# Five important security policies

Omarion Branch

Department of Cybersecurity, Old Dominion University

CYSE 300: Introduction to Cybersecurity

Professor Malik A. Gladden

September 17, 2023

After conducting research through several websites, I was able to come up with my five must have polices that need to be discussed when dealing with network security. The five polices that are certainly needed are acceptable use, security awareness & training, remote access, password creation & management and lastly network security policy.

## Acceptable Use

The acceptable use policy, also known as (AUP) goes over the acceptable usage of computer equipment within a network company. The AUP outlines and defines the inappropriate use of computer equipment and the risk it may cause of not followed correctly. Failure to comply with the rules may result in compromised networking systems and could possibly result into legal consequences. A simple example of inappropriate use would be when an associate/employee goes on social media or does personal online shopping on a company computer that should only be used for his or her job. The AUP also list appropriate behavior that is allowed as well.

## Security Awareness and Training

Security awareness training goes for all employees, so they can properly do their job while maintaining safety of company information. Employees have no choice but to sign a confidentiality agreement and provide proof of completion once training has been completed. Training should be constructed in a way to educate users on the security policy within the agreement while developing an understanding of how the policy protects the business, employees, and customers.

## Remote access

Remote access is when you’re trying to connect to the company’s network from any host. The remote access policy is created to minimize potential exposure from damages that can happen from unauthorized use of resources. This policy is to be directed to all employees and should include rules for sending and receiving emails and other outside resources. The policy also needs to include requirements for VPN access and disk encryption.

The rules are going to be quite the same as the ones implemented onsite. For instance, employees are not to engage in illegal activity on their remote access along with not letting unauthorized users to use their work device, along with logging out before leaving device unattended. They are also to be required to install every update to ensure their own devices have the last software and operating systems.

## Password Creation and Management Policy

The password creation and management policy provides guidance on developing and reviewing appropriate passwords used to identify users. This policy touches on awareness to why one should choose and string password. It includes rules for changing password and the risk of reusing a password. There should be set specifications on password complexity, length and reasons why you shouldn’t use a password that is connected to other personal applications.

## Network Security Policy

A complete network security policy ensures the confidentiality, integrity, and availability of data on a company’s network system by following procedure for conducting information system and network review on a daily basis. This policy makes sure that systems have appropriate software and hardware to complete the tasks necessary for the job. Audit events are required to include information on failed log in attempts, usage on privileged accounts, anomalies on firewalls, devices added or removed and a detailed report on date, time and origin of the activity conducted along with who did it.

In conclusion, these policies were the five most important ones that stood out to me. In order for a networking company to be successful and mitigate any attacks that happen, these have to be in place. Yes, there are over a hundred other policies out there that need to be use but for this paper purpose I only introduced those.

## References

Ekdahl, H. (2023, February 21). *5 must-have cyber security policies for your organization*. Idenhaus Consulting. https://www.idenhaus.com/5-must-have-security-policies-for-your-organization/

Irwin, L. (2023, September 13). *The top 5 information security policies your organisation must implement*. IT Governance UK Blog. https://www.itgovernance.co.uk/blog/5-information-security-policies-your-organisation-must-have

Security, A. (2023, August 23). *10 must have IT security policies for every organization*. Adsero Security. https://www.adserosecurity.com/security-learning-center/ten-it-security-policies-every-organization-should-have/