Security Plan

# Network Architecture Report

Kayla Echols

Julia Wilkins

Riley Dorough

Brett Wolff

January 29th, 2022

**Table of Contents**

|  |  |  |
| --- | --- | --- |
| **Section Title** | **Author** | **Page #** |
| 1. Minimum Security Standards/Procedures | Brett Wolff | 3 |
| 1. Incident Reponses Plans | Kayla Echols | 4 |
| 1. References |  | 5 |

**Minimum Security Standards/Procedures**

|  |  |
| --- | --- |
| **Antivirus/Windows Defender** | Windows defender will be used for applicable computers. Security definitions will be updated regularly. |
| **Application Patches** | Applications will be maintained on the latest available update so long as it does not impact utility. |
| **Firewall** | Firewall rules and status will be maintained only by authorized personnel. Rules will follow strict control. |
| **Credentials** | Credential assignments will be handled by HR and closely managed to ensure employees have only just as much permission as they need. |
| **Logging** | Any logs produced by the system will be saved and backed up to a centralized server for collection and analysis. |
| **Intrusion Detection System** | Possible tool to be used based around AI/ML, but until then all detection will be handled by windows defender. |
| **Physical Assets** | Only authorized personnel will be allowed access to sensitive areas, which will be limited by |
| **Training** | All training should be done as soon as released. Employees should be trained in anything pertaining to their work and any necessary security protocols. |
| **Passwords** | Passwords will follow a template to ensure strength, and will be required to be reset every six months.   * Minimum 8 characters * 1 lowercase letter * 1 uppercase letter * 1 number * 1 special character   Additional rules include   * Do not use the last five passwords * Do not reuse the same password on multiple accounts or services * Do not share passwords except in emergency circumstances or when there is an overriding operational necessity. |

**Incident Reponses Plans**

· Detection and Details: The incident will be found on a system and details must be documented using the Incident Response template. The data that must be collected from the incident includes the date/time of the start of the attack, the date/time the attack was discovered, the attacker source IP address, the targeted systems IP address, and the target port or service. How the detection was discovered also must be documented for future reference.

· Result of the attack and vulnerability: The result of the attack or incident must be documented to solve the problem correctly. The result will help with the discovery of the vulnerability on the system. The vulnerability must be found to move on to the next step of containing the problem.

· Containing the vulnerability: Once the incident is discovered, it must then be contained in a timely manner to keep the system safe from more attacks. The containing could look different for each situation but must be documented in the Incident Response Report.

· Remediation Actions/Controls: There must be steps put in place to keep this vulnerability from being an issue again. These steps must be documented in the remediation and controls section of the document. This step will help prevent this problem from being an issue in the future.

References

Bansley, R. (2021). Incident Response Report Template. CSIS 461: Technical Aspects of Computer Security.