I/78780/2022

No. J.15011/1/2016-e-Gov-Part (1)
Government of India
भारत सरकार
Ministry of Jal Shakti
जल शक्ति
Department of Water Resources, RD & GR
जल संसाधन, नदी विकास और गंगा संरक्षण विभाग
*****

श्रम शक्ति भवन,
रफी मार्ग, नई दिल्ली-1
21.12.2022

OFFICE MEMORANDUM
कार्यालय ज्ञापन

Subject – Cyber Security Best Practice for Compliance in the Department and its Organizations – reg.

I am directed to refer to the MeitY DO letter dated 08.09.2022 on the subject cited above, and to inform that the Department has prepared a 'Cyber Security Best Practice' to enhanced focus on cyber security.

2. The approved "Cyber Security Best Practice" for the Department and all the attached/subordinate offices as well as other organizations is attached for compliance.

3. All the Officers/Officials in the Department/Attached and Subordinate offices and other organizations are requested to take note on the Cyber Security Best Practice and to ensure compliance of the instruction mentioned therein.

Signed by Y.p.yadav
Date: 21-12-2022 09:58:51
Reason: Approved
(Y P Yadav)
Dy. Secretary(e.gov)

Encl: as above

To

All the Organizations/Wings/Divisions/Section heads of the Department (through email)

Copy to:

PPS to JS (Admn./IC & GW)

Cyber Security Best Practices

Department of Water Resources, River Development and Ganga Rejuvenation

Table of Contents

1.0 User's Roles and Responsibilities....2
1.1 Organization's Head....2
1.2 Chief Information Security Officer (CISO)....2
1.3 ICT Nodal Officer....4
1.4 IT Engineer....5
1.4.1 Software support....5
1.4.2 Hardware Support....5
1.4.3 Network Support....5
2.0 General Computer usage – Best practices....6
3.0 General Internet Browsing – Best Practices....7
4.0 Malware defence – Best practices....8
5.0 USB storage device (Pen Drive / External Hard disk etc.)....8
6.0 Smart device – Best Practice....9
7.0 Social Media Security....11
8.0 Email Communication Security – Best practices....12
9.0 Wi-Fi Device – Best practices....13
10.0 Password – Best Practices....14
11.0 Social Engineering – best practices....15
12.0 Best practices for Mobile Phones/ Tabs....16
13.0 Incident Prevention, Detection, Response....16
i. Incident Prevention....16
ii. Incident Detection....17
iii. Incident Response....17
14.0 Organization level Security Controls....18
15.0 Work From Home Environment (WFH)....18
16.0 Video Conferencing – Securing the VC Cameras....19

1.0 User's Roles and Responsibilities

The roles and responsibilities of officials across organization need to be defined as per their positions they chair. Following roles and responsibilities are envisaged for the effective monitoring in adoptions of best cyber security practices.

Level 1. Chief Information Security Officer (CISO)
Level 2. IT Nodal Officer / Security Manager
Level 3. Security Engineer
Level 4. IT Support Team

1.1 Organization's Head

Organization Head's roles and responsibilities are most important in achieving organization's objectives using ICT. Organization Head should take overview of following key areas to maintain & secure Cyber infra and eGov Apps.

- Critical ICT infrastructure security
- Application security
- Network security

1.2 Chief Information Security Officer (CISO)

IT Division Head / Chief Information Security Officer (CISO) roles is critical in implementation and maintenance of ICT services in the Organization. Following functionalities are to be performed by CISO.

i. Implementing and overseeing organisation's cyber security program

A key responsibility for a CISO within organisation is to provide guidance on cyber security program on a strategic level. It is a CISO's responsibility to make sure organisations remain compliant with cyber security standards, policy, regulations and legislation.

ii. Aligning cyber security and business objectives

CISO is to make sure that the objectives of organisation's cyber security program are in line with the goals that organisation hopes to achieve. One key function of this role is to ensure clear communication between security personnel and key stakeholders. It is also vital that CISOs SOPs on security measures that need to be put in place when new projects are started.

iii. Reporting on cyber security

CISOs play an important role when it comes to providing top line officers with intelligence on key cyber security trends. It is vital that CISOs provide upper-level management with a consolidated and comprehensive view of their organisation's cyber security posture.

