Cybersecurity Appropriate Behaviour for Government Employees of Assam

Document Version V1

Information Technology
DepartmentGovernment of Assam

Contents

A. INTRODUCTION

Cybersecurity appropriate behaviour is of utmost importance for Government employees because they handle sensitive information that, if accessed by unauthorized parties, can pose significant threats to national security. Government employees are entrusted with critical information, such as classified data, personal information of citizens, and other confidential records that require stringent security measures. A cybersecurity appropriate behaviour list is required for Government employees to ensure that they follow best practices to protect sensitive information from cyber threats. The list provides guidelines, protocols, and compliance requirements to follow, reduces the risk of insider threats, and promotes a culture of security within Government agencies.

In the View of the above, we have prepared a guideline in the form of "Do's and Don'ts" for appropriate cyber behaviour of Government employees of Assam to develop cyber safe resilience ecosystem in the Government of Assam.

In order to sensitize the Government employees and contractual/outsourced resources and build awareness amongst them on what to do and what not to do from a cyber security perspective, these guidelines have been compiled.

B. COMMON CYBER SECURITY: DO'S AND DON'TS

Do's:

1. Use complex passwords with a minimum length of 8 characters, using a combination of capital letters, small letters, numbers and special characters.
2. Change your passwords at least once in 3 months
3. Use multi-factor authentication, wherever available.
4. Save your important data and files on the secondary drive in the system
5. Maintain an offline backup of your critical data.
6. Keep your Operating System and BIOS firmware updated with the latest updates/patches.
7. Install enterprise antivirus client offered by the Government on your official desktops/laptops. Ensure that the antivirus client is updated with the latest virus definitions, signatures and patches.
8. Configure DNS Server IP and NTP Service as recommended by System Administrator / NIC.
9. Use authorized and licensed software only.
10. Ensure that proper security hardening is done on the systems.
11. When you leave your desk temporarily, always lock/log-off from your computer session.
12. When you leave office, ensure that your computer and printers are properly shutdown.
13. Keep your printer's software updated with the latest updates/patches.
14. Setup unique passcodes for shared printers.
15. Use Virtual Private Network (VPN) for connecting remotely to any IT assets located in the Data Centres / office resources from home / public network.
16. Keep the GPS, bluetooth, NFC and other sensors disabled on your computers and mobile phones. They maybe enabled only when required.

17. Download Mobile Apps from official app stores of apps providers.
18. Use a Standard User (non-administrator) account for accessing your computer/laptops for regular work.
19. While sending any important information or document over electronic medium, kindly encrypt the data before transmission. You can use a licensed encryption software or an Open PGP based encryption or add the files to a compressed zip and protect the zip with a password.
20. Observe caution while opening any shortened uniform resource locator (URLs) (ex: tinyurl.com/ab534/). Many malwares and phishing sites abuse URL shortener services.
21. Observe caution while opening any links shared through SMS or social media, etc., where the links are preceded by exciting offers/discounts, etc., or may claim to provide details about any current affairs. Such links may lead to a phishing/malware webpage, which could compromise your device.
22. Report suspicious emails or any security incident to incident@cert-in.org.in, itdepartment-as@assam.gov.in

Don'ts:

1. Don't install or use any pirated software (ex: cracks, keygen, etc.).
2. Don't open any links or attachments contained in the emails sent by any unknown sender.
3. Don't use any 3rd party toolbars (ex: download manager, weather tool bar etc.) in your internet browser.
4. Don't use the same password in multiple services/websites/apps.
5. Don't save your passwords in the browser or in any unprotected documents.
6. Don't write down any passwords, passphrase, Private key, IP addresses, network diagrams or other sensitive information on any unsecured material. (ex: sticky/post-it notes, plain paper pinned or posted on your table, etc.)
7. Avoid to save your data and files on the system drive (Ex: c:\ or root), instead save to another partitioned drive. (Ex: D:\)
8. Don't upload or save any internal/restricted/confidential Government data or files on any non-Government cloud service (ex: google drive, dropbox, etc.).
9. Don't use obsolete or unsupported Operating Systems.
10. Don't use any 3rd party DNS Service or NTP Service.
11. Don't use any 3rd party anonymization services (ex: Nord VPN, Express VPN, Tor, Proxies, etc.).
12. Don't share system passwords or printer passcode or Wi-Fi passwords with any unauthorized persons.
13. Don't allow internet access to the printer.
14. Don't allow printer to store it's print history.
15. Don't use official / Government mail ID in Social media unless it is authorised to do so.
16. Don't plug-in any unauthorized external devices, including USB drives shared by any unknown person

