ELITE American Private School

الإمـــارات THE EMIRATES

Cyber Safety and Security

Guidelines for School

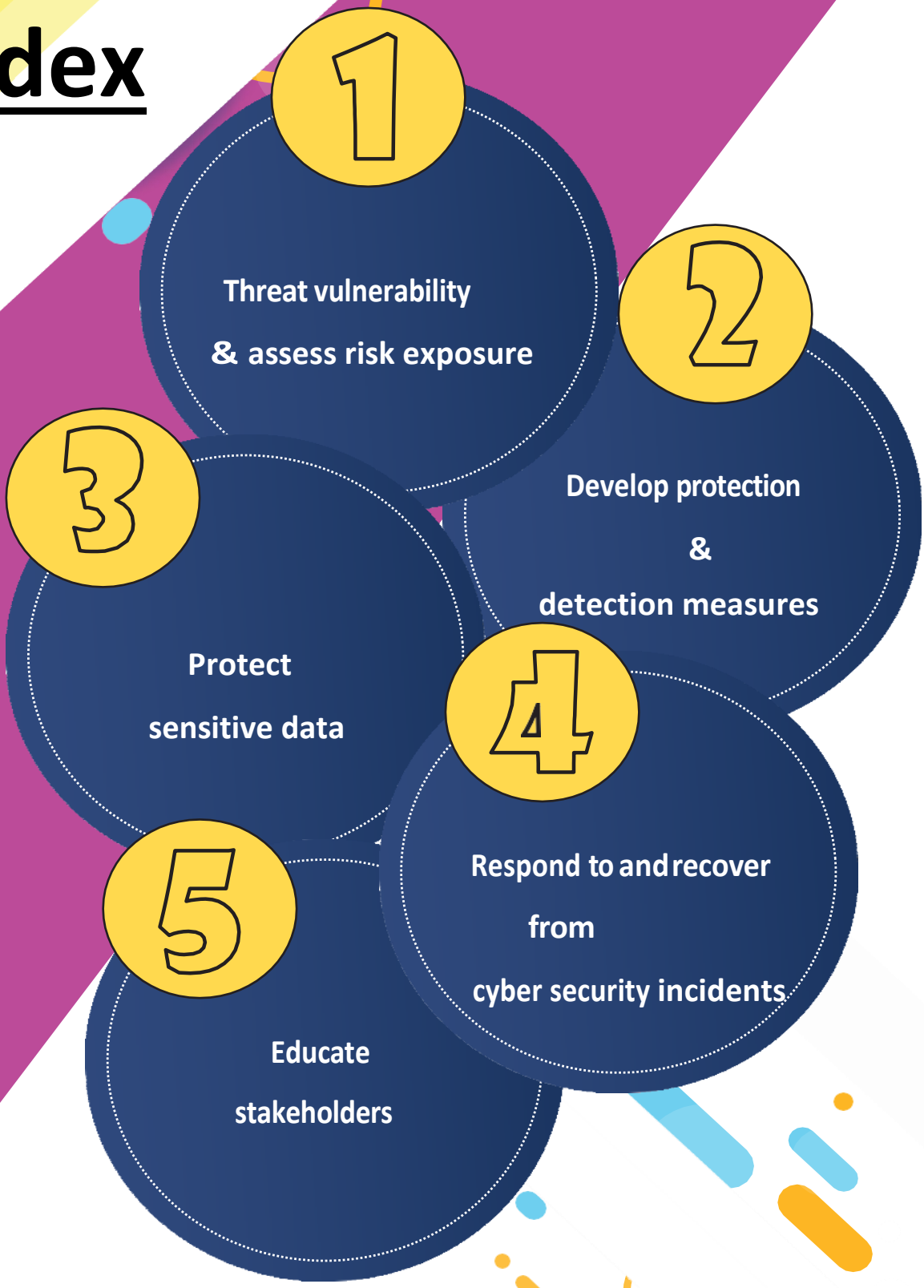
Be safe in the cyber world…

Cyber safety is the safe and responsible use of information and communication technology. It is not just about keeping information safe and secure, but also about being responsible with that information, being respectful of other people online, and practicing good internet etiquette.