iv. Monitoring Incident Response Activities

CISO plays key role in an organisation is during a security incident, it is the CISO's to oversee how well internal teams handle a cyber-security incident when it is identified. If needed a CISO is expected to step in and manage incident response, i.e. in a major security breach. Crisis management is the responsibility of the CISO. During a security incident, it is the CISO's to bring a level of clarity to the critical internal and external stakeholders. To be able to communicate information regarding incident response effectively to upper-level management, CISOs are required to monitor every single information security incident that occurs.

v. Managing business continuity and disaster recovery

Implementing existing business continuity and disaster recovery plans is another key role of a CISO. Security incidents can have numerous effects on an organisation's wellbeing. A CISO plays a vital role in managing business continuity in the aftermath of a security incident.

vi. Promote a culture of strong information security

Another key role of a CISO is to promote a culture of strong information security, and to facilitate broad security cultural change across the organisation, the CISO should act as a thought leader, continually communicating their strategy and vision. This can be effectively achieved by tailoring communications to different divisions/sections in the organisation and being topical for the intended audience

vii. Managing vendor relationships

There is a significant risk to your organisation's information security via the suppliers and service providers, officials work with. A CISO can help ensure that consistent vendor management processes are in place to mitigate these information security risks. For example, a CISO can advise and assist employees when assessing supply chain cyber threats and provide them with an understanding of the information security impacts of entering into vendor relationships.

viii. Utilising cyber security budgets effectively

It is also the responsibility of a CISO to use the allocated budget for an organisation's cyber security program efficiently and effectively. A CISO can help an organisation make decisions when it comes to investing in cyber security smartly.

ix. Overseeing cyber security personnel within the organisation

Cyber security isn't the sole responsibility of a chief information security officer, requires a team to ensure the well-being of an organisation's information security. Therefore the CISO is responsible for organisation's cyber security workforce, this includes plans to attract, train and retain personnel so that cyber security functions are being carried out in a timely manner.

x. Cyber security awareness and training

Finally, CISOs are also responsible for increasing the overall awareness of the importance of information security within the organisation. Cyber threats are constantly evolving with criminals adopting new and clever ways to trick employees; therefore it is the CISO's responsibility to ensure everyone within an organisation is well informed about the latest cyber threats. The development of an effective cyber security awareness and training program and overseeing its implementation is another vital role that a CISO plays.

To perform their role effectively Chief Information Security Officers (CISO) requires a multitude of technical and soft skills, such as the ability to make quick decisions, lead, communicate effectively and build relationships. Additionally, CISOs must adapt in order to maintain pace with the cyber threat landscape and new technologies, constantly learning on the job and picking up new skills. In this ever-shifting cyber world, CISOs require innovation and imagination in creating and delivering cyber security strategies for their organisations.

1.3 ICT Nodal Officer

IT nodal officer is key person for CISO in the organization to work consistently in maintaining following task assigned.

- Application security.
- Data loss prevention.
- Incident response.
- Network security.
- Security architecture.
- Threat intelligence.
- Vulnerability management.
- Set and implement user access controls and identity and access management systems
- Monitor network and application performance to identify and irregular activity
- Perform regular audits to ensure security practices are compliant
- Deploy endpoint detection and prevention tools to thwart malicious hacks
- Set up patch management systems to update applications automatically
- Implement comprehensive vulnerability management systems across all assets on-premises and in the cloud
- Work with IT operations to set up a shared disaster recovery/business continuity plan
- Work with HR and/or team leads to educate employees on how to identify suspicious activity

The IT Nodal officer shall work on the following areas for

- Provide information security awareness training to organization personnel
- Creating and managing security strategies
- Oversee information security audits, as per Cert-in guidelines and SOPs.
- Manage security team members and all other information security personnel
- Provide training to information security personnel during on-boarding
- Evaluate department budget and costs associated with technological training
- Assess current technology architecture for vulnerabilities, weaknesses and for possible upgrades or improvement
- Implement and oversee technological upgrades, improvements and major changes to the information security environment
- Serve as a focal point of contact for the information security team and the customer or organization
- Manage and configure physical security, disaster recovery and data backup systems
- Communicate information security goals and new programs effectively with other department managers within the organization

1.4 IT Engineer

1.4.1 Software support

- Ensure that Software/Applications should be developed using updated patches and vulnerabilities.
- Security Audit is regularly done and security audited codes are uploaded on web server for public domain
- Website need to be GIGW compliance and should be STQC certified.
- Operating System (OS) should be updated regularly with latest patches and as per SOPs
- Vulnerability Assessment (VA) should be regular i.e. every three month period.
- Each system should be over Anti-Virus with latest definition updates/signature updates.
- Regular /Scheduling for Antivirus Scanning for all the Desktop to be carried out.

