Naripokkho

Information and Data Protection Guideline

Naripokkho has been working since 1983 with the aim to establish women as entitled citizens and dignified human beings in family, society and state. At present, the organization is increasingly dependent on information technology for data storage and this dependency is growing day by day. With that, the importance of data security is increasing. While the use of technology has made the organizational operations easier, all modern devices can also cause serious damage as a result of hacking or cyber-attacks. The safe use of all types of information and technology based devices, protection of data from theft, staying safe from various types of malware are called cyber security. Cyber security applies to both software and hardware. Cyber security is the process of protecting and recovering networks, devices and programs from cyber-attacks. Therefore, data protection policy is necessary to keep Naripokkho's data safe and secure. This policy will play a role in keeping the organization's data secure and using social media with safe precautions.

The policy will be finalized after discussing with the members of the executive committee and taking their approval. Even after the data protection policy is approved at the executive meeting of Naripokkho, if any revision is needed in the future, only the executive committee of Naripokkho has the power to do so.

Organizations should take the following precautions to keep the data safe and secure:

What an individual/employee should do –

1. Many times office works are done at computer/laptop/mobiles that used by home/family members/friends. In that case, before using the device, make sure that, it is updated and protected (virus free). After completing the work, the file should be backed up and or deleted.

2. Laptops should not be left switched on/open unnecessarily after work, especially during travel (bus, train and car) and at home should be closed following proper rules/steps so that no one else can access the data.

3. Screens must be locked when employees are away from the desk. Screen lock will prevent anyone else from accessing the computer.

4. Any device used (cybercafe, personal, office, home/family members/ friends used) must logout the account after finishing work.

গীতা দাস
সভানেত্রী, নারীপক্ষ

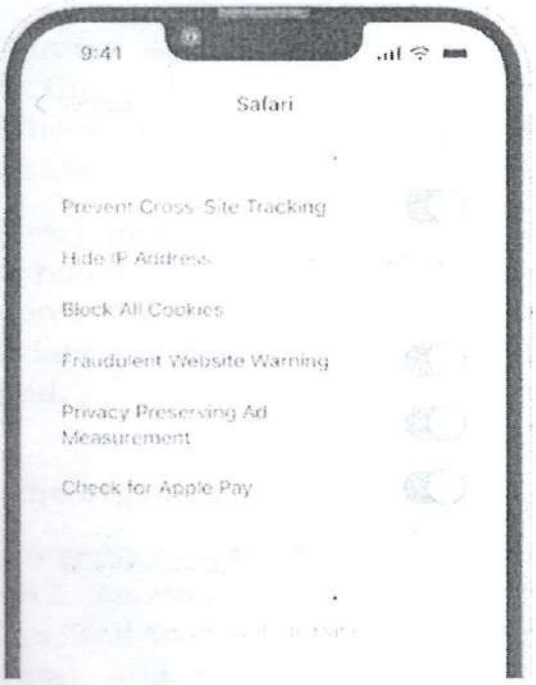
5. Regular file system checking, disk cleanup, disk defragment should be done. How to do it - Go to Start option and click > Run > type compmgmt.msc> click ok > Disk Management > Click Right Button on New Volume (C, D, E, F) > Properties > Disk Cleanup. Or right click on My Computer and select Manage to do disk cleanup.

6) Browsing History, Cache memory should always be kept clean. For this, on your computer, click on Chrome > click on the upper right ⋮ > click on more tools > click on clear browsing> select the side boxes for the information you want to clear in Chrome> click on clean data and complete the work.

7) Secure USB must be used. Nowadays laptops and desktops have USB facility and the risk of cyber-attack through USB is increasing. So avoid charging your phone with the help of USB port on other computer or installing USB. You should refrain from charging someone else's device or using your personal computer for data transfer unless it is necessary.

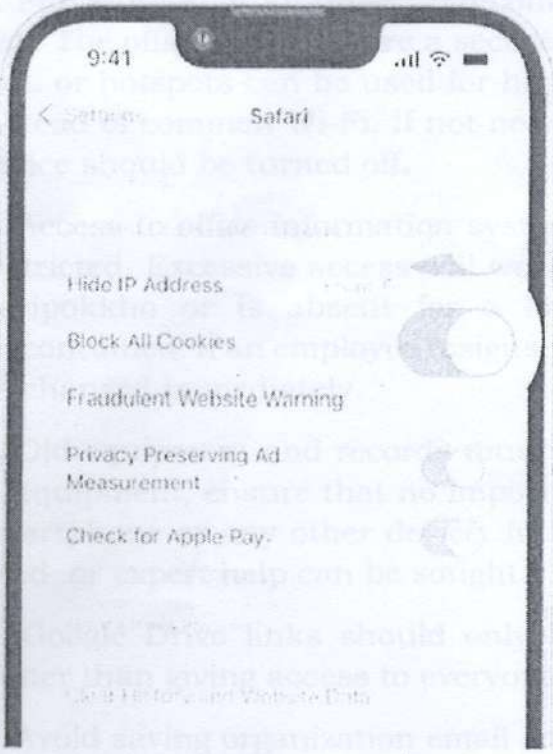
8) For Mac/ Iphone users-

• Delete History, Cache and Cookies – To clear your History and Cookies, tap Settings > Safari > History Ges Website Data clear button. Clearing your History, Cookies and Website Data from Safari will not change your password or any other information. Safari works fast through this.



