Ira A. Fulton Schools of Engineering
Arizona State University

Lab 10 – Cybersecurity Policy – A Strategic Focus

Student: Yengkong Sayaovong

Arizona State University

IFT 202

Instructor: Gary Grindle

Due Date: February 26, 2023

INTRODUCTION

This is where you type the introduction to the Lab by writing a summary of the purpose and goals.

1. IT Security Policy Review Summary Analysis

Information Technology Security Policy identifies procedures for individuals accessing an organization's resource.

Security threats are growing every day so company's must develop a security program to meet challenges. Without an information technology security policy, it is impossible to integrate a security program to communicate security measures to third parties.

Inside of any security policy there should be two parts. Maintaining the integrity of the network and reducing internal risks. Addressing external threats are done and available through external networks such as firewalls, antivirus software's, intrusion detection systems and email filters.

Legal concerns organizational features, contract terms, environmental issues and user inputs can all be incorporated into a company's policy.

2. New or Reconstructed Security Policy

Information Systems: All electronic means used to create or communicate in conduct of administrative activities.

Authorized User: an individual that is authorized to access resource within an organization.

Extranet: an intranet that is partially accessible to authorized people outside of an organization.

General Use:

Access requests must be authorized and submitted from departmental supervisors for employees to gain access to computer systems.

3. National Center of Education Statistics Publication 98-297, Chapter 3, and Checklist on Developing Security Policy Review

Accountability in the workplace is essential for any organization's success. Accountability is about setting and holding people to an expectation that is determined by the company's vision, mission, goals, and values.

Accountability that does not succeed often times starts with an individual who fails to meet expectations. Other times, it starts at the leadership level who simply accepts the unacceptable.

Accountability requires hard work and tremendous amount of consistency to follow through from both the leadership team and also the employees of the company.

CONCLUSION

In Conclusion, having a security set in place for any organization is necessary but the leadership team must train its employees and be consistent on what is acceptable and what is not acceptable in any work environment.

REFERENCES

How to develop an effective information security policy. (n.d.). Retrieved February 27, 2023, from https://www.powerdms.com/policy-learning-center/how-to-develop-an-effective-information-security-policy