1.4.2 Hardware Support

- Latest generation of HW items should be installed.
- External HDD/USB storage devices should not be used for data sharing. Instead of these use briefcase (NIC email).
- Obsolete Hardware should be recycled as per SOPs.

1.4.3 Network Support

- Network should be security audited.
- Sharing of System resources should not be allowed.
- Firewall policies should be implemented.

- Network Logs should regularly examined.
- All devices should be MAC-ID bind on IP with network switches.
- Wi-Fi Routers should be secured by Strong WPA2 key.

2.0 General Computer usage – Best practices

- Use account with limited privileges on systems and avoid accessing with administrator privileges for day-to-day usage.
- Keep Operating System, Application software and Anti-Virus software updated by applying the latest service packs and patches.
- Schedule Antivirus for Regular Scan of Complete files of Computer System
- Backup of important files at regular intervals.
- Do not leave system unattended. Log out of or lock your computer when stepping away, even for a moment
- Supervise maintenance or rectification of faults in the system by service engineers.
- Do not download unfamiliar software off the Internet.
- Remove unnecessary programs or services from computer: Uninstall any software and services you do not need.
- Restrict remote access. If file sharing is not required in your day-to-day work, disable file and print sharing.
- Treat sensitive data very carefully.
- Remove data securely: Remove files or data you no longer need to prevent unauthorized access to them. Merely deleting sensitive material is not sufficient, as it does not actually remove the data from your system
- If your networking devices are not using IPv6, disable IPv6 from computer.
- Always maintain a redundant power supply.
- Use systems screen locking functionality to protect against physical access, such as a screen saver that won't deactivate without a password, or just log out of everything so anyone that wants access has to log in again.
- Enable the option chassis intrusion in the BIOS settings to be aware of unauthorized users.
- The systems should be placed in a room which is dust free and has a good ventilation to avoid overheating of CPU.
- Do not plug the computer directly to the wall outlet as power surges may damage computer. Instead use a genuine surge protector to plug a computer.
- Scan all the files after you download whether from websites or links received from e-mails.
- Download anything only from trust worthy websites. Do not click links to download anything you see on unauthorized sites.
- Don't click the link or file and let it start download automatically, download the file and save where you want save and then run on the application.

- Never download from the links that offer free antivirus or anti spyware software, always download from trusted sites, if you are not sure about the site you are downloading, enter the site into favorite search engine to see anyone posted or reported that it contains unwanted technologies.

3.0 General Internet Browsing – Best Practices

- Always use updated anti-virus, Operating System and applications and browser.
- Use a web browser with sandboxing capability (like Google chrome, safari, etc.). Sandboxing usually contains malware during execution.
- Download software from trusted source only.
- Be wary of storing personal information on Internet.
- Do not store any information you want to protect on any device that connects to the Internet.
- Verify those you correspond with. It is easy for people to fake identities over the Internet.
- Make a habit of clearing history from the browser after each logout sessions.
- Delete Windows "Temp" and "Temporary Internet files" regularly.
- Avoid all cloud services (Google Drive, Dropbox, iCloud, Evernote, etc) that are based outside India.
- Avoid using services that require location information.
- Remember search engines track your search history and build profiles on you to serve you personalized results based on your search history (Use Search engine which Do not Store /Share Browsing data).
- Use Incognito/private mode of browsers while surfing internet for sensitive information.
- Be conscious of what you are clicking on/downloading.
- Some pop-ups have what appears to be a close button, but will actually try to install spyware when you click on it.
- Remember that things on the internet are rarely free. "Free" Screensavers, etc. generally contain Malware.
- Be wary of free downloadable software - There are many sites that offer customized toolbars or other features that appeal to users, which are likely to have backdoors.
- Don't follow email links claiming to offer anti-spyware software - Like email viruses, the links may serve the opposite purpose and actually install the spyware it claims to be eliminating.
- Frequently check unusual folder locations for document (.doc, docx .xls, .xlsx and .def) file extensions (in search options, select advanced search options, make sure you checked "Search System folder", "Search hidden files and folders" and "search subfolders")
- Avoid Internet access through public Wi-Fi.
- Never exchange home and office work related contents.
- Avoid posting of photos with GPS coordinates.

- Don't respond to email, instant messages (IM), texts, phone calls, etc., asking you for your password.
- Only click on links from trusted sources. Never click on a mystery link unless you have a way to independently verify that it is safe. This includes tiny URLs.