17. Don’t use any unauthorized remote administration tools (ex: Teamviewer, anydesk, etc.)
18. Don’t use any unauthorized 3rd party video conferencing or collaboration tools for conducting sensitive internal meetings and discussions.
19. Don’t use any external email services for official communication.
20. Don’t use administrator account or any other account with administrative privilege for your regular work.
21. Don’t use any external mobile App based scanner services (ex: Camscanner) for scanning internal Government documents.
22. Don’t use any external websites or cloud-based services for converting/compressing a Government document (ex: word to pdf or file size compression)
23.

C. INTERNET PRIVACY: DOS AND DON'TS

As a Government employee, it's important to protect your online privacy while also ensuring that you comply with applicable laws and regulations. Here are some dos and don'ts for internet privacy:

Do’s:

1. Use strong and unique passwords for all online accounts and change them regularly.
2. Use two-factor authentication for additional security on your online accounts.
3. Regularly update your operating system, web browsers, and apps to patch security vulnerabilities.
4. Be cautious of phishing scams and only click on links from trusted sources.
5. Read the privacy policies of websites and apps before using them.
6. Use ad-blockers and cookie managers to limit the amount of tracking that occurs.
7. Consider using a password manager to securely store your passwords.
8. Keep your personal and work-related online activities separate to avoid potential conflicts of interest.
9. Use a virtual private network (VPN) when accessing public Wi-Fi networks or when working remotely to protect your online activities from prying eyes.
10. Keep your software and operating systems up-to-date to protect against security vulnerabilities.

Don'ts:

1. Don't use public Wi-Fi networks to access sensitive information or conduct work-related activities unless you are using a VPN.
2. Avoid using public computers and public Wi-Fi connections to access and carryout any Government financial or sensitive transaction. Accessing Government email on such computers has a high risk of causing information breach.
3. Don't overshare personal information related to your work in the organisation on social media or other websites.
4. Don't use the same password for multiple accounts.
5. Don't open email attachments or click on links from unknown senders.

6. Don't install software or apps from untrusted sources.
7. Don't use default passwords for your devices or accounts.
8. Don't give out your personal information over the phone or email unless you initiated the contact.
9. Don't ignore privacy settings on social media and other online services.
10. Don't save passwords or personal information in your web browser.
11. Don't assume that your online activity is completely private.
12. Don't share sensitive or confidential information online, even with colleagues or other Government employees.
13. Don't store sensitive or confidential information of Government on personal devices or accounts.
14. Don't use personal email accounts for work-related activities or vice versa.
15. Don't engage in online activities that could compromise your professional reputation or be seen as representing your organisation / agency in a negative light.
16. Don't use social media during work hours for personal use or in a way that interferes with your job duties.
17. Don't disclose any sensitive details of your organisation on social media or 3rd party messaging apps
18. Don't use social media to engage in political discussions or express personal opinions that may be seen as representing your organisation/agency.

D. DIGITAL SIGNATURE: DO'S AND DON'TS

The dos and don'ts for the use of digital signatures by government employees are required to ensure the security, integrity, and authenticity of electronic documents. Digital signatures are a form of electronic signature that provides legal and official recognition to electronic documents, and as such, it is critical that they are used correctly.

Do's:

1. Use digital signatures only for authorized and legal purposes as per your official duties.
2. Ensure that your digital signature certificate (DSC) is obtained from a trusted certifying authority.
3. Keep your DSC password confidential and do not share it with anyone.
4. Verify the authenticity and integrity of the documents before signing them using your digital signature.
5. Follow the guidelines and policies related to the use of digital signatures issued by your organization or the government.
6. Regularly update your DSC and ensure that it is valid and not expired.
7. Keep your DSC safe and secure and avoid unauthorized access to it.
8. Properly log out of the system after using your digital signature for signing documents.
9. Use strong passwords for accessing the system and changing the DSC password.
10. Keep a record of all the documents signed using your digital signature for future reference.

