

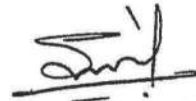
**CIRCULAR**

Sub: **Regarding Emergency Security Alert and Information Security**

This is reference to the subject and guidelines issued by the Ministry of Home Affairs "Information Security Best Practices" regarding basic precautions need to be taken by the Government Officers/Officials for the sake of information security and safeguarding Govt. Websites, Applications and ICT infrastructure.

Considering the aforesaid guidelines/practice directions and for the sake of data security, all the Judicial Officers/Officers/Officials posted within the jurisdictions of Central & West District are requested to adhere to the guidelines/practice directions contained in the "Information Security Best Practices" accessible on official website of Delhi District Courts ([www.delhidistrictcourts.nic.in](http://www.delhidistrictcourts.nic.in)).

This issues with the prior approval of Learned Principal District & Sessions Judge (HQs) and Learned Principal District & Sessions Judge (West).



(Sunil Kumar Sharma)  
Addl. Sessions Judge (West)/  
Officer In-Charge (Computers)  
Tis Hazari Courts, Delhi

Ref. No. 34597 - 34997 /CIS/S.R.(143)/THC/2023

Dated : 11 SEP 2023

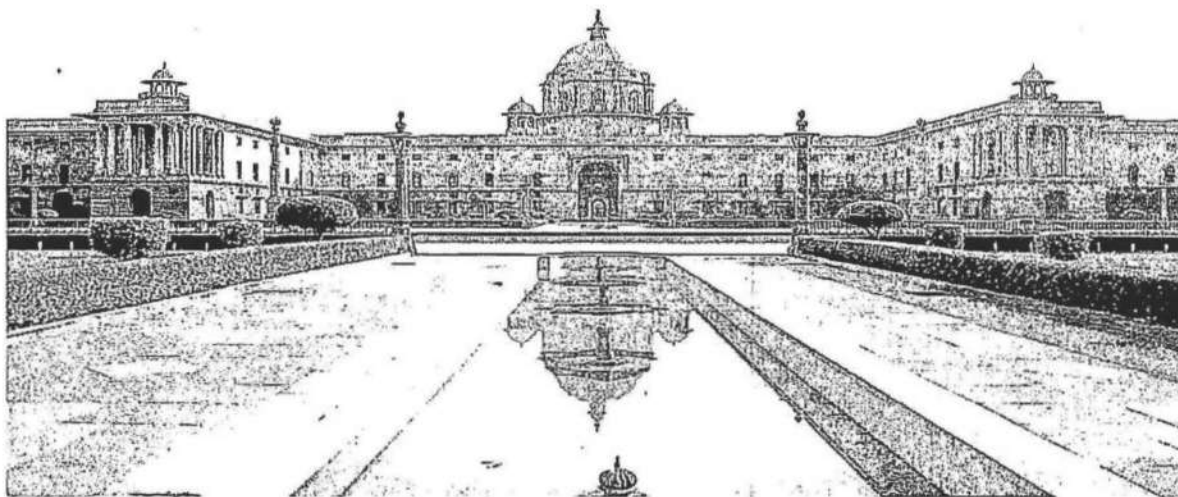
Copy forwarded for information and necessary action to:

1. Ld. Principal District & Sessions Judge of all districts except Central & West district with a request to convey the information to all concerned posted within the respective district.
5. All the Judicial Officers posted within the jurisdiction of Central and West District with a request to direct the staff posted under their kind control to adhere to the security guidelines as "Information Security Best Practices, issued by the Ministry of Home Affairs" available on the website of Ministry of Home Affairs and Delhi District Courts.
2. Sh. Pawan Kumar Jain, Chairman (IT & Digitization)/Centralized Computer Committee, Tis Hazari Courts, Delhi.
3. The Officer In-charge (Computers) of all districts/court complexes except Central & West District, Delhi/New Delhi.
4. PS to Id. Principal District & Sessions Judge (HQs) with request to place before Id. Principal District & Sessions Judge (HQs), Delhi.
5. PS to Id. Principal District & Sessions Judge (West) with request to place before Id. Principal District & Sessions Judge (West), Delhi.
6. Dealing Official (Website) to provide the link and upload the document as "Information Security Best Practices, Ministry of Home Affairs" on Delhi District Court Website.
7. Dealing Official {LAYERS (R&I) Central & West District/Website} to upload the same on the LAYERS/Website.