• Cookies are a part of a website that remembers information about your device and helps you access the same website later. If you do not want to store your information on the website, you can block cookies. Settings > Safari > Block all Cookies. Block all cookies may prevent some web pages from working.

গীতা দাস
সভানেত্রী, নারীপক্ষ



• It is very important to charge with a specific mobile charger and keep the charging port clean. Before charging the mobile, make sure that the charging port is clean. If there is anything stuck or stuck in the charging port, clean it.

• All unused Apps in the mobile must be deleted. iPhone stores settings include Offload Unused Apps. This app will automatically delete the unused app if the mobile storage is low and save the necessary documents and data. If you want, you can always download it from the app store.

• It is very important to update mobile IOS and apps regularly. When the update notification comes on the mobile, the mobile will automatically update if you press the update button. The update option cannot be turned off until the update is complete. After the update is completed, the mobile must be restarted.

What the organization should do

1. The organization's data and storage devices must be protected by a strong password. Set strongpasswords to all computers, laptops, email, social media websites, and Wi-Fi. Apply combined numbers, letters (both uppercase and lowercase), and symbols to create complex passwords. Ensure that the account recovery system and authentication system must also be switched on.

2. All data must be saved from portable devices regularly through a backup system. Data files must be protected with a separate password, and each file has to be stored in a separate safe place (email hard drive, Google Drive, pen drive, cloud, etc.).

গীতা দাস
সভানেত্রী, নারী [illegible]

3. Public Wi-Fi or an unsecured connection can put data and information at risk. The office must ensure a secure Wi-Fi connection for work. Also, mobile data or hotspots can be used for highly confidential meetings or information instead of common Wi-Fi. If not necessary, the Bluetooth and hotspot of the device should be turned off.

4. Access to office information systems and IT systems should be limited or restricted. Excessive access will weaken the systems. If any employee leaves Naripokkho or is absent for a long period, employee access must be discontinued. If an employee resigns, the password of the project email should be changed immediately.

5. Old equipment and records must be disposed of safely. Before selling the IT equipment, ensure that no important data is left on the computer, laptop, smartphone or any other device. In this case, data deletion software can be used, or expert help can be sought.

6. Google Drive links should only be shared with responsible individuals rather than giving access to everyone.

7. Avoid saving organization email and social media passwords on devices.

8. The organization must specify the number of administrators for Naripokkho's social media websites. Additionally, the responsibilities of these administrators should be documented.

9. Before discussing or sharing information about the organization with any person outside Naripokkho in conversations and social media (organizational and personal) should be discussed with the relevant responsible persons.

10. Important information of the organization should be stored as a soft copy in a medium or cloud that complies with security laws and regulations.

11. Local Area Network (LAN) is a computer network that interconnects multiple computers in alimited area at home, school, computer library, or office. LAN is much faster. In the case of LANsecurity, remote access to digital devices should be protected.

12. A Security Socket Layer (SSL) must be used for the web application. SSL is required to establish communication between two devices. Internet is used for networking, and the device is connected by password to the socket to establish the connection.

13. For the staff and members of the organization, there should be a training session about "Guidelines for data protection of Naripokkho". Detailed guidelines should be prepared for new employees or members in this regard.

14. If an employee has valuable information and data about the organization, they have to sign a non-disclosure agreement. When an employee works on projects involving sensitive information, a non-disclosure agreement should be signed between the employee and Naripokkho. For example, if Naripokkho

গীতা দাস
সভানেত্রী, নারীপক্ষ

plans politically sensitive advocacy and outsiders know this information, it can be a threat to Naripokkho and the members of the team. This agreement's objective is to ensure extra security.

Applies to both:

1. Use Multiple layers of security- Password, Code, two factor authentication).

2. Backup files must be saved in a drive other than C drive, download and system C.

3. Avoid clicking or sharing suspicious emails and links. (e.g. requests to work on an urgent basis, requests for money or if someone blackmailed by sending a text that he/ she saw private photos, avoid clicking or sharing such emails or links).

4. Anti-virus and malware protection must be installed and kept up to date. Along with that,electronic devices must be regularly cleaned and updated.

5. Avoid storing unnecessary information on devices (computers, laptops). This initiative will help protect information and data.

6. Avoid downloading free software without being sure about security. Use reliable and secure websites to provide information. If the website has https:/ then the website can be considered as trusted or safe.

7. If you need to enter the password on any website, you must check the link so the password cannot be stolen/copied or phishing. At times, pages like Facebook may come, but the link is not for Facebook. There is a possibility of hacking if you enter the password there. So check the link carefully before using Facebook or a website or software.

8. Must have a clear understanding of cyber laws for reporting processes against cyber harassment/crimes.

গীতা দাস
সভানেত্রী, নারীপক্ষ