CMSGu2016-05

National Computer Board

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Guideline on IT security for Academic Institutions

CERT-MU

National Computer Board
Mauritius

Version 1.0

October 2016

Issue No. 5

Table of Contents

DISCLAIMER: *This guideline is provided "as is" for informational purposes only. Information in this guideline, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

1.0 Introduction

1.1 Purpose and Scope

This document provides an overview of how academic institutions should manage network security, often referred to as cyber-security or e-security. It is intended to support academic institutions in drawing up a policy setting out their approach for the ongoing management of e-security risks, issues and incidents.

1.2 Audience

The target audience for this document includes academic institutions management staff, IT technicians, ICT educator, lecturer and students.

1.3 Document Structure

This document is organised into the following sections:

Section 1 contains the document's content, the targeted audience and the document's structure.

Section 2 gives a background on the use of Internet in academic institutions.

Section 3 discusses some issues that academic institutions encounter on the Internet.

Section 4 provides the precautionary measures that academic institutions should take.

Section 5 concludes the document.

Section 6 contains a list of references that have been used in this document.

Appendix A illustrates some security rules for academic institutions.

2.0 Background

Academic institutions, just like any other commercial or public sector institutions, are now reliant upon the Internet services for day-to-day operations and activities. The Internet brings a wide range of opportunities and advantages, offering news ways to support teaching and learning as well as restructuring operational and administrative processes. However, it also poses risks if the technologies used are not managed and maintained appropriately. These risks include the loss of sensitive and confidential personal data. Another potential risk could also involve network failure due to a security incident, reduced or lost capability to deliver timetabled events and scheduled teaching and learning.

Internet access is now imperative for academic institutions. As such, all academic institutions need to have in place appropriate mechanisms to maintain the integrity and availability of their network services and resources. Security threats and incidents do not just come from outside the institution. Internal users can pose a threat too, whether through accidents, carelessness, and ignorance of their responsibilities or malicious intent.

While the Internet has made it easier for criminals to obtain weapons or to learn how to build their own, technology is also a vital factor in academic institution security preparedness.

3.0 Internet Dangers for Academic Institutions

Academic institutions today face increasing Internet security risks from the number of new platforms and technologies used by students and teachers in and out of the classroom. The proliferation of social networks such as Facebook, Twitter, YouTube and MySpace, instant messenger, file-sharing and peer-to-peer applications mean that the IT teams in academic institutions have to cope with an even greater number of threats than many corporate networks. Violence in academic institution has become commonplace. Experts have attributed the trend to several social factors:

- The ease of anonymously obtaining tools online
- Cyberbullying, where social media is used to humiliate peers
- Endless cycles of escalating violence perpetrated by kids against kids

Below are some of the threats that academic institutions are prone to encounter:

3.1 Malware

The most common threats to academic institution networks, comes from downloading malware. This is most commonly done by clicking on links shared between students within, for example, instant messages (e.g. on social networks like Facebook) and emails. This risk is elevated by the use of file sharing and peer-to-peer technologies such as BitTorrent, by which users can download files including rich media such as music and film from multiple, and usually unsecured sources. Using such technologies can expose academic institutions to malware that could take over one or more computers and use them to run a botnet, for example, or even, steal personal information on the academic institution and its students.

3.2 Denial of service

The unauthorised downloading of video and music files, even if free from malware, can present another problem to academic institutions. The time and bandwidth that downloading a movie from the Internet normally takes can slow down an Internet connection. If many students download music and video files simultaneously, with or without authorisation, it can seriously affect the performance of the network.

3.3 Inappropriate websites

Many students explore sites not meant for their age. Academic institutions have a responsibility to prevent children visiting adult, illegal or otherwise inappropriate websites. It is up to the academic institution's security system to do this. A teacher simply cannot oversee every website that a student visits. Web filtering technology can ensure that blacklisted websites, or sites containing potentially damaging content, are blocked from use. Filtering should work both ways, and prevent students from being able to upload explicit, offensive or abusive images or messages to websites.

