**Lab Rats Inc.**

Project Plan

# Final Project

# Date: 11 June 2023

**This Report was prepared by:**

**Andrew Waddell**

**andwadde@uat.edu**

# Executive Summary

### Introduction to the report

Final Project.

### Project Report

Detailed report.

# Introduction

This report is generated from the NTW216 contract to Lab Rats Inc., work order number 2020021700FIN. Lab Rats Inc. is pleased to present the Security Program Implementation Plan for the new data center of our organization. This plan outlines the strategies and measures to be implemented to protect sensitive customer information stored within the data center. The proposed data center will be one of the largest in our organization's western region and will play a crucial role in supporting our continued growth.

# Project Report

The Company requires a new infrastructure setup for continuing operations. The primary goals of the security program implementation plan are to ensure the confidentiality, integrity, and availability of sensitive customer information, protect against unauthorized access, data breaches, and other security threats. Comply with relevant regulatory requirements and industry best practices and minimize downtime and maintain business continuity in the event of a security incident.

Please refer to the attached logical network diagram (PowerPoint) for the proposed Enterprise layout. This diagram provides an overview of the network infrastructure, including the placement of key components and their connectivity.

The current network infrastructure consists of one domain controller, one file server with an attached storage array, one update server doubling as a print server, a storage array of 24 drives in a RAID 1 configuration and a UPS only on the domain controller.

Based on our previous assignments, we propose the following improvements to the network infrastructure as shown below:

* Implement a redundant domain controller for high availability and failover. This ensures high availability and failover capability. In the event of a hardware failure or maintenance, the redundant domain controller can seamlessly take over the authentication and authorization processes, minimizing downtime and ensuring uninterrupted access for users.
* Introduce a dedicated print server to separate print services from other critical functions. Separating print services into a dedicated server provides several benefits. Firstly, it reduces the load on the update server, allowing it to focus solely on its primary function. Secondly, it improves security by isolating print services from other critical functions, minimizing the attack surface and reducing the risk of unauthorized access or exploitation.
* Implement a separate update server to ensure timely and secure software updates. Having a dedicated update server ensures timely and secure software updates for the entire network. By separating update services from other functions, it minimizes potential disruptions caused by updates, allows for more efficient patch management, and enhances security by ensuring that critical security patches are promptly deployed.
* Upgrade the storage array to a more robust and scalable storage solution, such as a SAN (Storage Area Network), to enhance performance, reliability, and data protection. This offers several advantages. SANs provide improved performance, scalability, and data protection capabilities compared to local storage arrays. They enable efficient centralized management, high-speed data transfers, and better fault tolerance through features like RAID (Redundant Array of Independent Disks) configurations. This upgrade enhances the overall storage infrastructure's reliability, performance, and ability to handle future growth.
* Deploy additional UPS units to provide power backup for critical servers and networking equipment. By deploying additional UPS units ensures power backup for critical servers and networking equipment. This mitigates the risk of data loss or system downtime due to power outages or fluctuations, ensuring the availability and integrity of sensitive customer information.

Because our customers are our main priority, we must ensure that we protect their information at all costs. In order to protect sensitive customer information, we recommend implementing the security measures and controls shown below:

* Access control: Implement strong authentication mechanisms, such as two-factor authentication, and enforce the principle of least privilege. This type of authentication ensures that only authorized personnel can access the network and sensitive information. Enforcing the principle of least privilege ensures that users are granted only the necessary permissions to perform their job functions, reducing the risk of unauthorized access or accidental data exposure.
* Firewalls and network segmentation: Configure firewalls to segregate network segments and control traffic flow, minimizing the risk of unauthorized access. By segmenting the network into logical zones, each with its own firewall rules, we can control traffic flow, restrict access to sensitive systems, and minimize the impact of potential breaches.
* Intrusion Detection and Prevention System (IDPS): Deploy IDPS to monitor network traffic for signs of unauthorized activity and block or mitigate potential threats. This type of system can detect and block intrusion attempts, suspicious behavior, or known attack patterns, protecting sensitive customer information from unauthorized access or compromise.
* Encryption: Implement data encryption at rest and in transit to protect customer data from unauthorized access. Encryption ensures that data remains confidential and protected, both when stored within the data center and when transmitted over the network.
* Security monitoring and logging: Deploy a centralized security information and event management (SIEM) system to collect and analyze logs from various systems for detecting and investigating security incidents. By monitoring and analyzing security events, organizations can identify and mitigate potential threats, investigate incidents, and ensure regulatory compliance.
* Incident response: Develop and implement an incident response plan to ensure a timely and effective response to security incidents. It establishes clear procedures for detecting, responding to, and recovering from security breaches, minimizing the impact on customer data and the organization's operations.
* Regular security assessments: Conduct periodic vulnerability assessments and penetration testing to identify and address any security weaknesses. By proactively identifying vulnerabilities, organizations can remediate them before they are exploited by malicious actors, reducing the risk of data breaches and maintaining a robust security posture.

We have broken up the proposed timeline for the implementation of the security program in the new data center is as shown below:

Week 1-2: Conduct a comprehensive security assessment and risk analysis.

Week 3-4: Design and procure necessary security infrastructure and software.

Week 5-6: Implement access control measures and configure firewalls.

Week 7-8: Deploy intrusion detection and prevention systems.

Week 9-10: Implement encryption mechanisms and security monitoring/logging.

Week 11-12: Develop and test the incident response plan.

Week 13-14: Conduct employee training and awareness programs.

Week 15-16: Finalize the security program implementation and conduct a post-implementation review.

We have also provided the proposed labor cost for the security program implementation, based on the provided information, is as follows:

* Jr. System administrator hourly rate: $64
* Sr. System administrator hourly rate: $94

Please understand that the exact labor cost may vary depending on the specific tasks, expertise required, and number of hours worked by each team member.

We at Lab Rats Inc. are committed to ensuring the utmost security for our customers’ sensitive information. The proposed Security Program Implementation Plan provides a comprehensive strategy to protect customer data and mitigate potential security risks. By following this plan and implementing the recommended security measures and controls, we aim to establish a robust and secure data center that meets the requirements of our organization and complies with industry standards.