Be extremely careful with file sharing software. File sharing opens your computer to the risk of malicious files and attackers. Also, if you share copyrighted files, you risk serious legal consequences.

4.0 Malware defence – Best practices

- Always set automatic updates for Operating System, Anti-Virus and Applications. (My Computer -> properties -> automatic updates -> select Automatic and time)
- Enable hidden file & system file view to find any unusual or hidden files. (My computer -> tools -> folder options -> view -> select enabled with "Show hidden file and folders" option and disable "Hide protected operating system files")
- Turn off auto play (Windows OS 8 and above version :- Start -> Run -> type gpedit.msc -> Computer Configurations -> Administrative Templates -> Windows Components - > Select "AutoPlay Policies" -> Double Click at "Turn off Auto play" -> Select Enabled -> Set "Turn off Auto play on:" to "All drives" and Click OK.)
- Type: dir %temp% in "run" and delete all entries after opening any suspicious attachments.
- Type cmd in run and type netstat –na. Checkout foreign Established connection and IP addresses. Check the IP address for its ownership.
- Type "msconfig" in "run" and check for any unusual executable running automatically.
- Check Network icon (for packets received and sent) / ADSL lights for data in non browsing mode. Check data usage pattern in Mobile. If the outgoing is unusually high, then it is very likely that the system is compromised.
- Type " ipconfig/displaydns" in command prompt and look out for any URLs which you have not accessed recently.
- Always be cautious while opening attachments even from the known sources. Try to use non native applications for opening attachments. Example for word document use, WordPad to open the attachment.
- When in doubt, better to format the Internet connected computer rather than doing some "patch works".

5.0 USB storage device (Pen Drive / External Hard disk etc.)

- Damaged / faulty RISM should never be handed over to outsiders / manufacturer for repair.
- Sensitive information should be stored on removable media only when required in the cases of assigned duties.

- All media must be stored in a safe, secure environment
- All media must be handled with care and it must be ensured that it is not kept near magnetic material and not exposed to extreme heat or pollution;
- The computers should be enabled with "Show hidden file and folders" option and "Hide protected operating system files" should be disabled to view hidden malicious files in USB storage devices.
- Make sure there is no hidden file and folders present in the Media.
- Autorun/ Autoplay feature should be disabled in all the computers.
- Avoid Baiting. (Someone gives you a USB drive or other electronic media that is preloaded with malware in the hope you will use the device and enable them to hack your computer). Do not use any electronic storage device unless you know its origin is legitimate and safe.
- Scan all electronic media for Malware before use.

6.0 Smart device – Best Practice

Smart device is a device having any of the features like computation power, Internet access, storage capability, camera, recordings, GPS, etc. Smart phone, Tablets, etc. falls under this category.

Most of the Smart Phones and Tablets (Tabs) are having equal computing power of a normal Desktop / Laptop systems. These gadgets are capable of delivering many services on Video, Voice, GPS and other computational apps like any other computer. Therefore, all cyber security issues related to computers are also applicable to these devices. Following are some of the security concerns of Smart devices:

- These are equally vulnerable to malware attacks and data leakages as ordinary Internet connected computers.
- More application, features and service are available on Smart device for exploits than ordinary feature phones.
- These gadgets are known to be used for bugging (audio and video), monitoring call details, contents, SMS monitoring, sending malicious SMS, Emails, spoofing, and other malicious activities without the knowledge of the user.
- Android and IOS platform based Smart Phones and Tabs are known to have multiple vulnerabilities, which are being widely exploited by the attackers and adversaries.
- Smart device must not be used for sensitive telephonic conversation. The Wi-Fi and blue-tooth should be kept in turned-off mode.
- A low-end basic mobile phone without camera / internet / Wi-Fi may be carried for sensitive voice conversation and contact details.
- Internet connection in the Smart device will normally be kept in off-mode and it will be made on on need basis to access internet.
- No free Apps should be loaded in the Smart device.