3.4 Social media/ Disclosing personal information

Facebook, Twitter and other social networks make it easy to communicate and share personal information. They can, however, represent a problem for academic institutions with bullying and the publishing of information that the academic institution would not want to share with the public.

The most serious security issue is that of protecting children from carelessly giving out their personal information online. Most online websites, virtual worlds and games for children will use moderators to prevent children from giving out personally identifiable information about themselves, such as address, phone number or academic institution details that could lead to grooming. Academic institutions should monitor websites that children access to ensure that they have safety measures such as moderation in place and might consider blocking those that do not.

3.5 Social issues

There are a number of social issues that Internet security raises for academic institutions, too. Students tend to be much more inclined to the newest technology than adults. So they need a security system that can compensate for this. Dedicated security companies that manage the latest technologies to combat trends in Internet use are worth considering, rather than stand-alone systems that require manual updating and configuring by the academic institution's IT staff. Equally, academic institutions should put in place security at the network gateway, so updates apply across all computers rather than individual computer security. This means updates can be pushed out across the network, rather than having to be applied individually, and keeps all computers are up to date all the time.

4.0 Preventive Measures for Academic Institutions

To safeguard an academic institution today represents various challenges. These challenges include the number of people visiting the institution on any given day and the size of academic institutions' facilities, with their several entry and exit points. Today's academic institutions now recognise the increased need for security preparedness. Everyone wants to make sure that academic institutions are equipped to protect their students and staff from the potential for violent attacks.

4.1 Database security

- Use a password policy
- Enforce password changes on a set period
- Make sure no default passwords are left set
- Use strong passwords
- Admin accounts should change password more often than general users
- Use the least privilege security model
- Only provide the privileges an account needs to do the work required
- When user's roles change the privileges must match the role
- All access must be through an authenticated login
- Rename, lock and expire default accounts
- Apply all security patches for the host operating system and the database system
- If possible harden the operating systems (OS)
- Restrict anonymous access as much as possible; where possible do not allow at all
- Any batch jobs must not have user ID or passwords within them
- If possible encrypt the network traffic using certificates

4.2 Risk Management

Academic institutions need effective risk management and governance, and policies and procedures to protect the personal data held in emails, faxes; staff training and through actions such as shredding all confidential paper waste and checking the physical security of premises. Measures that can be taken to keep data secure include:

- Promote a risk management culture.
- Take regular backups of files (backup copies should be stored in fireproof safes or offsite).

- Use a system of passwords so that access to data is restricted.
- Safely store important files on removable disks, e.g. locked away in a fireproof and waterproof safe or off-site.
- Allow only authorised staff into certain computer areas, e.g. by controlling entry to these areas by means of ID cards, magnetic swipe cards or other devices
- Always log off or turn terminals off or lock them.
- Avoid accidental deletion of files by write-protecting disks or files.
- Use data encryption techniques to code data.
- Ensure third-party managed IT services have security controls in place – check contracts and service level agreements.
- Remove any software or equipment that you no longer need
- Delete data before disposing or re-allocating equipment.
- Review and manage any change in user access, such as the creation of accounts when staffs arrive and deletion of accounts when they leave.
- If your academic institution system is disrupted or attacked, ensure that the response includes removing any ongoing threat such as malware, understand the cause and review security.

4.2 Portable Devices and staff / student policies

When staff and students work remotely on mobile devices, ensure that suitable measures are taken to protect laptops and tablets and the systems on which the data is stored.

Write and publish a written policy so that all staff or students know their responsibilities, e.g.

