Draft SOP

Handling Cyber Incidents / Attacks in UT of Puducherry

(Submitted for approval)

As the Puducherry Cyber Crime is the local nodal agency to coordinate and communicate with the Indian Computer Emergency Response Team (CERT-In), which is the national agency for performing various functions in the area of cyber security in the country as per provisions of section 70B of the Information Technology Act 2000.

In accordance with the notification issued by the MEITY (Notification No. 20(3)/2022-CERT-In dated 28th April 2022), the Puducherry Cyber Crime Unit has given the following guidelines to the stakeholders of Cyber Incident / Cyber attacks falling within the jurisdiction of Puducherry UT.

A. List of institutions covered under the notification:

As per the notification of MEITY (No. 20(3)/2022-CERT-In dated 28th April 2022), For example

1. Data Centers
2. Corporate Body
3. Government Organizations
4. Virtual Private Server (VPS) Providers
5. Virtual Asset Service Providers
6. Virtual Asset Exchange Providers
7. Custodian Wallet Providers
8. Cloud Service Providers
9. Virtual Private Network Service (VPN) Providers
10. All Intermediaries

B. Cyber security incidents must be reported to Cyber Crime PS in addition to Cert-In & I4C:

The following Cyber incidents/attacks must be reported immediately as per the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules in 2013. For example

1. Targeted scanning/probing of critical networks/systems.
2. Compromise of critical systems/information.
3. Unauthorized access to IT systems/data.

4. Defacement of website or intrusion into a website and unauthorized changes such as inserting malicious codes and links to external websites etc.
5. Malicious code attacks such as the spreading of viruses/ Ransomware/ Spyware/ Crypto miners/worms/ Trojan/ Bots.
6. Attack on servers such as Database, Mail, and DNS and network devices such as Routers.
7. Identity Theft, spoofing and phishing attacks.
8. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks
9. Attacks on Critical Infrastructure, SCADA and operational technology systems, and Wireless networks.
10. Attacks on Applications such as E-Governance, E-Commerce etc.
11. Data Breach.
12. Data Leak.
13. Attacks on Internet of Things (IoT) devices and associated systems, networks, software, and servers.
14. Attacks or incidents affecting Digital Payment systems.
15. Attacks through Malicious Mobile Apps.
16. Fake mobile Apps.
17. Unauthorized access to social media accounts.
18. Attacks or malicious/ suspicious activities affecting Cloud computing systems/ servers/ software/ applications.
19. Attacks or malicious/ suspicious activities affecting systems/ servers/ networks/ software/ applications related to Big Data, Blockchain, virtual assets, virtual asset exchanges, custodian wallets, Robotics, 3D and 4D Printing, additive manufacturing, and Drones.
20. Attacks or malicious/ suspicious activities affecting systems/ servers/software/ applications related to Artificial Intelligence and Machine Learning.

C. Mandatory Reporting of Cyber Incidents within 6 Hours:

According to the Directions of Cert-In, respective entities must report Cyber security incidents to the Cert-In and State Cyber Crime PS within 6 hours of becoming aware of them or being made aware of them. The incidents to be reported as per the contact details tabled below

CERT-IN:

1	Email	incident@cert-in.org.in
2	Phone	1800- 11-4949
3	Fax	1800-11-6969
4	website	www.cert-in.org.in

State Cyber Crime PS:

1	Email	Cybercell-police@py.gov.in
2	Phone	04132276144
4	Website	www.police.py.gov.in
5	Whatsapp	9489205246

D. Designated Single Point of Contact (SPoC)

All the entities who are covered under the above-mentioned notification of MEITY should designate a person as the Single Point of Contact.

The entities include of

1. The service providers, intermediaries, data centers, corporate bodies, and Government organizations shall designate a Nodal Officer as SPOC for coordination with CERT-In and State Cyber Crime PS. The details of the nodal officer/SPoC may be communicated to Cert-In and Cyber PS and to be periodically updated.
2. All communications from CERT-In / State Cyber PS seeking information and providing directions for compliance shall be sent to the designated SPoC/Nodal Officer

E. Mandatory Logs to be maintained

All institutes/entities, intermediaries, data centers, corporate bodies and Government organizations shall

1. Logs of all ICT systems
2. Logs to be preserved for a minimum period of 6 months.
3. Logs to be maintained within the Indian jurisdiction.

The above data is to be attached while reporting the incident/cyber attack or if requested by concerned authorities.

F. Mandatory maintenance of data for a minimum of Five Years

1. The virtual asset service providers, virtual asset exchange providers, and custodian wallet providers 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.
2. For the purpose of KYC, 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.