Don'ts:

1. Don't use someone else's DSC or sign on behalf of others without proper authorization.
2. Don't use digital signatures for personal or unofficial purposes.
3. Don't share your DSC with anyone or store it on a shared system or device.
4. Don't use an expired or invalid DSC for signing documents.
5. Don't sign documents without verifying their authenticity and content.
6. Don't sign documents without proper authorization or approval from higher authorities.
7. Don't use weak or easily guessable passwords for accessing the system or changing the DSC password.
8. Don't leave the system unattended while using your digital signature for signing documents.
9. Don't modify or alter the signed documents after signing them using your digital signature.
10. Don't ignore the policies and guidelines related to the use of digital signatures issued by your organization or the Government.

E. USE OF Wi-Fi: DO'S AND DON'TS

Use of Wi-Fi / setting up Wi-Fi in an office environment for a Government organization:

Do's:

1. Use Wi-Fi for official purposes only: Employees should only use Wi-Fi for official purposes and not for personal use. This will help to prevent security breaches and ensure that the network is not overwhelmed by non-work related traffic.
2. Disconnect from Wi-Fi when not in use: Employees should disconnect from Wi-Fi when they are not using it. This will help to conserve bandwidth and ensure that the network is available for other users.
3. Use strong encryption: Implement strong encryption, such as WPA2, to secure your Wi-Fi network. This will ensure that only authorized personnel can access the network and sensitive information remains protected.
4. Set up a guest network: Create a separate Wi-Fi network for guests and visitors. This will ensure that guests do not have access to sensitive information or network resources and minimize the risk of a security breach.
5. Use strong passwords: Use strong passwords for your Wi-Fi network and ensure that passwords are changed regularly. This will prevent unauthorized access and ensure that only authorized personnel can access the network.
6. Implement access controls: Implement access controls, such as MAC address filtering, to restrict access to your Wi-Fi network. This will ensure that only authorized devices can connect to the network.
7. Use VLANs: Implement VLANs to segregate network traffic and ensure that sensitive information is kept separate from other network traffic. This will help to prevent unauthorized access to sensitive information.
8. Report security incidents: Employees should report any security incidents or suspicious activity to their IT Support / Security incident team. This will help to prevent security breaches and protect sensitive information.

Don'ts:

1. Use default passwords: Do not use default passwords for your Wi-Fi network. Default passwords are easily accessible and can be used to gain unauthorized access to your network.
2. Use weak encryption: Do not use weak encryption protocols, such as WEP, as they can be easily cracked by attackers. This will leave your network and sensitive information vulnerable to attack.
3. Allow unrestricted access: Do not allow unrestricted access to your Wi-Fi network. This will make it easier for attackers to gain access to your network and sensitive information.
4. Share passwords: Do not share Wi-Fi passwords with unauthorized personnel. This will increase the risk of a security breach and make it harder to track who has access to the network.
5. Ignore updates: Do not ignore software and firmware updates for your Wi-Fi network. Updates often include security patches that address vulnerabilities and keep your network secure.
6. Install unauthorized devices: Employees should not install unauthorized devices on the Wi-Fi network. This can introduce security vulnerabilities and increase the risk of a security breach.

F. RANSOMWARE ATTACKS: DO'S AND DON'TS

The popularity and ease of use of Windows OS / Applications, along with its legacy code and the prevalence of third-party software, make it a more attractive target for hackers. It's important for Windows users to take steps to protect themselves against ransomware attacks, such as keeping their systems up to date, using antivirus software, and being cautious with email and attachments.

Do's

Windows OS configuration steps that can help you avoid ransomware attacks:

1. Enable Windows Defender Antivirus: Windows Defender Antivirus is built into Windows 10 and provides basic protection against malware, including ransomware. To enable Windows Defender Antivirus, go to Settings > Update & Security > Windows Security and turn on Real-time protection.
2. Enable Controlled Folder Access: Controlled Folder Access is a feature in Windows 10 that prevents unauthorized access to important files and folders. To enable Controlled Folder Access, go to Settings > Update & Security > Windows Security > Virus & threat protection > Manage ransomware protection and turn on Controlled folder access.
3. Keep Windows 10 up to date: Windows 10 updates often include security updates that can protect against ransomware attacks. To keep Windows 10 up to date, go to Settings > Update & Security > Windows Update and click Check for updates.