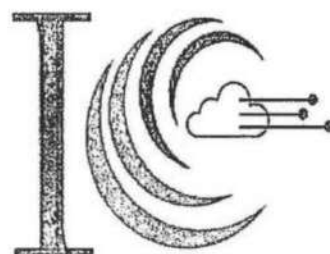


(Sunil Kumar Sharma)  
Addl. Sessions Judge (West)/  
Officer In-Charge (Computers)  
Tis Hazari Courts, Delhi

# INFORMATION SECURITY BEST PRACTICES



**MINISTRY OF HOME AFFAIRS**



Indian Cyber Crime Coordination Centre

# INFORMATION SECURITY BEST PRACTICES

## Table of Contents

1. Introduction.....	3
2. General Computer Usage.....	3
3. General Internet Browsing.....	5
4. Password Management.....	9
5. Removable Information Storage Media.....	12
6. Email Communication.....	15
7. Home Wi-Fi Network.....	16
8. Avoiding Social Engineering Attacks.....	17
9. Glossary.....	20

# INFORMATION SECURITY BEST PRACTICES

## 1. Introduction

Ministry of Home Affairs, Cyber & Information Security (CIS) Division has prepared this document to disseminate Information Security best practices for the benefit of Government Officials/Officers.

This should not be considered as an exhaustive list of prescription for Information Security but basic minimum precautions to be taken. Each organization should identify additional measures for information security in accordance with their use scenarios, sensitivity of data, business continuity and other relevant factors.

## 2. General Computer Usage

Following are some of the best practices for computer use on day to day basis:

- 2.1 All classified work should be strictly carried out only in a standalone computer which is not connected to the internet.
- 2.2 Create strong passwords for login by using a combination of letters, numbers, and special characters with minimum of 10 characters.
- 2.3 Computers should be protected from virus/worms using an Antivirus software permitted for use by your organization.
- 2.4 Make sure your operating system, application and software patches including anti-virus software are up to date; and auto updates are turned on in your computer.
- 2.5 Don't leave the computer unattended with sensitive information on the screen.

## INFORMATION SECURITY BEST PRACTICES

- 2.6 Always lock your computer before leaving workplace to prevent unauthorized access. A user can lock computer by pressing 'ctrl +alt+del' and choosing 'lock this computer' or "window button+ L".
- 2.7 Enable a password-protected screen saver with a timeout period of 2 minutes to ensure that computers that were left unsecured will be protected.
- 2.8 Be careful of what you plug in to your computer. Malware can spread through infected USB drives, external hard drives, and even smart phones.
- 2.9 Use non-administrator account privileges for login to the computer and avoid accessing with administrator privileges for day-to-day usage.
- 2.10 Treat sensitive data very carefully and use encryption to securely encode sensitive information.
- 2.11 Backup your important files at regular intervals to avoid unexpected loss.
- 2.12 Remove unnecessary programs or services from computer which are not required for day to day operation.
- 2.13 Do not give remote access, file and print sharing option to other computers.
- 2.14 Do not use file sharing softwares as file sharing opens your computer to the risk of malicious files and attacks.
- 2.15 Avoid entering sensitive information onto a public computer like cyber cafe, library computers etc.,

## INFORMATION SECURITY BEST PRACTICES

- 2.16 If you store or download any personal information on computers in cyber café, make sure you delete permanently all the documents after you are done with your work. You may press Shift and Delete button together to make it difficult to recover deleted files.
- 2.17 Remove files or data you no longer need to prevent unauthorized access to such data. Merely deleting sensitive material is not sufficient, as it does not actually remove the data from your system. File shredder software should be used to delete sensitive files on computers.
- 2.18 Ensure to use un-interrupted power supply to computers through UPS or other backup sources.
- 2.19 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.
- 2.20 The systems should be placed in a room which is dust free and has a good ventilation to avoid overheating of CPU.

