BIT Project Management Plan

Real Estate Network

March 6th, 2020

Team Members

Domonic Neal

Ny Tran

Ronny Soto

Document Control

Change History

Revision	Change Date	Description of changes
V1.0	03/06/2020	Initial release
V1.2	03/07/2020	Finishing touches

Document Storage

This document is stored in the project's repository at:
https://github.com/umkc-cs-451-2020-spring/semester-project-group-15

Document Owner

Domonic Neal is responsible for developing and maintaining this document.

Table of Contents

1 *Overview*

1.1 Purpose and Scope

Monstrosity Inc. is in need of a secure network that will allow its employees to access their company resources along with Wifi connectivity and functionality for their customers. Within their network web trafficking filtering needs to be performed to control the access and restriction of certain websites. Along with web filtering the network and its employees need a secure email option that is spam and virus detection capable as well as intrusion detection being a high priority feature. The network also contains a database that needs to be hosted with capability to handle clustering and backups. The purpose of this document is to provide information on the needs and requirements of the network that will be implemented for Monstrosity Inc. In the introduction of this document you will find the Goals & Objectives, Scope and Definitions. This document then goes on to outline Design Constraints, Non-Functional Requirements, and Functional Requirements for the network implementation for Monstrosity Inc.

To address other areas of this project there will be separate documents in which outline and address Project Constraints, Project Management Plan, & Test Specifications and procedures.

1.2 Goals & Objectives

The main objective for this project is to create a secure and efficient network for employees of Monstrosity Inc. along with other required specifications outlined in this document. The network and system is expected to provide:

- Access to company resources
- Wifi Connectivity
- Web Filtering
- Secure email with spam & virus detection
- Intrusion Detection
- Database Hosting with clustering & backup

1.3 Project Deliverables

With the implementation of this network employees of Monstrosity should be able to use company resources effectively and efficiently while also remaining secure. Customers who visit locations should also have the ability to connect to wifi access points safely and securely as well. Behind the scenes assisting both employees and customers will be web filtering, spam & virus detection, intrusion detection, and database hosting implemented with clustering and backup capabilities.

The following items will be delivered to the customer on or before:

1. User's Guide
2. System Administrators Manual
3. Test Plan
4. System Test Cases

1.4 Assumptions and Constraints

Assumptions:

1. The hardware of the network will work correctly when implemented
2. Network Security will have no leaks and emails will be protected from spam/phishing
3. Facility and Staff will learn how to use the system easily

Constraints:

1. The network must operate across 6 locations enabling access to company resources regardless of location.
2. Resources like storage, files, and database clustering will effectively use AWS cloud services for hosting and secure and efficient data backup.
3. Raid 6 storage configuration will be used due to its high security, fast data transactions, and ability to adapt to failures with access to data remaining sustained.
4. The network must be completed and ready by 5/04/2020

1.5 Schedule and Budget Summary

Schedule Information (Major milestones and deliverables):

02/10/2020 - Gather requirements
02/23/2020 - Project Charter Complete
02/28/2020 - Requirements Document Baselined
03/02/2020 – Iteration 1 Closeout, Iteration 2 Begins
03/04/2020 – Requirements Document
03/06/2020 – Project Plan
03/16/2020 – Iteration 2 Closeout, Iteration 3 Begins
03/31/2020 – Iteration 4 Begins
04/07/2020 – Iteration 3 Closeout
04/20/2020 – Iteration 4 Closeout, Iteration 5 Begins
04/26/2020 – Test Plan
04/27/2020 – User and System Guide Due
05/01/2020 – Project Results, Slack/Discord & GitHub Communication

05/04/2020 – Iteration 5 Closeout

Financial Information (Cost estimate and budget information):

1 project manager at 4 hours per week for 14 weeks	56 hours * $50/hr = $2800
1 researcher at 4 hours per week for 14 weeks	56 hours * $40/hr = $2240
1 business analyst at 4 hours per week	56 hours * $30/hr = $1680

168 hours total, $6720 total, avg, $40.00 per hour

1.6 Success Criteria

- The project will be completed on the set date of 5/04/2020.
- Total cost of tools and requirements will not exceed our given budget.
- Testing will be conducted thoroughly so there will be a minimal risk exposure.