4. Use strong passwords: Use strong passwords for your user account and other accounts you use on your Windows 10 computer. A strong password should be at least eight characters long and include a combination of uppercase and lowercase letters, numbers, and symbols.
5. Disable Remote Desktop Protocol (RDP): Ransomware attacks often use RDP to gain access to computers. If you don't need RDP, it's best to disable it. To disable RDP, go to Settings > System > Remote Desktop and turn off Enable Remote Desktop.
6. Enable Windows Firewall: Windows Firewall can help prevent unauthorized access to your computer. To enable Windows Firewall, go to Settings > Update & Security > Windows Security > Firewall & network protection and turn on Windows Defender Firewall.
7. Use an updated antivirus program: Use an antivirus program that can detect and remove ransomware. Make sure the antivirus program is up to date and set to scan your computer regularly.
8. Backup your data regularly: Regularly back up your important files and data to an external hard drive or cloud storage service. If you're hit by a ransomware attack, having a backup can help you recover your data without paying the ransom.

Don’ts

Configurations on Windows 10 that you should avoid to minimize the risk of a ransomware attack:

1. Don't use outdated software: Using outdated software can make your system vulnerable to ransomware attacks, as hackers can exploit known security vulnerabilities to gain access to your system. Keep your software up to date to ensure that you have the latest security patches.
2. Don't disable User Account Control (UAC): User Account Control is a security feature in Windows 10 that helps prevent unauthorized changes to your system. It's important to keep UAC enabled to prevent ransomware from making changes to your system without your knowledge.
3. Don't allow remote access to your system: Remote access tools like Remote Desktop Protocol (RDP) can be used by hackers to gain access to your system and install ransomware. If you don't need to use remote access, disable it to minimize the attack surface of your system.
4. Don't disable Windows Firewall: Windows Firewall is a built-in feature in Windows 10 that helps prevent unauthorized access to your system. Disabling the firewall can leave your system vulnerable to ransomware attacks and other security threats.
5. Don't open suspicious email attachments: Email attachments can be a common way for ransomware to spread. Don't open attachments from unknown or suspicious senders, and be cautious with attachments from even known senders if they are unexpected or seem out of character.
6. Don't disable automatic updates: Windows 10 has automatic updates that provide security patches and updates for your system. Don't disable these updates, as they can help protect your system from ransomware and other security threats.
7. Don't give administrative privileges to unauthorized users: Administrative privileges give users access to sensitive system settings and files. Don't give administrative

privileges to unauthorized users, and limit administrative access only to those who need it.

G. USE OF ANTIVIRUS: DO'S AND DON'TS

Do's:

1. Install enterprise antivirus client offered by the Government on your official desktops/laptops.
2. Ensure that the antivirus client is updated with the latest virus definitions, signatures and patches.
3. Enable Windows Defender Antivirus: Windows Defender Antivirus is built into Windows and provides basic protection against malware, including ransomware.
4. Make sure the antivirus program is up to date and set to scan your computer regularly.

Don'ts:

1. Never Disable Antivirus or firewall off while using internet.
2. Don't stop Windows startup for windows defender services.
3. Never turnoff automatic update or scan for the system.

H. USE OF OFFICE COMPUTERS: IT SECURITY TIPS

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

1. All classified work should strictly be carried out only in a standalone computer which is not connected to internet.
2. Don't leave the computer unattended.
3. Always lock the computer before leaving workplace to prevent unauthorized access. The computer can be locked by pressing 'ctrl + alt + del' and choosing 'lock this computer' or 'window button+ L'.
4. Enable password-protected screen saver with a timeout period of 5 minutes to ensure that computers that were left unsecured can be protected.
5. Be careful of what is plugged into the computer. Malware can spread through infected USB drives, external hard drives, and even smart phones.
6. Use non-administrator account privileges for login to the computer and avoid accessing the computer with administrator privileges for day-to-day usage.
7. Treat sensitive data very carefully and use encryption to securely encode sensitive information.
8. Backup important files at regular intervals to avoid unexpected loss.
9. Remove unnecessary programs or services from computer which are not required for day to day operation.
10. Do not give remote access, file and print sharing option to other computers. Remote access or screen sharing options shall be disabled.
11. Do not use file sharing software such as torrents etc. as file sharing opens computer to the risks of malicious files and attacks.
12. Avoid entering sensitive information onto a public computer like cyber cafe, library computers etc.