### **3. General Internet Browsing**

Following are some of the best practices to keep in mind when browsing on Internet:

- 3.1. Always be careful when clicking on links or downloading. If it's unexpected or suspicious for any reason, don't click on it.
- 3.2. Do not download any type of files/software from any source other than those allowed by your system administrator/department.
- 3.3. Use web browser which has been permitted by your Organization.



## INFORMATION SECURITY BEST PRACTICES

- 3.4. Always use updated web browser for browsing. If you run a web browser that is out of date, it may contain security vulnerabilities and you risk having your computer compromised. Depending on the security exploit, your personal information (including emails, banking details, online transactions, photos and other sensitive information) could be stolen or destroyed.
- 3.5. Do not store/ share any sensitive information on any device that is connected to the Internet.
- 3.6. The "Save password" option prompted by the browser should not be selected if a window appears after entering information on the login screen, asking you to do so. Don't save account information, such as passwords or credit card information in web browsers, especially on those PCs which are shared with other users.
- 3.7. Look for HTTPS sign in the browser address bar. The "s" in "https" stands for secure, meaning that the website is employing SSL encryption. Check for an "https:" with a green padlock icon in your browser address bar to verify that a site is secure.
- 3.8. Make a habit of clearing history from the browser after each logout session. Following are the settings in various browsers to automatically clear the history on each browser session ends:

### Chrome

- Click on the menu icon in the upper right corner and select **Settings**> Show **advanced settings...**>**Privacy** and then tap the **Content settings** button.

## INFORMATION SECURITY BEST PRACTICES

- In the next window that opens, under Cookies, enable the option that says "**Keep local data only until you quit your browser.**"
- Press **Done** at the bottom of the window.

### Firefox

- Click on the menu icon in the upper right corner and select **Options**. Then in the window that opens, click on the **Privacy** tab.
- Under **History**, click the drop down menu next to "Firefox will:" and select Use **custom settings for history**.
- Check the option **Clear History when Firefox** closes.
- Once you're done click **OK**.

### Internet Explorer

- Click **settings** icon in the upper-right corner of the browser and select **Internet Options**.
- Open the **General Tab** in the window that appears.
- Under the **Browsing History** section, check the box next to "**Delete browser history on exit.**" Once you're done click **OK**.

3.9. No classified information of government can be stored on private cloud services (Google drive, Dropbox, iCloud etc.,) and doing so may make you liable for penal action, in case of data leakage.

3.10. When on tour, avoid using services that require location information, unless it is necessary for discharge of office duties.



## INFORMATION SECURITY BEST PRACTICES

- 3.11. While browsing, some pop-ups may appear with option of close button. These may be fake and may actually try to install spyware when you click on it. Beware of such pop-ups and avoid clicking on it.
- 3.12. Popup blocker option should be kept **turned ON** in the browser and may be selectively allowed for trusted sites, if required. Doing so will help prevent any nuisance web ads or malware embedded in ads from appearing on screen. Following are the settings to turn on popup blocker configuration in various browsers:

### Firefox

- Select **Tools** from the Mozilla Firefox taskbar
- Select **Options** from the drop-down menu
- Select **Content** from the Options dialog box
- To enable all pop-ups, check the **Block pop-up windows** radio button
- Click **Close**

### Chrome

- Click on the **Menu**
- Click on **Settings**
- Scroll to **Privacy**, Click on **Content Settings**
- Scroll to **Pop-Ups**
- **Uncheck** Allow All Sites to show Pop-Ups

## INFORMATION SECURITY BEST PRACTICES

- Click **OK**

### Internet Explorer

- Click **Tools** menu
- Click **Internet Options**
- Click **Privacy** tab
- Under Pop-up Blocker, Check **Turn on Pop-up Blocker**
- Click **OK**

- 3.13. Remember that things on the internet are rarely free. "Free" Screensavers etc., often contain malware. So be aware of such online free offers.
- 3.14. Avoid using public computers and public Wi-Fi connections to access and carryout any financial or sensitive transactions. Accessing government email on such computers has a risk of causing information breach.
- 3.15. If your job requires you to access certain information systems in a secure way, it is advisable to use security controls such as MPLS link, VPN over internet etc., for such access.