- During repairs, do not leave Smart device unattended to deny the possibility of installation of malware.
- Relevant anti-virus software should be installed in the smart device.
- If the Smart device gets de-activated for any reason for few hours / one day, the service provider should be contacted immediately to ascertain the reason for deactivation.
- If the battery gets unusually discharged very fast or device gets heated up without any user activity, then it is very likely some malicious traffic is consuming battery.
- Free Wi-Fi should not be used at public places such as Airport. Turn off blue-tooth and Wi-Fi when use of the same is not required for operational purposes. Even when the same is in use, set default blue-tooth / Wi-Fi configuration to "non-discoverable".
- Compromised smart device should not be connected with computer even for the purpose of charging.
- Turn off the applications which are not needed.
- When device is idle, it should get locked and require a password / pin or swipe pattern. Set the device to lock in relatively short time.
- Don’t reply or click on link on SMS or messages sent by strangers.
- Don’t Root/jail-break your device as jail-breaking removes the restrictions on which apps can be installed or not installed. This removes the protection set by the company.
- Watch for un-authorized GPRS/data connection during idle mode of the Smart device.
- Check the memory frequently if any unusual data is stored there. Malware stores temporarily, the data collected in the memory of the phone till the same is sent to the destination.
- Suitable non-transparent tape/sticker may be applied to block the camera view.
- Think before you click, download, forward, or open. Before responding, registering, downloading or providing information, get the facts. No matter how tempting the text, image, or application is, if the download isn’t from a legitimate app store or the site of a trusted company, don't engage with the message.
- Understand the terms of use. Some applications claim extensive rights to accessing and leveraging your personal information. If the app requires more access to your account and/or device than is needed to run the service, do not continue. In addition, be aware that terms can change over time. Review your terms of use often.
- Be cautious with public Wi-Fi. Many Smartphone users use free Wi-Fi hotspots to access data (and keep their phone plan costs down). There are numerous threats associated with Wi-Fi hotspots. To be safe, avoid logging into accounts, especially financial accounts, when using public wireless networks.
- Disable Bluetooth and Near Field Communication (NFC) capabilities when not in use. Capabilities such as Bluetooth and NFC can provide ease and convenience in using your Smartphone. They can also provide an easy way for a nearby, unauthorized user to gain access to your data. Turn these features off when they are not required.

- Enable encryption. Enabling encryption on your Smartphone is one of the best ways to safeguard information stored on the device, thwarting unauthorized access.
- Securely dispose of your device. With the constant changes and upgrades in the Smartphone market, many are upgrading their devices on a regular basis. It is important that you wipe the information from your Smartphone before disposal. Additionally, make sure any SD cards are removed and erased. If you are not redeploying the SIM card to another device, then make sure your personal information stored on the SIM card is erased or destroyed.

7.0 Social Media Security

- Strongly recommended to use one dedicated device for posting & managing social media information for public.
- Managing social media at different devices for public posting may lead to leakage of security credentials as many devices stores user login details in local device history.
- The dedicated device should be used exclusively for managing department's official social media accounts only and should not be used for any other social media accounts/ tasks/ internet browsing etc.
- Use Multi-Factor authentication to secure the social media accounts.
- Limit and control the use/exposure of personal information while accessing social media and networking sites.
- Always check the authenticity of the person before accepting a request as friend/contact.
- Do not click on the links or files sent by any unknown contact/user.
- Do not publish or post or share any internal government documents or information on social media.
- Do not publish or post or share any unverified information through social media.
- Do not give share the @gov.in/@nic.in email address on any social media platform.
- It is recommended to use NIC's Sandes App instead of any 3rd party messaging app, for official communication. Do not store any information you want to protect on any device that connects to the Internet.
- Always use high security settings on social networking sites, and be very limited in the personal information you share. Monitor what others are posting about you on their online discussions.
- Use anti-virus and firewall software. Keep them and your browser, and operating systems patched and updated.
- Change your passwords periodically (recommended to changed monthly), and do not reuse old passwords. Do not use the same password for more than one system or service. For example, if someone obtains the password for your email, they can access your online banking information with the same password.
- Do not post anything that might embarrass you later, or that you don't want strangers to know.

- Do not automatically download, or respond to content on a website or in an email. Do not click on links in email messages claiming to be from a social networking site. Instead go to the site directly to retrieve messages.
- Only install applications or software that come from trusted, well-known sites. "Free" software may come with malware. Verify what information applications will be able to access prior to enabling them. Once installed, keep it updated
- Avoid accessing your personal accounts from public computers or through public Wi-Fi spots.
- Disable Global Position System (GPS) encoding. Many digital cameras encode the GPS location of a photo when it is taken. If that photo is uploaded to a site, so are the GPS coordinates, which will let people know that exact location.
- Whenever possible, encrypt communications with websites. It may be a feature (like HTTPS site rather than HTTP site) social network sites allow you to enable.
- Beware of unsolicited contacts from individuals in person, on the telephone, or on the Internet who are seeking corporate or personal data.
- Do not share usernames, passwords, credit cards, bank information, salaries, computer network details, security clearances, home and office physical security and logistics, capabilities and limitations of work systems, or schedules and travel itineraries.
- No legitimate service or network administrator will ask you for your password.
- Do not provide information about yourself that will allow others to answer your security questions—such as when using "I forgot my password" feature.
- Be thoughtful and limit personal information you share such as job titles, locations, hobbies, likes and dislikes, or names and details of family members, friends, and co-workers.
- Verify those you correspond with. It is easy for people to fake identities over the Internet.
- Do not click advertisement shown in the social web pages