13. After storing or downloading any personal information on computers in cyber café or library computers, make sure to delete all the documents permanently before leaving the computer. By pressing Shift and Delete button together may delete documents. This makes it difficult to recover deleted files.
14. Remove files or data that is no longer needed to prevent unauthorized access to such data. Merely deleting sensitive material is not sufficient, as it does not actually remove the data from system. File shredder software should be used to delete sensitive files on computers.

I. INTERNET BROWSING: IT SECURITY TIPS

Following precautions are to be taken while browsing on Internet:

1. Always be careful when clicking on links or downloading. If it is unexpected or suspicious for any reason, don't click on it.
2. 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 browser address bar to verify that a site is secure.
3. Always use updated web browser for browsing internet. Running an outdated web browser may contain security vulnerabilities and risk of computer getting compromised increases.
4. The "Save password" option prompted by the browser should not be selected if a pop-up window appears after entering information on the login screen. Don't save account information, such as passwords or credit card information in web browsers.
5. Use web browser which has been permitted by Organization.
6. Remember that things on the internet are rarely free. "Free" Screensavers etc., often contain malware. So please be aware of such online free offers.
7. Make a habit of clearing history from the browser after each session. Following are the settings in various browsers to automatically clear the history at the end of browser session:

J. PASSWORD MANAGEMENT: IT SECURITY TIPS

Unauthorized access is a major problem for anyone who uses a computer or device such as smartphone or tablet or computer. The consequences for victims of these unauthorized 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 commonly used passwords enable intruders to easily gain access and control a device. Following practices may be considered while setting up and managing a password,

1. Create strong password with a minimum length of ideally 10 characters and comprising of combination of alphabets (both lower case and upper case), numbers and special characters.
2. All passwords (e.g., email, computer, etc. passwords) should be changed periodically at least once every three months. Don't reuse old passwords.
3. Passwords should not be stored in readable form in computers, notebook, and notice board or in any other location where unauthorized persons might discover or use them.
4. Treat passwords as sensitive information and do not share them with anyone.

5. Always use different passwords for every log-in account. Using same password for more than one account risks multiple exposures if one of the passwords is hacked.
6. If it is necessary to communicate passwords, such as password for a password protected file which are sent as an attachment through email. Such passwords should be communicated through a different channel such as phone call or SMS.
7. Always decline the use of the "Remember Password" feature wherever it is prompted by the applications.
8. 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 contains without special characters
    - 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, aaaaaa, qwert1234, asdfg, zxcvb, etc.

K. REMOVABLE STORAGE MEDIA: IT SECURITY TIPS

One of today's biggest security concern is the use of removable storage devices (USB devices such as pen drives, CD, DVD, Blu-ray discs, Media cards etc.,) in 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 defences, 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 practices may be considered while dealing with Removable storage media:

1. Auto run/ Auto play feature must be disabled for all removable media.
2. The classified data should be encrypted before copying into the removable storage media designated to store classified information.
3. Classified information should be stored only on organization allocated removable storage media for work purpose.
4. The computers should be enabled with "Show hidden file and folders" option to view hidden malicious filesin any folder / USB storage devices.
5. Removable media like USB's, CDs etc., must not be left unattended, if they contain official information.
6. Technical controls may be implemented to restrict use of portable storage media drives outside of the Government network.
7. Removable media should not be taken out of office unless permitted by the competent authority.
8. In order to minimize physical risk, loss, theft or data corruption, all storage media must be stored in an appropriately secure and safe environment.

9. In case of damage or malfunction of device, the same should be returned to the designated authority in office for repair/replacement. Never ever handover such devices to outsiders or other vendors for repair as it might have classified information.
10. If the USB device is no longer a functional requirement after issuance, then the same should be returned to the issuing authority.
11. The contents of removable media must be removed/ erased after the official purpose has been served.