- If possible mobile device should be encrypted.
- Do not leave devices visible when away from the car
- Do not allow non-employees to access devices
- Do not connect to public Wi-Fi
- Use encrypted Wi-Fi traffic e.g. WPA2
- Do not use third party USB devices
- Secure home routers
- Change default passwords
- User higher WIFI security level
- Change the default SSID
- If possible assign static IP addresses

- Install and keep up to-date antivirus, firewall and malware software
- Have an automatic partial antivirus sweep of the device on start up or daily
- Have a full antivirus sweep of the device weekly
- Keep device patches up to date

4.3 Anti-virus software

- Antivirus, firewall and malware software should be running all the time; this is known as “Real Time Protection”
- An antivirus and malware sweep should happen daily; usually at or just after start-up.; this would be a partial sweep
- A full sweep should take place at least once a week
- Antivirus, firewall and malware software can usually be bought as a single product e.g. Sophos, MacAfee, Symantec, Microsoft
- If possible the product should be centrally managed by the academic institution or a supplier
- Have a support contract with the vendor of the system/application.
- Read the vendor advisory notices for your system/application.
- Apply all patches relevant to your system/application.
- Relevant staff should keep their training up to-date as possible for the systems/applications they support.

4.4 Data Protection Act

If you handle and store information about identifiable, living people, such as students and staff, you are legally obliged to protect that information under the **Mauritian Data Protection Act 2004**. As an employer the academic institution is obliged to protect employees’ personal information. Your students have a right to see their personal information. They can make a subject access request to see the personal information you hold about them. Students and parents have the right to see their educational records. If the academic institution intends to publish examination results in the media, pupils and students must be informed first.

5.0 Conclusion

The Internet brings many benefits to academic institutions as it offers new ways of supporting teaching and learning. It also streamlines operational and administrative processes. However, the Internet beings many risks with it and if these are not managed properly they can be disruptive. It is not appropriate simply to block students from using new technologies. They need to learn how to use technologies, and should be encouraged. So, the approach that academic institutions take to IT security needs to be safe, but not restrictive. There needs to be flexibility for security to be effective.

6.0 References

- **http://www.securadyne.com**
- **http://www.weareevery.com**
- **http://www.nen.gov.uk**
- **http://www.teachingtimes.com**

Appendix A

10 Security Rules for Academic Institutions

1. **Create clear security guidelines**

   Creating clear rules for both students and teachers will help everyone know exactly what is expected of them, and what the consequences are in case of any breach. The rules need to be enforced by the security system and IT staff, but should be made clear to users. Knowing what they can and can't do is an important part of security. Guidelines should be reviewed and it should be speficied how new technologies and platforms can be used, such as social media access, which Instant Messaging (IM) platform can be used and what the limits are on file downloads.

2. **Educate students on the importance of security**

   Students should ensure they understand why the rules are in place, that is, for their own online protection and that of other students and teachers.

3. **Stay informed**

   Teachers and IT staff in academic institutions should make sure that they are up to date with the latest technologies and platforms that are being used in and out of the classroom by their students. Advice on new technologies should be available online to help you stay on top of new trends.

4. **Keep your security systems up to date**

   Even if you are informed about what IM platform to use, if your security system is allowing an unauthorised technology without your knowledge, the system will be vulnerable.

5. **Agree what platforms are and aren't acceptable**

   For example, agree which provider to use for IM, blogging, video streaming, etc., and don't allow any other onto the system.

6. **Set strict web filters and password systems, and monitor web and IM use**

   Check the bandwidth usage. If the system is slow, check that no-one is downloading video, or using a file-sharing or peer-to-peer application. Set limits on music or video

download (if required), except on secure, password-protected computers. This will limit bandwidth use.

7. **Monitor access to the Internet, and to platforms and applications**

   For example, check which student has accessed which sites by using individual, secure IDs and passwords. Security companies such as Network Box can integrate with the active directory of the academic institution and transparently cross-check logins against the material being accessed.

8. **Set the same stringent security controls to information leaving the network as to information coming in to the network**

   This can help prevent unauthorised applications (such as the wrong IM provider) from being used, and prevent an academic institution's IT network from unknowingly being used to distribute information.

9. **Block all third party plug-ins and devices, except those approved by the academic institution**

   This will help decrease the possibility of external sources corrupting the network.

10. **Do not allow unsupervised time on academic institution computers where possible.**

    If you spot any unusual activity, this can be checked against the registered login system or log book.