## 4. Password Management

Unauthorized access is a major problem for anyone who uses a computer or devices such as smartphones or tablets. The consequences for victims of these break-ins can include the loss of valuable data such as classified information, personal data etc. One of the most common ways that hackers break into computers is by guessing passwords. Simple and

## INFORMATION SECURITY BEST PRACTICES

commonly used passwords enable intruders to easily gain access and control a computing device.

Following are some of the best practices to consider while setting up and managing a password,

- 4.1. Create strong password with a minimum length of ideally 10 characters and comprising of mix of alphabets, numbers and characters.
- 4.2. All passwords (e.g., email, computer, etc.) should be changed periodically at least once every three months.
- 4.3. Don't reuse old passwords.
- 4.4. Passwords should not be stored in readable form in computers, notebook, notice board or in any other location where unauthorized persons might discover or use them.
- 4.5. Treat passwords as sensitive information and do not share it with anyone.
- 4.6. Always use different passwords for every log-in accounts you have. Using the same password for more than one account risks multiple exposures if one site you use is hacked.
- 4.7. If your work requires you to communicate passwords, such as while sending password for an encrypted file sent as an attachment through email it must be communicated through a different channel such as over a phone call or SMS.
- 4.8. Always decline the use of the "Remember Password" feature wherever it is prompted by the applications.

## INFORMATION SECURITY BEST PRACTICES

4.9. Remember weak passwords have the following characteristics:

- The password contains less than 10 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 123456, aaaaa, qwerty, asdfg, zxcvb, etc.

4.10. Some suggested way to construct a strong password are as follows,

- A secure password not only consist of letters, must also use numbers, special characters and caps. One suggested way to replace letters with numbers and special characters, so an "i" will become "!", an "o" turns into a "0" and "s" is written as "\$". This way, the simple term "Microsoft" changes to the substantially harder word "**M!cr0\$oft**".
- Password length matters, the longer the password, the harder it is to crack.
- Think of a sentence and select the first letters of each word in a row will get a complex password and easy to remember as well.

## INFORMATION SECURITY BEST PRACTICES

For example, sentence like this, "My Name is Dinesh Anandan and I was born on 1 January 1986!" would produce the following password: "MNiDAalwbo1J1986!". It's long, contains numbers, special characters, caps and letters, and it's easy to remember and won't be in dictionary.

### 5. Removable Information Storage Media

One of today's biggest security concern is the use of removable storage devices (USB devices such as pen drives, CD-RW, DVD-RW, Blu-ray discs, Media cards etc.,) in their networks. The amount of data that can be quickly copied to removable storage devices is increasing every day. While these devices can significantly boost productivity, they can also cause dangerously high risks in data security and control policies.

External removable portable storage devices allow users to bypass perimeter defenses, including firewalls and email server anti-malware, and potentially introduce malware into the office network. Since the malware enters the network from an internal device, it may go undetected until significant damage is caused to the network. Removable storage devices also facilitate easy pilferage of sensitive information from an organization's premises. This information might include classified information.

Following are some of the best practices to be considered while dealing with Removable storage media:

- 5.1. Auto run/ Auto play feature must be disabled for all removable media.

## INFORMATION SECURITY BEST PRACTICES

- 5.2. The classified data should be encrypted before copying into the removable storage media designated to store classified information.
- 5.3. Classified information should be stored only on organization allocated removable storage media for work purpose.
- 5.4. The computers should be enabled with “Show hidden file and folders” option to view hidden malicious files in USB storage devices.

Steps to enable hidden file & system file view to find any unusual or hidden files in computer are as follows:

### **Windows 10**

- In the search box on the taskbar, type **folder**, and then select **Show hidden files and folders** from the search results.
- Under **Advanced settings**, select **Show hidden files, folders, and drives**, and then select **OK**.