G. Other Mandatory Logs

Data Centers, Virtual Private Server (VPS) providers, Cloud Service providers, and Virtual Private Network Service (VPN Service) providers, shall be required to register the following accurate information which must be maintained by them for a period of 5 years or longer duration as mandated by the law after any cancellation or withdrawal of the registration as the case may be:

1. Validated names of subscribers/customers hiring the services
2. Period of hire including dates
3. IPs allotted to / being used by the members
4. Email address, IP address, and time stamp used at the time of registration/onboarding
5. Purpose for hiring services
6. Validated address and contact numbers
7. Ownership pattern of the subscribers/customers hiring services

H. Requirements of Maintaining Transaction Records:

With respect to transaction records, accurate information shall be maintained in such a way that individual transactions can be reconstructed along with the relevant elements comprising of, but not limited to, –

1. Identification of the relevant parties
2. IP addresses
3. Timestamps and time zones of transaction
4. Transaction ID
5. Public keys (or equivalent identifiers)
6. Addresses or accounts involved (or equivalent identifiers)
7. Nature and date of the transaction
8. Amount transferred

I. Advisory specific to Remote Access Trojan (RAT) malware

1. Update software, including operating systems, applications, antivirus and firmware, on IT network assets.
2. Prioritize patching known exploited vulnerabilities, critical and high vulnerabilities that allow for remote code execution or denial-of-service on internet-facing equipment.
3. Enforce MFA (Multi Factor Authentication) where login access required.
4. Minimize access of RDP connections, VPN and proxy connection from network.
5. Enforce plug-play USB device connection policy.
6. Implement User access control policy & Restrict users' ability (permissions) to install and run unwanted software applications.

7. Do not add users to the local administrators group unless required.
8. Exercise caution when opening email attachments even if the attachment is expected and the sender appears to be known.
9. Enable a personal firewall on agency workstations, configured to deny unsolicited connection requests.
10. Disable unnecessary services on agency workstations and servers.
11. Scan for and remove suspicious email attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
12. Scan all software downloaded from the Internet prior to executing.
13. Block malicious attachments to reduce the attack surface.
14. Uninstall any unwanted application or extension.
15. Maintain situational awareness of the latest threats and implement appropriate Access Control Lists (ACLs).
16. Implement Network defense solutions and install Firewall, IDS/IPS, and cyber threat intelligence solutions.
17. Implement network segmentation to separate network segments based on role and functionality.

J. Cyber Crime Helpline 1930:

The 1930 telephone Helpline number is functioning on a 24x7 basis for instantaneous reporting of Cyber Incidents/Attacks.

K. Mandatory Cyber Security Do's and Don'ts

I. Do's for administrator:

1. Physical access to network equipment, data centers, and server rooms, should be accessed by authorized personnel only.
2. Always check for attached unknown devices to the computer system whenever auditing any system.
3. Keep network cables organized and secure to prevent tampering or accidental disconnection.
4. Enable Power ON/BIOS password, Windows administrator (Main user) password, user account, screen saver password. Disable the guest account and delete the unwanted user accounts.
5. Enable the 'show hidden files' and 'File Extension' options.
6. Keep the Operating System software (Windows) up-to-date.
7. Enable built-in security features such as Microsoft Defender or reputed Anti-Virus software like Kaspersky and Quick Heal should be installed and which should be regularly updated.
8. Deploy a properly configured firewall.

9. Create a System Restore point (It can reverse harmful changes to your computer).
10. Periodically format the Internet/stand-alone computers.
11. The "HOSTS" file in the Windows operating system should be checked for any alterations. (This PC>OS (C:)>Windows>System 32> Drivers>etc>host> Open with notepad.)
12. Secure all the wireless access points (wi-fi, routers) with a strong password.
13. The Operating System of the computers used for NIC mail communications must be upgraded to the latest version of Windows.
14. Always review the application permissions before installing any mobile application.
15. If a single lease line of appropriate bandwidth is used to facilitate internet in organization it is recommended that it should be managed, monitored, controlled, and secured by deploying a Unified Threat Management System (UTM).
16. The unused ports of switches should be disabled.
17. Necessary measures to be taken for data security e.g. installing of NASS (Network attached Storage System). If any NASS is not available whitelisted external Hard disk may be used to take backups.
18. Unused USB ports should be disabled.
19. Regularly monitor network rules and access privileges.
20. Delete unneeded drivers and update those that are needed.
21. Before downloading an App, check the popularity of the app and read the user reviews. Observe caution before downloading any app that has a bad reputation or less user base, etc.
22. Use a Hardware Virtual Private Network (VPN) Token for connecting privately to any IT assets located in the Data Centers.
23. By default remote access may not be allowed from running remote desktop applications like Anydesk, TeamViewer etc which can give remote access and can make your computer system vulnerable.

