Guidelines
for
Schools on Cyber Safety and Security

विद्ययाऽमृतमश्नुते

एन सी ई आर टी
NCERT

Be safe in cyber world ...

Index

Identify threats vulnerability and assess risk exposure

Slow and sluggish behavior of the system.

Inexplicable disappearance of system screen while working.

Unexpected popups or unusual error messages.

Drainage of system battery life before expected period.

Appearance of the infamous BSOD (Blue Screen of Death).

Crashing of programs/ system.

Inability to download updates.

Avigation to new browser homepage, new toolbars and/or unwanted websites without any input.

Circulation of strange messages from your email id to your friends.

Appearance of new , unfamiliar icons on Desktop.

Appearance of unusual message or programs which start automatically.

Unfamiliar programs running in Task Manager.

Develop protection & detection measures

2

Invest in a robust firewall.

Have students and teachers create strong passwords.

Have a password protocol that specifies strong password guidelines, frequent change of passwords, and prevents reuse of old passwords.

Use only verified open source or licensed software and operating systems.

Ensure that computer systems and labs are accessed only by authorized personnel.

Discourage use of personal devices on the network, such as personal USBs or hard drives.

Set up your computer for automatic software and operating system updates

Check that antivirus softwares in each system are regularly updated.

Consider blocking of file extensions such as .bat, .cmd, .exe, .pif by using content filtering software.

2

Read the freeware and shareware license agreement to check if adware and spyware are mentioned, before installing them on systems.
Use encryption such as SSL or VPN for remote access to office or school lab through internet.

Ensure that third-party vendors (who have contract with the school) have strong securitymeasures in place.

Consider contracting with a trusted / verified third-party vendor vendor to monitor the security of your school's network.

Institute two- or multi factor authentication for students, teachers and administrators when they log on. Usually a login requires a username and password, but experts suggest also uploading a photo or getting a code texted to your phone to verify that the user is valid.

Protect your Wi-Fi Connection with secure password, WEP encryption, etc.

Encrypt the network traffic.

Change the administrator's password from the default password. If the wireless network does not have a default password, create one and use it to protect the network. Disable file sharing on computers .

Turn off the network during extended periods of non-use etc.

Use "restricted mode", "safesearch", "supervised users" and other similar filters and monitoring systems, so that no child can access harmful content via the school's IT systems, and concerns can be spotted quickly

3

Protect sensitive data

Design and implement information security and access control programmes and policies, by evaluating the storage (used/ unused), access, security and safety of sensitive information.

Never store critical information in system's C drive.

Backup critical data (mobile numbers, aadhaar number etc.,) in an off-site location.

Establish safe reporting guidelines and escalation methods to protect the identity the person who reports

Respond to and recover from cyber security incidents

4

Initial assessment: To ensure an appropriate response, it is essential that the response team find out:

How the incident occurred

Which IT and/or OT systems were affected and how

The extent to which the commercial and/or operational data was affected

To what extent any threat to IT and OT remains.

Recover systems and data: Following the initial assessment of the cyber incident, IT and OT systems and data should be cleaned, recovered and restored, so far as is possible, to an operational condition by removing threats from the system and restoring software.

Investigate the incident: To understand the causes and consequences of a cyber incident, an investigation should be undertaken by the company, with support from an external expert, if appropriate. The information from an investigation will play a significant role in preventing a potential recurrence.

Prevent re-occurrence: Considering the outcome of the investigation mentioned above, actions to address any inadequacies in technical and/or procedural protection measures should be considered, in accordance with the company procedures for implementation of corrective action

5

Educate your stakeholders.

Frame cyber safety rules as Do's and Don'ts (Refer Annexure - I)

Orient school administrators with latest tools that can be used to monitor the sites visited by the students/ teachers.

Orient the stakeholders on cyber laws (http://cyberlawsindia.net/)

Bring in cybersecurity professionals to raise awareness levels about the risks in cyberspace and its preventative measures

Introduce courses/ lessons/ activities for students and teachers on major components of cyber security and safety.

Advocate, model, and teach safe, legal, and ethical use of digital information and technology.

Promote and model responsible social interactions related to the use of technology and information

Celebrate Cyber Security Week and conduct activities to create awareness through cyber clubs

Establish a relationship with a reputable cybersecurity firm/ organisation.

Be aware about policies and procedures to keep the school safe and secure in cyberspace.