**TECHNICAL ARCHITECTURE**

**[Monstrosity Inc.]**

**[BIT Project: Real Estate]**

|  |  |
| --- | --- |
| VERSION: [Version 1.0] | REVISION DATE: 4/4/2020 |

Approval of the Technical Architecture indicates an understanding of the purpose and content described in this deliverable. By signing this deliverable, each individual agrees with the content contained in this deliverable.

|  |  |  |  |
| --- | --- | --- | --- |
| **Approver Name** | **Title** | **Signature** | **Date** |
| Zach Foss | Project Manager | Zach Foss | 4/20/20 |
| Tyler DeWitt | Developer | Tyler DeWitt | 4/20/20 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Contents**

[**Section 1 DOCUMENT SCOPE 3**](#_30j0zll)

[**Section 2 OVERALL TECHNICAL ARCHITECTURE 3**](#_1fob9te)

[2.1 System Architecture Context Diagram 3](#_3znysh7)

[2.2](#_2et92p0) System Architecture Model 3

[2.2.1 Overall Architectural Considerations](#_tyjcwt) 4

[2.3 System Architecture Component Definitions 4](#_3dy6vkm)

[2.3.1](#_1t3h5sf) System Architecture Component A 4

[**Section 3 SYSTEM ARCHITECTURE DESIGN 5**](#_2s8eyo1)

[3.1 System Architecture Component A 5](#_17dp8vu)

[3.1.1 Component Functions 5](#_3rdcrjn)

[3.1.2 Technical Considerations](#_26in1rg) 6

[3.1.3 Selected Product(s)](#_lnxbz9) 6

[3.1.4 Selection Rationale](#_35nkun2) 6

[3.1.5 Architecture Risks](#_1ksv4uv) 6

[**Section 4 System Construction Environment**](#_2jxsxqh) 6

[4.1 Development Environment](#_z337ya) 6

[*4.1.1* Developer Workstation Configuration](#_3j2qqm3) 6

[*4.1.2* Supporting Development Infrastructure Configuration](#_1y810tw) 7

[*4.2* QA Environment](#_4i7ojhp) 7

[*4.2.1* QA Workstation Configuration](#_2xcytpi) 7

[*4.2.2* Supporting QA Infrastructure Configuration](#_1ci93xb) 7

[*4.3* Acceptance Environment](#_3whwml4) 7

[*4.3.1* Acceptance Workstation Configuration](#_2bn6wsx) 7

[*4.3.2* Supporting Acceptance Infrastructure Configuration](#_qsh70q) 8

# Section 1: DOCUMENT SCOPE

This document describes the Technical Architecture of the networking system for Monstrosity Inc that will satisfy business requirements as documented in the Requirements Document, 3/1/2020, and that implements the functionality and satisfies technical, operational and transitional requirements described in the Project Plan, 3/8/2020.

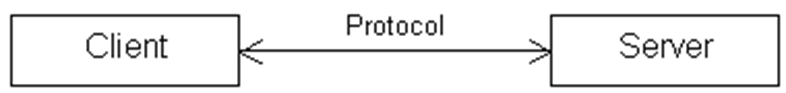
The goal of this Technical Architecture is to define the technologies, products, and techniques necessary to develop and support the system, and to ensure that the system components are compatible and comply with the enterprise-wide standards and direction defined by Monstrosity Inc..

This document will also:

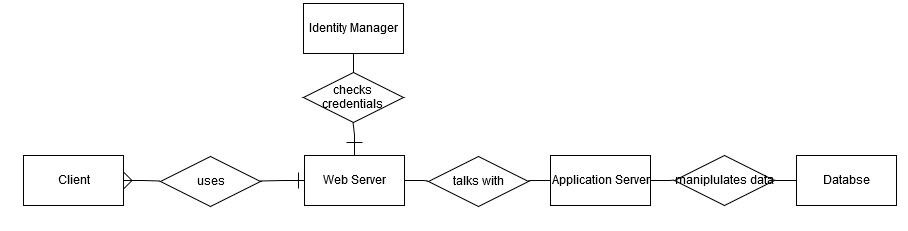
* Identify and explain the risks inherent in this Technical Architecture;
* Define baseline sizing, archiving and performance requirements;
* Identify the hardware and software specifications for the Development, Testing, QA and Production environments;
* Define procedures for both data and code migration among the environments.