1.7 Definitions

Network - the product that is being implemented and delivered specified in this document

Project - the activities that will lead to the production and implementation of the product

Client - the person or organization the product is being delivered to; Monstrosity Inc.

User - those who will be using and interacting with the delivered product

Use Case - a detailed description of an interaction between the system and an actor. Use cases can have multiple alternative that are referred to as scenarios which take different routes to arrive at different outcomes

Actor - a user who is interacting with the system through a use case

Network Engineer - the person or people who organize, develop, implement / deploy or make any necessary changes to a network.

Stakeholder - a person of interest in the project and its results.

1.8 Evolution of the Project Plan

Before the start of each project initiation this document will be updated. These updates will include any new tasks to be scheduled and at the completion of the iteration this document will be updated again to reflect the actual required effort to complete each task.

2 Startup Plan

2.1 Team Organization

Project Manager: The project manager is responsible for planning, organizing, and managing risks. The main deliverables of the project manager is the project plan, schedule, budget, and risk management plan with the help of team members.

Product Manager: The product manager is responsible for the definition and evolution of the product concept

Network Engineer: the person or people who organize, develop, implement / deploy or make any necessary changes to a network.

Tester: Testers are responsible for devising testing procedures and detailed work of designing, writing, and executing test plans.

Writer: The writer is responsible for authoring or editing system documentation including user guides, system help text, release notes, etc.

2.2 Project Communications

The project will be distributed through Slack and Github. Information gathered will be discussed and added to our Google Drive.

2.3 Technical Process

Our methodology will be to do as much research to find quality tools, make sure things are secure, test thoroughly, and provide help & documentation.

2.4 Tools

- Version Control - Github repository will be used to store project documents
- Cisco Packet Tracer & GNS3 - allows us to build a network in a virtual environment
- AWS - cloud management and database clustering to effectively manage and store files and data

3 Work Plan

3.1 Activities & Tasks

Equipment Selection - Correct devices, servers, personal employee devices, routers, etc all need to be picked out and also needs to fit within the company budget

- Group members will focus on picking specific items depending on their area of research and according to the budget
- Work Estimate: 5 Hours
- Begins: 03/09/2020

Virtualization - Virtualization will be used to connect devices to the network. Various virtualization are programs available.

- Team will need to research and decide on which virtualization program to use.
- Work Estimate: 2 Hours
- Begins: 03/09/2020

3.2 Release Plan

03/11/2020 - All equipment for the company will be chosen

03/13/2020 - Determine specific Wi-Fi set up

03/16/2020 - Determine email security for the employees

03/27/2020 - Determine company network connection with all available locations

04/03/2020 - Network connected and fully operational with security for the network

04/17/2020 - Connect all available locations with Monstrosity Inc. Corporate location

05/06/2020 - Security access and Active Directory (SSO) will be developed for employees & customers

3.3 Iteration Plans

Iteration 1 - Develop specific documents and project charter

Iteration 2 - Determine the proper equipment selection and email security

Iteration 3 - Determine how the other 5 satellite locations will connect to the same network

Iteration 4 - Set up network at the 5 satellite locations along with the corporate location along with the Active Directory (SSO) for customers and employees

Iteration 5 - Set up wifi for employees and customers with proper restrictions. Implement different levels of security access for higher level employees

3.4 Budget

At the beginning of this project, there was no specified budget. We are aiming to deliver a technical solution based on the specific needs of the company and we are estimating that this could take around $45,000 to implement.

4 Control Plan

4.1 Monitoring and Control

Weekly - Team discussion before/after classes

02/17/2020 - Iteration 1

02/23/2020 - Project Charger

03/01/2020 - Requirements

03/02/2020 - Iteration 2

03/08/2020 - Project Plan

4.2 Project Measurements

Phase	Measurement	Source
Release Planning	Record effort estimates for product features	Mgr
Iteration Planning	Record effort estimates for scheduled tasks Update effort estimates for product features Update estimated dates in release plan	Mgr, Pgr
Iteration Closeout	Record actual effort for scheduled tasks Record actual effort for product features	Mgr, Pgr
Project Closeout	Archive project performance data in process database.	Mgr, Pgr
Ongoing	Record defects found from integration testing through first	Mgr, Pgr,

	year release. Assign each defect to one of the following categories: blocker, critical, major,minor, or trivial.	Tester