L. EMAIL COMMUNICATION: IT SECURITY TIPS

Following practices may be considered in regards to email communication:

1. Use only Government provided email address for official communications (e.g. NIC email).
2. Designation based email address with "nic.in" or "gov.in" domain shall be used for official purposes instead of personal name based email in order to avoid official communications getting stored in personal email. This will also enhance security of official information.
3. While relieving from the post, the official email account shall be handed over to the successor or surrendered.
4. System administrator may deploy appropriate controls to restrict use of personal email address for any official communications.
5. Avoid downloading email attachments or clicking on suspicious links received in emails from unknown or untrusted sources.
6. Classified information shall not be communicated via emails. In case of emergent requirements to do so, the approval of competent authority should be obtained.
7. Avoid accessing official email accounts from public Wi- Fi connections.
8. Auto save of password for email accounts should not be enabled.
9. Logout from mail accounts after work is done.
10. User should type the complete URL in the browser instead of clicking links received in an email.
11. Do not open / forward / reply to any suspicious e-mails.
12. Be cautious on tiny or shortened URL's (appears like http://tiny.cc/ba1j5yyyy etc.) and don't click on it as it may take to a malware infected website.
13. Do not open attachment having extension such as .EXE, .DLL, .VBS, .SHS, .PIF, .SCR. Typical example, xxxxx.txt.exe, xxxxx.doc.exe etc.

M. GLOSSARY TERMS:

Term	Definition
DigitalSignature	A digital signature is a way to ensure that anelectronicdocument(e-mail,spreadsheet,text file, etc.) is authentic. Authentic meansthatthecreatorofthedocumentisknownandit has not been altered in any way since thatpersoncreatedit.
DNS	The domain name system (DNS) is the wayinternetdomainnamesarelocatedandtranslatedintointernetprotocola

	ddresses.
NTP	NTP stands for Network Time Protocol. It is a protocol used to synchronize the clocks of computers and other devices on a network to a common time reference.
GPS	GPS stands for Global Positioning System, which is a satellite-based navigation system used to determine the precise location and time of a receiver anywhere in the world
NFC	NFC stands for Near Field Communication, which is a wireless communication technology used for short-range communication between two electronic devices.
Encryption	Encryptionistheprocessofencodingamessage or information in such a way thatonlyauthorized parties canaccessit.
DSC	DSC can also refer to Digital Signature Certificate. It is a digital certificate issued by a Certifying Authority (CA) that verifies the identity of the person holding the certificate.
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer is a URL scheme used to indicate a secure HTTP connection.
WPA2	WPA2 (Wi-Fi Protected Access 2) is a security protocol that is used to protect wireless networks from unauthorized access.
WEP	WEP (Wired Equivalent Privacy) is an older security protocol that was used to protect wireless networks.
UAC	User Account Control (UAC) is a security feature in Windows operating systems that aims to improve the security of the system by limiting the privileges of applications that run with administrator permissions.
RDP	Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft that allows users to remotely access and control a computer over a network connection.
Malware	Malware is short for malicious software and used as a single term to refer to virus, spy ware, worm etc.
Ransomware	Ransomware is a type of malware that encrypts the victim's files and demands a ransom payment in exchange for the decryption key needed to restore access to the files.
SMS	SMS is a text messaging service component of most telephone, internet, and mobile- device systems.
URL	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.
USB	A Universal Serial Bus (USB) is a common interface that enables communication between devices and a host controller such as a personal computer.
Virus	Virus is a program written to enter to the computer and damage/alter files/data and replicate themselves.
VPN	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.

N. CYBER SECURITY RESOURCES

The following resources may be referred for more details regarding the cyber security related notifications/information published by Government of India:

Sl.No.	Resource URL	Description
1	https://it.assam.gov.in/sites/default/files/swf_utility_folder/departments/it_dept_webcomindia_org_oid_2/menu/document/assam_cyber_security_policy_2020_0.pdf	Assam Cyber Security Policy
2	https://it.assam.gov.in/sites/default/files/swf_utility_folder/departments/it_dept_webcomindia_org_oid_2/menu/document/cyber_crisis_management_plan_v2.pdf	Cyber Crisis Management Plan
3	https://it.assam.gov.in/sites/default/files/swf_utility_folder/departments/it_dept_webcomindia_org_oid_2/menu/document/isms.sop_.pdf	ISMS (ISO 27001) Information Security Management System of Assam
7	https://www.meity.gov.in/cyber-security-division	Laws, Policies & Guidelines
	https://www.cert-in.org.in	Security Advisories, Guidelines & Alerts
	https://nic-cert.nic.in	Security Advisories, Guidelines & Alerts
	https://www.csk.gov.in	Security Tools & Best Practices
	https://infosecawareness.in/	Security Awareness Materials
	http://cybercrime.gov.in	Report Cyber Crime, Cyber Safety Tips