### **Windows 8.1**

- Go to **Search**.
- Then type **folder** in the search box, then select **Folder Options** from the search results.
- Select the **View** tab.
- Under **Advanced settings**, select **Show hidden files, folders, and drives**, and then select **OK**.

### **Windows 7**

- Select the Start button, then select **Control Panel -> Appearance and Personalization**.



## INFORMATION SECURITY BEST PRACTICES

- Select **Folder Options**, then select the **View** tab.
- 5.5. It is advisable to scan all removable media with anti-virus software before use.
  - 5.6. Removable media like USB's, CDs etc., must not be left unattended.
  - 5.7. Technical controls may be implemented to restrict use of portable storage media drives outside of the Government network.
  - 5.8. Removable media should not be taken out of office unless permitted by the competent authority in your office.
  - 5.9. In order to minimize physical risk, loss, theft or electrical corruption, all storage media must be stored in an appropriately secure and safe environment.
  - 5.10. In case of damage or malfunction of device, the same should be returned to the designated authority in your office for repair/replacement. Never ever handover such devices to outsiders or other vendors for repair as it might have classified information.
  - 5.11. If the USB device is no longer a functional requirement after issuance, then the same should be returned to the issuing authority.
  - 5.12. The contents of removable media must be removed/erased after the official purpose has been served.

## INFORMATION SECURITY BEST PRACTICES

### 6. Email Communication

Following are some of the best practices in regards to email communication:

- 6.1. Use only Government provided email address for official communications (e.g. nicemail).
- 6.2. System administrator may deploy appropriate controls to restrict use of personal email address for any official communications.
- 6.3. Avoid downloading email attachments or clicking on suspicious links received in emails from unknown or untrusted sources.
- 6.4. Classified information be not communicated via emails. In case of emergent requirements to do so, the approval of competent authority should be obtained.
- 6.5. Avoid accessing official email accounts from public Wi-Fi connections.
- 6.6. Auto save of password for email accounts should not be enabled.
- 6.7. Logout from mail accounts after your work is done.
- 6.8. User should type the complete URL in the browser instead of clicking links received in an email.
- 6.9. Do not open / forward / reply to any suspicious e-mails.
- 6.10. Be cautious on tiny or shortened URL's (appears like <http://tiny.cc/ba1j5y>) and don't click on it as it may take you to a malware infected website.

- 6.11. Do not open attachment having extension such as EXE, DLL, VBS, SHS, PIF, SCR. Typical example., .txt.exe, .doc.exe

### **7. Home Wi-Fi Network**

With the mass explosion of Laptops, Smart Phones and Tablets, pervasive wireless connectivity is widely used an option for connecting to the Internet. Insecure wireless configuration can provide an easy open door for malicious threat actors. Government officials may use their home Wi-Fi network to do office work and in order to secure their home Wi-Fi network, following are some of the best practices:

- 7.1. Turn on WPA2 or higher encryption feature in wireless routers.
- 7.2. Change the default network device name, also known as its service set identifier or "SSID." When a computer with a wireless connection searches for and displays the wireless networks nearby, it lists each network that publicly broadcasts its SSID. It is advisable to have SSID name which does not disclose your identity in any manner.
- 7.3. Change the network device default password. Unauthorized users may be familiar with the default passwords, so it is important to change the router device's password.
- 7.4. Consider using the Media Access Control, or "MAC," address filter in your wireless router. Every device that can connect to a Wi-Fi network has a unique ID called the "physical address" or "MAC" address. Wireless routers can screen the MAC addresses of all devices that connect to them, and users can set their wireless network to accept

## INFORMATION SECURITY BEST PRACTICES

connections only from devices with MAC addresses that the router will recognize. To create another obstacle to unauthorized access, consider activating your wireless router's MAC address filter to include your devices only.

- 7.5. Turn off your wireless router when not needed for any extended period of time.
- 7.6. Update the firmware of wireless devices regularly as it will reduce the number of security loop holes in the device.
- 7.7. Disable remote management feature in routers to protect against unauthorized access.