8.0 Email Communication Security – Best practices

- Auto save of password should not be enabled.
- Users must check their last login details while accessing the Email account.
- Use of encryption and digital signature certificate (DSC) may be considered for mails deemed necessary.
- Email IDs should have a strong password (at least 13 characters with alpha numeric and special characters)
- Once in every 30 days the email passwords should be changed.
- Logout properly from mail accounts.
- Before opening any attachment, the same should be scanned through an updated anti-virus for malicious contents.

- Do not keep mails in Inbox, sent box, draft, etc. which are no longer required.
- User should type the complete URL in the browser instead of clinking links from other sources.
- Before accepting the SSL certificate, the user should verify the authenticity of the certificate.
- Make a habit of clearing history from the browser after each logout sessions.
- Do not open / forward / reply to suspicious E Mail. Do not click any URLs mentioned in the body of the E Mail text.
- Be cautious of Tiny URLs in Email contents.
- Do not open attachment having extension :EXE, DLL, VBS, U64, SHS, PIF , SCR Typical example .txt.exe , .doc.exe
- Some malicious program starts executing as soon as they appear on the Outlook Express preview pane. Disable that option (view -> layout -> uncheck "show preview pane"). Do not open unsolicited or unexpected attachments. If you can not verify an attachment is legitimate, delete it.
- Do not log in to web sites or online applications unless the login page is secure (HTTPS). Do not enter personal or sensitive information online unless you are using a trusted, secure web page.
- Internet users may be advised to follow the basic email security practices mentioned below:
    - Not to open/reply email links (hyperlinks/web links/URLs mentioned in the body of such mails) claiming to offer anti-spyware software. The links may serve the opposite purpose and actually install the spyware it claims to be eliminating.
    - Scan mail attachments before downloading / opening.
    - Use two factor authentication wherever possible.
    - Use different email accounts for personal and professional purposes.
    - Periodically check last log-in activity for any unauthorized access.
    - Change passwords of all their online accounts (emails and others) from another secure computer, if any suspicious activities like email access from foreign IP addresses, etc. are noticed.

9.0 Wi-Fi Device – Best practices

- Information/Data on the Wi-Fi Network should always be in the encrypted form.
- Do not connect the access point directly to the wired network. As there is a chance of compromised wireless client in turn effecting the systems in the wired network, a firewall and an antivirus gateway should be placed between the access point and the wired network
- In order to allow authorized users to connect to the access point, wireless clients should be provided access based on MAC address.
- Do not auto-Connect to open Wi-Fi Networks.
- Do not use WEP encryption use WPA2 or higher graded encryption
- Don't use easy guessable password for Wifi Router/Access point like (your Name, Mobile Number, 12345, Admin etc).

- Change your SSID (Wireless Network Name)
- Turn off SSID broadcasting.
- Change the default passwords while configuring the access point/Wifi Router.
- When the number of users accessing the access point is less, it is recommended to disable the DHCP service. As this may make the attackers easy, to connect to the network once they get associated with the access point.
- Update the firmware of access point. It will reduce the number of security loop holes in the access point.

10.0 Password – Best Practices

- Passwords must be changed at regular intervals.
- Always use different passwords for different accounts.
- Do not share passwords with anyone.
- All passwords are to be treated as sensitive.
- Passwords should never be written down or stored on-line without encryption.
- Do not reveal a password in email, chat, or other electronic communication.
- Do not reveal a password on questionnaires or security forms
- Always decline the use of the "Remember Password" feature of applications
- All users should be aware of how to select strong passwords.
- Strong passwords contain combination of lower case characters, upper case characters, numbers, “Special” characters (e.g. @#$%^&*()_+|~-=\`{}[]:";<>/ etc).
- Contain at least thirteen alphanumeric characters (except in the case of BIOS, if the same is not possible).
- Weak passwords have the following characteristics:
    - The password contains less than thirteen characters
    - The password is a word found in a dictionary (English or foreign)
    - The password is a common usage word such as: Names of family, pets, friends, colleagues, Movie / Novel / Comics characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patterns like aaaaa, qwerty, asdfg, zxcvb, etc.
- Password history should be enforced wherever possible to ensure that the users are forced to select different passwords with a user account.
- Maximum password age should be configured to enforce the period of time (90 days) that a password can be used before the system forces the user to change it.
- Always use different passwords for different accounts.
- Do not reveal a password in email, chat, or other electronic communication.