5 Supporting Process Plans

5.1 Risk Management Plan

Technical Risks

1. Network Compromisation
2. Hardware Failure
3. Data Manipulation
4. Data Leaks
5. Spam Activity

High Priority Risk Prevention

1. Network Compromisation
    a. Secure Firewalls
    b. Spyware
    c. Antivirus
    d. Network, Traffic, Server, & Backup monitoring
    e. Network Traffic Recording - allows us to monitor attacks and unusual behavior
2. Hardware Failure
    a. Maintenance
    b. Software Updates
    c. Scheduled Equipment Upgrades / Replacements
3. Data Manipulation
    a. File Integrity Monitoring - can determine what data was manipulated and send alerts
    b. Integrity Checking - allows us to ensure there are no errors when data is restored from backups
    c. Encryption
    d. Activity Logs - log and monitor changes to files

Contingency Plan

1. Network Compromisation
    a. For any instances where the network is or has been compromised temporarily shut the network down, check monitoring systems, make any

necessary changes to hardware devices and software whether it is passwords or configurations. Ensure firewalls, antivirus, and vpn are all configured properly as well. Once monitoring has resulted in normal traffic and everything has been reconfigured to bring back up the network. All attacks, reconfigurations and or changes must be documented.

2. Hardware Failure
    a. For any instances where there are hardware failures equipment shall be reconfigured or replaced as needed.
3. Data Manipulation
    a. For any instances where data has been manipulated activity logs will need to be verified to confirm who, what, when, and where the file was manipulated. Once this information has been verified and documented that file can be restored from its previous backup version.

The risk management plan will be updated based on any major network changes whether hardware or software based. Any instances of failures, attacks, or manipulation the plan will also need to be updated to fit these needs to prevent such risks from becoming recurring issues.

5.2 Configuration Management Plan

1. All work products will be stored in a centralized GIT repository.
2. The naming convention for documents will be: XXX.suffix where XXX is the name of the document, and ‘suffix’ is the standard/normal suffix for the document type. For Example, the second version of the requirements document created as a Microsoft word document might be labeled: REQ-002.doc.
3. All project (work products) items (documents, source code, test cases, program data, test data, etc) will be stored in the GIT repository but not all will be under change control (subject to formal change control procedures.) Only the system requirements, project plan and source code will be baselined and under configuration control.
4. Items that are subject to change control will be considered baselined after a group review at the end of the life cycle phase during which they are created. Baselined here means that the product has undergone a formal review and can only be changed through the prescribed change control procedures.
5. The change control procedure once a product is laselined is: (1) anyone wanting to make a chance to a baselined item sends an email to the rest of the group describing the change, reason for the chance, expected impact, and timeline for integrating the change. (2) if no one responds to the group within 3 days with a reason for why the change request shouldn’t be permitted, it will be considered accepted and the person proposing the change may proceed with the change. If anyone does object to the change, the reason for objecting will be discussed at a meeting where everyone is invited to attend and voice their opinion. At the end of the meeting at democratic vote will be held to decide whether or not the change should be allowed.

6. Including a change history with all documents is encouraged but only required for baselined documents. The change history should be at the front of the work item and include: (1) the name of the person making the change, (2) brief description of what has changed, (3) reason for the change, and (4) the date the change was integrated.

5.3 Verification and Validation Plan

Within the team, there are many actions that can be taken to ensure that risks and problems are minimized and that the quality of the project does not suffer. Communication is a #1 priority and is necessary to keep everyone informed and on the same page. Checking in with one another regularly will help keep track of our current progress and ensure an overall understanding.

5.4 Product Acceptance Plan

We are developing a technical solution for a main corporate location and 5 satellite locations. Although no budget is specified, providing a technical solution that meets Monstrosity Inc. requirements while keeping the budget as low as possible would be great. We can think of our acceptance criteria as the overall satisfaction of the client. We aim to provide quality equipment choices along with the proper use of said equipment. After proper implementation and integration, we can expect some support related communication with Monstrosity Inc. There will be proper documentation provided for many specific tasks and procedures, but some other unforeseen difficulties may arise.