### **8. Use of Social Media by Government Officers/Officials:**

All personnel including employees, contractual staff, consultants, partners, third party staff etc., who manage, operate or support information systems, facilities, communication networks; and information created, accessed, stored and processed by or on behalf of the Government of India, unless authorized to do so, shall not:

- a. Access social media on any official device (computer, mobile etc.).
- b. Disclose official information on social media or social networking portals or applications.

### **9. Avoiding Social Engineering Attacks**

Social Engineering is an approach to gain access to information through misrepresentation. It is the conscious manipulation of people to obtain information without realizing

## INFORMATION SECURITY BEST PRACTICES

that a security breach is occurring. It may take the form of impersonation via telephone or in person and through email. Following are some of the best practices should follow to avoid social engineering attacks:

- 8.1. Be careful to unsolicited phone calls, visits, or email messages from individuals asking about personal or other Government information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- 8.2. **Phishing** is one of common type of social engineering scam. The hacker typically sends an email or text to the target, seeking information that might help with a more significant crime. So do not reveal personal, sensitive or financial information in email or messages, and do not respond to such emails.

For example, a hacker might send emails that appear to come from a source trusted by the victim. That source might be a bank for instance, asking email recipients to click on a link to log in to their accounts. Those who click on the link, though, are taken to a fake website that, like the email, appears to be legitimate. If they log in at that fake site, they're essentially handing over their login credentials and giving the crook access to their bank accounts.

- 8.3. **Vishing** is the voice version of phishing. "V" stands for voice, but otherwise, the scam attempt is the same. The hacker uses the phone to trick a victim into handing over valuable information. So don't reveal any sensitive information over phone calls.

## INFORMATION SECURITY BEST PRACTICES

For example, a hacker might call an officer, posing as a Government officer. The hacker might prevail upon the victim to provide login credentials or other information that could be used to target the Organization.

- 8.4. **Quid pro quo** scam is another type of social engineering attack that involves an exchange like I give you this, and you give me that. Hackers make the victim believe as a fair exchange, but that's far from the case, as the cheat always comes out on top.

For example, a hacker may call a target, pretending to be an IT support technician. The victim might hand over the login credentials to their computer, thinking they're receiving technical support in return. Instead, the hacker can now take control of the victim's computer, loading it with malware or, perhaps, stealing personal information from the computer to commit identity theft.

- 8.5. Be cautious of 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). In general, all government websites have gov.in or nic.in at the end of their names. For example, a malicious website may have name as [www.npagov.in](http://www.npagov.in) or [www.npa-gov.in](http://www.npa-gov.in) against the actual name [www.npa.gov.in](http://www.npa.gov.in)
- 8.6. It's safer to type a URL into your browser instead of clicking on a link. Hovering over links in email will show the actual URL at the bottom, but a good fake can still steer you wrong.
- 8.7. Hacker wants you to act first and think later. If the message conveys a sense of urgency or uses high-pressure sales tactics be skeptical; never let the urgency influence your careful review.





- 8.8. If you receive an email from a foreign lottery or sweepstakes, money from an unknown relative, or requests to transfer funds from a foreign country for a share of the money it is guaranteed to be a scam and do not respond and delete such emails.
- 8.9. Immediately change any passwords you might have revealed to anyone. 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.

## **10. Glossary**

<b>Term</b>	<b>Definition</b>
DDoS	A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources.
DHCP	The Dynamic Host Configuration Protocol (DHCP) is a network management protocol used on UDP/IP networks whereby a DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network so they can communicate with other IP networks.
Digital Signature	A digital signature is a way to ensure that an electronic document (e-mail,

## INFORMATION SECURITY BEST PRACTICES

	<p>spreadsheet, text file, etc.) is authentic. Authentic means that you know who created the document and you know that it has not been altered in any way since that person created it.</p>
DNS	<p>The domain name system (DNS) is the way internet domain names are located and translated into internet protocol addresses.</p>
Encryption	<p>Encryption is the process of encoding a message or information in such a way that only authorized parties can access it.</p>
GPS	<p>The Global Positioning System (GPS) is a space-based satellite navigation system that provides location and time information.</p>
HTTPS	<p>Hypertext Transfer Protocol over Secure Socket Layer is a URL scheme used to indicate a secure HTTP connection.</p>
IM	<p>Instant Messaging a type of communications service that enables you to create a kind of private chat room with another individual in order to communicate in real time over the Internet.</p>