- Do not speak about a password in front of others.
- Do not hint at the format of a password
- Do not reveal a password on questionnaires or security forms

11.0 Social Engineering – best practices

Social Engineering is an approach to gain access to information through misrepresentation. It is the conscious manipulation of people to obtain information without realizing that a security breach is occurring. It may take the form of impersonation via telephone or in person and through email.

- Some emails entice the recipient into opening an attachment that activates a virus or malicious program in to your computer.
- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person authority to have the information.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
- Don't send sensitive information over the Internet before checking a websites security. Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information.
- Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic.
- Take advantage of any anti-phishing features offered by your email client and web browser.
- If you believe your financial accounts may be compromised, contact your financial institution immediately and close any accounts that may have been compromised. Watch for any unexplainable charges to your account.
- Immediately change any passwords you might have revealed. If you used the same password for multiple resources, make sure to change it for each account, and do not use that password in the future.
- Don't make you mobile phone as a source for your personal data, which is dangerous if it falls in to the hands of strangers. It is advisable not to store important information like credit card and bank cards passwords, etc. in a mobile phone.

- Note the IMEI code of your cell phone and keep it in a safe place. This helps the owner to prevent access to the stolen mobile. The operator can block a phone using the IMEI code.

12.0 Best practices for Mobile Phones/ Tabs

- Do not store any classified / sensitive data (text / video / photograph) in the device.
- Before downloading any App, same should be checked for its reputation / review. Read vendor privacy policies before downloading apps and app permission should be reviewed closely
- Disable installing of third party apps from unknown sources.
- Disable background data for apps.
- Avoid use of wallet aggregator apps, which stores / links other e-wallets and bank apps.
- Auto start, data usage for each App and App permission should be controlled through the security features available (depends on OS and make of the phone)
- Review the default privacy settings of smart phone apps or services and, if needed, change the settings; e.g. settings about whether or not to attach location data to images, to social network posts, etc.
- Relevant anti-virus software should be installed in the smart device and same be updated regularly.
- Turn off GPS location services when not needed.
- Turn off / remove the apps which are not needed.
- When device is idle, it should get locked and require a password /pin or swipe pattern. Set the device to lock in relatively short time.
- Take back-up of data (contacts, personal photos, etc.) on external media
- Do not reply or click on link on SMS or messages or photos sent by strangers.
- Be cautious with public Wi-Fi. Many Smartphone users use free Wi-Fi hotspots to access data (and keep their phone plan costs down). There are numerous threats associated with Wi-Fi hotspots.
- To be safe, avoid logging into accounts, especially financial accounts, when using public wireless networks.

13.0 Incident Prevention, Detection, Response

i. Incident Prevention

- Use firewalls to create a buffer zone between the Internet and other untrusted networks used by creating firewall rules to deny traffic by white-listing only authorised protocols, ports and applications to exchange data across the boundary to reduce the exposure of systems to network based attacks.
- To limit the lateral movement as well as other attack activities, use end point / network firewall to prevent Remote Procedure Call (RPC) and Sever Message Block (SMB) communication among endpoints whenever possible

- Adopt application whitelisting policy on all endpoint workstations to prevent malicious code or unauthorized software from gaining execution on endpoints
- Remove unused or unpatched software from the computer, particularly remote desktop software, if any
- Ensure that application control (to allow only approved scripts to run) prevents unapproved programs running regardless of their file extension
- Ensure all end point systems having antivirus or a malware protection program running on it and is always up to date with latest signatures
- To mitigate certain malware family, which executes from user directory, block execution from user profile directories (%AppData%, %LocalAppData%, %TEMP%) and its subdirectories.
- To prevent malicious scripts from running on click, the notepad program can be associated (with always use this app option) with script file extensions such as .hta, .js, .jse, .vbs, .vbe, .wsf and .psl
- Perform regular red-team / blue team exercises on the network to re-establish the rules, configurations and policies
- Conducting of phishing drills among users via simulation will make them more sensible to handle such attacks.