II. Do's for user:

1. Always check for attached unknown devices to the computer system.
2. Keep network cables organized and secure to prevent tampering or accidental disconnection.
3. All removable media should be scanned with anti-virus software before use.
4. Enable show hidden files and File Extension option.
5. Enable screen saver with a timeout period of 5 minutes or less.
6. Keep good, hard-to-guess passwords for computer/e-mail accounts.

7. Use 'non-administrator account' privileges for login to the computer and avoid accessing with 'administrator' privileges for day-to-day usage of computers.
8. Use External Hard Drive to store Secret and Top Secret data.
9. CDs must be used for the transfer of operational data between our dedicated standalone computers.
10. Use your web browser's pop-up blocker.
11. Always sign out your e-mail account and other applications.
12. Regularly delete Temp folder files and temporary Internet files.
13. Enable the "Delete browsing history on exit' option in the Cookies folder.
14. Periodically change all passwords.
15. Make sure that your web/email access is via secure (https) connections.
16. Restrain from running remote desktop applications like Anydesk, TeamViewer, etc that can give remote access and can make your computer system vulnerable.
17. Save your data and files on the secondary drive (ex: d:\).
18. While sending any sensitive/secret information or document over an electronic medium, encrypt the data before transmission and share the password separately via other mediums.

III. Don'ts for Administrator

1. Do not interchange Stand-alone computers with Internet-connected ones and vice versa.
2. Do not allow computers to be repaired outside the office premises, in case of emergency HDD may be removed and retained at the office.
3. Do not enable Hot spots, free WiFi, or Internet. Officials are strictly prohibited from using any WiFi-enabled device in the office complex.
4. Do not enable Internet telephony services i.e. Skype, Googletalk, MagicJack Yahoo, etc on the router/firewall.
5. Do not enable unsolicited websites and untrusted VPNs on the router/firewall.
6. Do not add users to the local administrator's group unless required.
7. Do not give remote access, or file and printer sharing access to un-trusted computers.
8. Do not enable Social Networking sites like Facebook, Myspace, or X (Twitter). LinkedIn etc. on switches where sensitive systems are placed.
9. Do not leave the system unattended, always lock/log off from computer session, and always lock the IT room where servers are placed.
10. Do not allow any unauthorized person to enter the IT room.
11. Do not enable the internet and intranet on the same router/switches.

12. Do not download or install pirated software, or applications as it increases vulnerability to potential cyber threats.

IV. Don'ts for User

1. Do not reveal personal or financial information to anyone. Avoid uploading personal information on social media.
2. Do not use Pen drives.
3. Do not open e-mail from an unknown source.
4. Do not download files or applications from unknown sources/websites.
5. Do not open any email attachments received from untrusted sources and received unexpectedly from trusted sources. Even .doc, .pdf, etc may contain malware. Extension .pif, .scr, etc. are also executable attachments.
6. Do not click on any link in unsolicited e-mails, pop-up ads, or windows.
7. Do not open files sent via instant messengers from unknown sources.
8. Do not enable the Auto Saved option for the user ID and Password of the e-mail account.
9. Do not reveal your password or OTP to anyone
10. Do not do any operational work on the internet connected system.
11. Do not use free Internet Hot spots, free WiFi, or Internet. Officials are strictly prohibited from the use of any WiFi-enabled device in the office complex.
12. Do not use Internet telephony services i.e. Skype, Googletalk, MagicJack and Yahoo etc. for official purposes.
13. Do not install third-party/free software on your PC. E.g Adobe PDF Reader is free software but this should be installed only from the official Adobe website.
14. Do not browse unsolicited websites and never download files containing pornographic materials as these are used as honey-raps to trap unsuspecting users.
15. Avoid the use of official computers for online banking, shopping, entering credit card details, etc.
16. Do not use Social Networking sites like Facebook, Myspace, X (Twitter), Linkedin etc.
17. Be careful what you plug into your computer. Malware can spread through infected USB drives, external hard drives, and even smartphones.
18. Be aware of the sites that offer free Screensavers, anti-virus or anti-spyware software. These may spread malicious content on your device.
19. Do not download or install pirated software, or applications as it increases vulnerability to potential cyber threats.
20. Do not allow computers to be repaired outside the office premises, in case of emergency HDD may be removed and retained at the office.

21. Do not leave the system unattended, always lock/log off from the computer session.
22. Do not upload or save any internal/restricted/confidential government data or files on any non-government cloud service (ex: Google Drive, Dropbox, etc.).

L. Reporting format of Cyber Incident / Attack:

A Format has been prepared in accordance with the format recommended by the CERT-In. The Format is enclosed in the **Annexure (Incident Reporting Form)**. If any incident is reported the particulars should be sent to Cyber Crime Unit in this format.