***Intrusion Prevention System*** |
| **IRC** | ***Internet Relay Chat*** |
| **ISMS** | ***Information Security Management System*** |
| **ISP** | ***Internet Service Provider*** |
| **IoT/IIoT** | ***Internet of Things/ Industrial Internet of Things*** |
| **IT** | ***Information Technology*** |
| **ISO** | ***International Organization for Standardization*** |
| **KPIs** | ***Key Performance Indicators*** |
| **KRIs** | ***Key Risk Indicators*** |
| **LAN** | ***Local Area Network*** |
| **LEAP/PEAP** | ***Lightweight Extensible Authentication Protocol/ Protected Extensible Authentication Protocol*** |
| **NCIIPC** | ***National Critical Information Infrastructure Protection Centre*** |

| | |
|---|---|
| **NIXI** | ***National Internet Exchange of India*** |
| **PLCs** | ***Programmable Logic Controllers*** |
| **SCADA** | ***Supervisory Control And Data Acquisition*** |
| **SLA** | ***Service Level Agreement*** |
| **SDLC** | ***Software Development Life Cycle*** |
| **SMTP** | ***Simple Mail Transfer Protocol*** |
| **SQL** | ***Structured Query Language*** |
| **SSL** | ***Secure Sockets Layer*** |
| **SWIFT** | ***Society for Worldwide Interbank Financial Telecommunication*** |
| **SSH** | ***Secure Shell*** |
| **URL** | ***Uniform Resource Locator*** |
| **VLAN** | ***Virtual Local Area Network*** |
| **VRM** | ***Vendor Risk Management*** |
| **WAN** | ***Wide Area network*** |
| **XSS script** | ***Cross Site Scripting*** |