

LABORATORY INFORMATION MANAGEMENT TRAINING

Module 5- Information Security and Contingency Planning

SUPRANATIONAL REFERENCE
LABORATORY, UGANDA

Module Objectives

At the end of this module, participants will be able to:

- ☁ Define information security and Contingency Planning
- ☁ Describe benefits of a Contingency Plan in Information Security

Information Security

- ☁ The practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information.
- ☁ The information or data may take any form, e.g. electronic or physical.

Information security...

☁ Information security's primary focus is the balanced protection of the confidentiality, integrity and availability of data (also known as the CIA triad) while maintaining a focus on efficient policy implementation, all without hampering organization productivity.

Confidentiality

☁ In information security, confidentiality "is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes."

☁ Examples of confidentiality of electronic data being compromised include laptop theft, password theft, or sensitive emails being sent to the incorrect individuals



Integrity

- ☁ In information security, data integrity means maintaining and assuring the accuracy and completeness of data over its entire lifecycle.
- ☁ This means that data cannot be modified in an unauthorized or undetected manner.



Availability

- ☁ For any information system to serve its purpose, the information must be available when it is needed.
- ☁ This means the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly.

Contingency Plan

☁️ A contingency plan is a plan devised for an outcome other than in the usual (expected) plan.

☁️ It is often used for risk management for an exceptional risk that, though unlikely, would have catastrophic consequences.

Risk management

☁ Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resources to the organization.



Security classification for information

☁ An important aspect of information security and risk management is recognizing the value of information and defining appropriate procedures and protection requirements for the information. Not all information is equal and so not all information requires the same degree of protection.

Security classification for information

☁ Some factors that influence which classification information should be assigned include how much value that information has to the organization, how old the information is and whether or not the information has become obsolete.



Information Security Measures

☁ Establish strong passwords.

- Implementing strong passwords is the easiest thing you can do to strengthen your security.

Information security measures

☁ Put up a strong firewall.

- In order to have a properly protected network, firewalls are a must.
- A firewall protects your network by controlling internet traffic coming into and flowing out of your business.



Information security measures

☁ Install antivirus protection

- Antivirus and anti-malware software are essentials in your arsenal of online security weapons, as well.
- They're the last line of defense" should an unwanted attack get through to your network.



Information Security Measures...

☁ Update your programs regularly

- Making sure your computer is "properly patched and updated" is a necessary step towards being fully protected; there's little point in installing all this great software if you're not going to maintain it right.

Information Security Measures

☁ Secure your laptops

- Because of their portable nature, laptops are at a higher risk of being lost or stolen than average company desktops. It's important to take some extra steps to make certain your sensitive data is protected.

Information Security Measures

- Backup regularly
- Scheduling regular backups to an external hard drive, or in the cloud, is a painless way to ensure that all your data is stored safely.

Exercise

1. What is information security?
2. What is Contingency planning?
3. What measures can be taken to ensure information security?

Summary

Referece

- <https://www.entrepreneur.com/article/217484>
- Roland Cloutier, Chief Security Officer for ADP and a board member for the [National Cyber Security Alliance](#)

Acknowledgments