As information infrastructure and Internet became bigger and more complex, it became critical to maintain systems functional and alert to security issues. Though the system administration tasks have become easier in recent years, school administrators need to be more updated on the systems and network security In recent years, all systems are exposed to Internet; hence there is increased challenge in maintaining and protecting them from the attackers.

Schools play a key role in promoting internet safety. Schools are primarily responsible for keeping systems, computers, network devices secure and functional. It is important to keep the information as secure as we keep the systems and network devices in the organization.

Index


1
Threat vulnerability
& assess risk exposure
2
Develop protection
&
detection measures
3
Protect
sensitive data
4
Respond to and recover
from
cyber security incidents
5
Educate
stakeholders

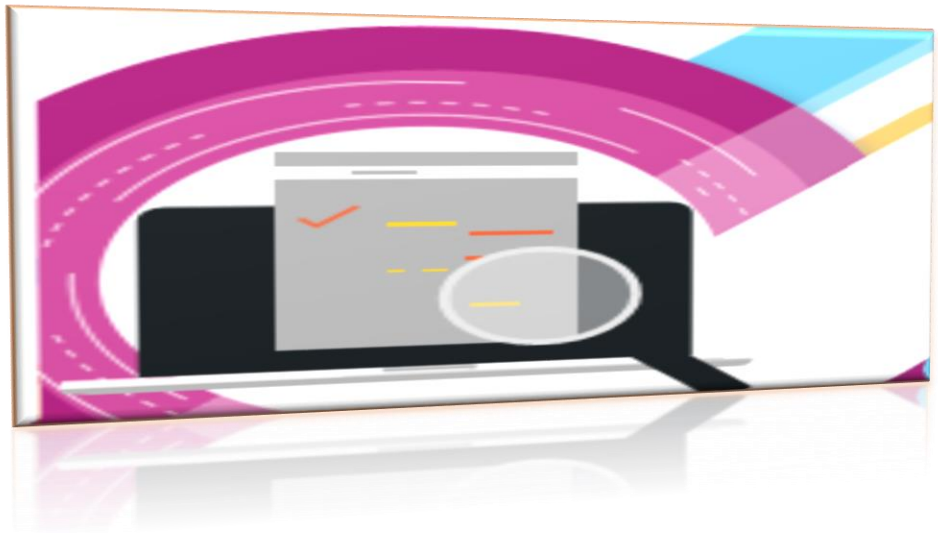
1 Identify threat vulnerability & assess risk exposure

- Slow and sluggish behavior of the system.
- Inexplicable disappearance of system screen while working.
- Unexpected pop ups 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.
- Navigation 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.

2 Develop protection & detection measures

- 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, avoid 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 drive.
- Set up your computer for automatic software and operating system updates. Check that antivirus software in each system is regularly updated.
- Consider blocking of file extensions such as .bat, .cmd, .exe, .pif by using content filtering software.
- Ensure that third-party vendors (who have contract with the school) have strong security measures in place.
- Consider contracting with a trusted / verified third-party vendor to monitor the security of our school's network.
- Protect the 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", "safe search", "supervised users" and other similar filters and monitoring systems, so that no child can access harmful content via the school's IT systems, and any concerns can be detected quickly.



3 Protect sensitive data

- Design and implement information security and access control programs 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 (contact numbers, email IDs etc. in an off-site location.
- Establish safe reporting guidelines and escalation methods to protect the identity of the person who reports the breach of security.

4 Respond to and recover from cyber security incidents

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

  - How the incident occurred?

  - Which IT systems were affected and how?

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

  - To what extent any threat to IT remains?

- **Recover systems and data:** Following the initial assessment of the cyber incident, IT systems and data should be cleaned, recovered and restored, as much as possible, to an operational condition by removing threats from the system and restoring the 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:** Complying with the outcome of the investigation mentioned above, any inadequacies in technical and/or procedural protection measures should be addressed, in accordance with the company procedures for implementation of corrective action.

5

Educate stakeholders

- **Frame cyber safety rules as Do's and Don'ts for the Schools.**
- **Orient school administrators with latest tools that can be used to monitor the sites visited by the students/ teachers.**
- **Consult cyber security professionals to raise awareness levels about the risks in cyber space and their preventive 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**
- **Follow guidelines, policies and procedures to keep the school safe and secure in cyberspace**