## INFORMATION SECURITY BEST PRACTICES

IoT	Internet of Things (IoT) is an ecosystem of connected objects that are accessible through the internet.
Malware	Malware is short for malicious software and used as a single term to refer to virus, spy ware, worm etc.
SMS	SMS is a text messaging service component of most telephone, internet, and mobile-device systems.
SNMP	Simple Network Management Protocol is used in network management systems to monitor network attached devices for conditions that warrant administrative attention.
SSH	Secure Shell is a network protocol that allows data to be exchanged using a secure channel between two computers.
SSID	Service Set Identifier is a name used to identify the particular 802.11 wireless LAN to which a client wants to attach.
Trojan	A Trojan horse is not a virus. It is a destructive program that looks as a genuine application. Unlike

## INFORMATION SECURITY BEST PRACTICES

	<p>viruses, Trojan horses do not replicate themselves but they can be just as destructive. Trojans open a backdoor entry to your computer which gives malicious users/programs access to your system, allowing confidential and personal information to be theft.</p>
URL	<p>A Uniform Resource Locator (URL), colloquially termed a web address is a reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it.</p>
USB	<p>A Universal Serial Bus (USB) is a common interface that enables communication between devices and a host controller such as a personal computer.</p>
Virus	<p>Virus is a program written to enter to your computer and damage/alter your files/data and replicate themselves.</p>
VPN	<p>A virtual private network extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.</p>
Wi-Fi	<p>Wi-Fi certified is a program for testing</p>

## INFORMATION SECURITY BEST PRACTICES



Certified	products to the 802.11 industry standards for interoperability, security, easy installation, and reliability.
Worms	Worms are malicious programs that make copies of themselves again and again on the local drive, network shares, etc.

### NOTE:

- In case of any doubt, *National Information Security Policy & Guidelines* (NISPG) issued by Ministry of Home Affairs may be referred to.
- Due care has been taken while preparing this booklet. If any suggestion for improvement(s) is felt, same may be shared at [cyberdost@mha.gov.in](mailto:cyberdost@mha.gov.in).

(version 1.0)

NIC-CERT/2023-08/EA-1  
Dated: 14-08-2023  
Threat Level : HIGH

**Emergency Security Alert: Security Precautions to be Undertaken for Safeguarding Govt Websites, Applications and ICT Infrastructure**

**A. Description:**

Due to the prevailing geo-political situations and increased threat perception in the cyberspace, all NIC Employees are advised to stay on high alert and ensure proper cyber security hygiene and best practices are followed both at their Client level (i.e., desktop, laptop...etc) and at the Application, Database, Server, Data Centre and Network level.


**B. Cyber Security Precautions to be Undertaken:**

The following Security Precautions should be adhered to by all NIC/Govt employees and other Third Party/ contractual manpower who are involved in the development, design, testing, implementation, audit, operations, management and troubleshooting of any Government Website or Application or Database or ICT Infrastructure/Services:

- Ensure that the Operating systems running on all Client machines and Servers are installed with/patched with the latest OS updates/patches.
- Ensure that all Open Source or Proprietary - Applications, Frameworks, Softwares, Packages, IDEs, Databases, Reporting/BI/Analytical Tools, Services, APIs, Components, Libraries, Plugins...etc., used on both the server and client machines and with the latest updates/patches.
- Ensure that NIC Provided Endpoint Security Agents are installed on all Client machines and Servers. Full System scan should be done at least once in a week and Quick/Flash scans should be done at least once in a day.
- Ensure that proper security hardening is carried out on all servers, client machines, webservers, databases..etc.
- Ensure that only the necessary ports and protocols are opened from the server for communication
- Ensure that logging is enabled in all servers, webservers, CMS, Databases, network devices, security devices, storage, VMs and any other ICT Infrastructure or Services, where logging is supported.
- If the Application/Website is behind a Load Balancer or WAF, then please ensure that X-Forwarded For (XFF) is enabled, so that the Original IP is captured in the web access logs.
- Remote desktop, Telnet, SSH and any other Administrative Access should be allowed only for VPN IPs.
- Do not use any remote administration tools like Anydesk, Ammy Admin, Team Viewer...etc.
- Critical Applications should be placed behind the Web Application Firewall (WAF)