ii. Incident Detection

- Monitor DNS activity for potential indications of tunnelling and data exfiltration.
- Regularly check for configuration changes and appropriate usage of configuration for possible intrusion.
- Deploy Microsoft Syslnternals Tool 'SysMon' to monitor and log system activity to the Windows Event Log.
- Block / Restrict connectivity to the malicious domains /IPs shared by various security agencies. Take the forensics image of the identified machine connecting to such domains after Isolating.
- Restore the system to a last-known good back up or proceed to a fresh installation.

iii. Incident Response

- Disconnect the infected computers from LAN / Internet immediately;
- Remove unused or unpatched software from computers, particularly remote desktop software, if any;
- Change passwords of all email and online services from another secure computer;
- Hard disks of the infected computers may be formatted after taking backup of data files;
- Operating systems and applications should be re-installed from clean software;
- Backup data should be scanned for virus before restoring it.

14.0 Organization level Security Controls

- Enforce Multi-factor Authentication (MFA) to prevent phishing attacks that steal email credentials. In case MS Office 365 is being used MFA should be enabled. MFA should also be enabled for Windows logins which would be effective against brute force attacks particularly using Remote Desk Protocol (RDP).
- Enable network segregation (partitioning of a network to keep critical parts of the infrastructure away from the internet and from less secure internal networks) to contain malicious activity and prevent successful propagation of the malware. This can prevent direct attacks on systems that should not be internet facing. Effective monitoring of log-ins and auditing of sensitive data can be put in place to ensure that the data is tracked.
- Install Anti-Phishing software that can run on the mail server and examine emails for any hyperlinks containing phishing websites/malwares. This can prevent credential loss and malicious code execution through phishing.
- Ensure Patch management (software running on the network is patched and up-to-date) is done on regular basis especially on servers where unpatched remote desktop software if present could lead to cyber-attacks. Else remove unused or unpatched software from computers, particularly remote desktop software. Close ports that need not be connected to the internet
- Enforce Password policy in the organization to ensure that a minimum strength of password is complied with across the network. This would help in preventing brute force attacks and from attackers taking advantage of default passwords.
- Periodical audit of IT systems to be carried out.
- Legacy computers (particularly internet facing servers) to be taken off so as to reduce attack surface.
- Educate staff on phishing attacks and email Compromise frauds.
- Use Firewall Access Control Lists to restrict direct network access to user machines so only approved devices are allowed to connect to them.
- Perform regular backups to allow quick restoration of impacted devices. Ensure backups are kept offline and make sure there is a recovery plan in place.
- To secure the web application, regular Vulnerability Assessment and Penetration Testing (VAPT) of the entire ICT systems from competent auditors and testers, may be carried out.

15.0 Work From Home Environment (WFH)

- Only approved users and devices by the head of the organization should be allowed.
- The organizations must ensure provision of accessing personal computer / devices of employees is done in a standardized and secure manner.

- Appropriate device configuration must be maintained and security capability must be deployed, to prevent remote access of data from outside the organizations boundary by allowing only approved devices based on the unique parameters (MAC ID, IP etc.) of the device.
- Two factor authentications should be implemented on different communication channels (like SMS for OTP and user name and password through secure protocol over the Internet).

16.0 Video Conferencing – Securing the VC Cameras

VC cameras, which are not protected with any password or having weak password, could be exploited to eavesdrop into the on-going video conferencing, monitor calls, read call logs, CDR's of VC, intrude/interrupt on-going call, etc. The vulnerability could be further exploited through remote maintenance module to switch on the camera and monitor activities. To prevent such attacks:

- Set a strong password to manage the VC camera.
- Disable administration interfaces from remote access.
- Disable use of default accounts/passwords.
- Check periodically to detect any misconfigurations or missing patches.

For Secure use of commercial VC solutions for discussions between Governments and parent partner organizations

- A separate system may be designated by the organization. Such system should not store any classified or sensitive information
- The background for the meeting should be chosen in such a manner (like plain wall, curtains or background option of the VC application) no sensitive documents / surroundings are visible during VC.
- Wherever possible, an isolated Internet connection should be preferred for such VCs. Logical isolation may also be considered for VC systems so that other internal systems are not exposed to the VC network.
- Don’t Share VC/Meeting link with any unauthorized persons or Don’t Post link on Social Media.