- Ensure that NIC's DNS Server Settings (1.10.10.10/2409::1) is configured on all servers in NDCs and on all machines in NICNET
- Ensure that NIC's NTP Server settings (samay1.nic.in / samay2.nic.in) is configured on all servers and client machines present in NDCs and NICNET.
- Always download updates and patches from the Official website or Repositories of the OEM. Never download the updates/patches from any unauthorized third-party websites.
- Disable Powershell in Windows based servers and client machines
- Don't use the Root Account or Super Administrator Account in your servers/clients, for day to day activities
- On a daily basis check all files present under the Website root directory and Upload directory for any unauthorized file modifications and deletions.
- Ensure that the Websites, Applications and Databases are monitored round the clock for any unauthorised changes or modifications
- On a daily basis check the web access logs, Database logs, CRON Jobs, scheduled tasks, maintenance tasks, User activity logs for any unusual or suspicious activities
- Restrict the access of CMS/Site Administration Access to NIC's VPN based IPs only. These Admin URLs should not be accessible over the internet.
- Change all administrator credentials for servers, databases, Applications, Content Management Systems and other management components atleast once in 60 days.
- Ensure that all the sites and applications are using https (i.e., valid ssl certificate).
- Ensure that all API Calls are done through encrypted channel.
- Ensure that all credentials, API Keys, connection strings are encrypted
- Ensure that IP based Whitelisting is done for API communications, between Applications/Services
- Identify the target user base for your site or Application. If the target user base is within India, or restricted to certain countries, then please share the information with NDC Security Team , so that the access to your site or application can be geo-fenced and will be allowed only for the specific countries.
- Ensure that the root/super Administrator credentials of all Applications, Sites, Databases, Servers, Storage, ICT Infrastructure resides with the Government employee.
- Ensure that the team has implemented proper input sanitisation, query parameterization and error/exception handling, in all Applications and Websites
- Ensure that Application Source Code is not hosted in any external repositories (ex:github) outside Government Network
- Ensure that proper Source Code Composition Analysis (SCA) Audit is done at least once in every 3 months
- Don't install any pirated software or cracks on your Servers and Client machines.
- Always use a non-administrator account for carrying out day to day activities.
- Don't store or exchange any sensitive information or credentials through third party messaging Apps/Email and social media.
- Don't store any credentials or passwords on your phone or computer
- Don't Use the same credentials on multiple websites/applications/servers/client machines
- Don't install any browser plugins or toolbars on the machine which is used for accessing the NDC
- Adhere to all Advisories published by NIC-CERT/Cyber Security Group/Audit Group.

- 
- Take prompt action on any security issues pointed out by NIC-CERT/Cyber Security Group/Audit Group.
  - Observe Caution while opening any attachments or links sent over Email, attackers could try to compromise the Developers/Administrators to initiate a Supply Chain Attack. Report suspicious Emails to [incident@nic.in](mailto:incident@nic.in)
  - Temporarily shutdown all staging servers and ensure that staging environment is not hosting any production data
  - Change/disable, all credentials, connection strings, keys, secrets...etc., used in staging environment. Ensure that they are not used in the production environment.
  - Staging environment should not be directly exposed to the internet. Restrict access to the staging environment only for the users who are involved in the testing/development.
  - In case of any security incident kindly report it to NIC-CERT at: [incident@niccert.nic.in](mailto:incident@niccert.nic.in)

Everyone is requested to ensure strict adherence to the above mentioned guidelines.

---