# Section 2: OVERALL TECHNICAL ARCHITECTURE

## 2.1 System Architecture Context Diagram



## System Architecture Model



### 

### 2.2.1 Overall Architectural Considerations

*The* ***Overall Architectural Considerations*** *section defines how additional technical requirements have been addressed by the architecture. Representative items in this section may include:*

* *Security Strategy*
  + Web Filtering, Virus Protection, Intrusion Prevention, Secure Socket Layers (Firewalls Fortigate, FireEye, Inky)
* *Performance requirements*
  + Internet Performance must be high, computers must be able to run databases, internet must be able to handle the traffic. (Azure, AP’s, Switches, Network)
* *Accessibility*
  + We want everything to be accessible for the employees, while limiting what guest can see (Firewalls Fortigate)
* *Database sizing*
  + Database sizing must be able to be expandable if needed. (Azure, MySQL)
* *Concurrent user* 
  + Must be able to allow the traffic on the network and allow everyone to work and not get a lack of experience. (BlueBird, other network providers)
* *Data import and export*
  + We want to make sure the employess can import the data safely and quickly while being able to do the same in exporting. (Azure)
* *Data encryption and decryption*
  + To make sure everything is secure, we need to be able to securely encrypt and decrypt the data. (Azure, Firewalls FortiGate)
* *Disaster recovery*
  + Cloud Services, Back-Ups (Azure)

## 2.3 System Architecture Component Definitions

### System Architecture Component A

The **Architecture Component Definitions** section provides narrative describing and explaining each architecture component in the System Architecture Model, and identifies specific elements that comprise that component in this system. The following are examples of architecture components and elements:

|  |  |
| --- | --- |
| **Architecture Component** | **Component Elements** |
| Database Server | Server Hardware Configuration  Server Operating System  DBMS |
| Client Application | Development Tool  Online Help Tool  Client Characteristics |
| Web Server | Server Operating System |
| Identity Manager | Credential Checking |
| Application Server | Server Operating System |

# 

# Section 3: SYSTEM ARCHITECTURE DESIGN

*The* ***System Architecture Design*** *section provides detailed descriptions of each product implementing architecture components, and explains the rationale for product selection.*

## 3.1 System Architecture Component A

*For each* ***System Architecture Component*** *(identified in Section 2.3 above), the narrative describes specific* ***Component Functions****, requirements and other* ***Technical Considerations*** *that were used in the decision-making process, as well as any specific* ***Products*** *selected to implement this component. The* ***Selection Rationale*** *identifies any other products that may have been considered, and provides rationale for the decision.* ***Architecture Risks*** *identifies any potential risks associated with the architecture element.*

### 3.1.1 Component Functions

1. Firewall
   1. Fortigate 100E
   2. Fortigate 60E
      1. Functions of the Fortigates is to protect the company from external forces and keep our network secure. Providing the company with the security capabilities such as intrusion prevention system (IPS), web filtering, secure sockets layer (SSL) inspection, and automated threat protection.
2. Acces Ports
   1. MR42
   2. MR33
      1. These will allow us to broadcast our WiFi or Network in the buildings to allow everyone to connect to the internet, unless they are hardlined in.
3. Switches
   1. MS225-24
   2. MS225-48
      1. These two will either have 24 ports or 48 ports for providing seamless network service that is high-performance. These switches combine the benefits of cloud-based centralized management with a powerful, reliable access platform. With cloud management, thousands of switchports can be configured and monitored instantly, over the web.
4. Hosting
   1. Microsoft Azure
      1. This is what Monstrosity Inc. will be using for the Cloud Computing, which will allow us to store any imformation we need, and works with the database allowing us to do everything we need to keep everything safe.
5. Network
   1. BlueBird
      1. This will be the network we will use for our hub here in Kansas City, while chosing other options that best suit us in our other locations to best support what we need.
6. Database
   1. MySQL
      1. We chose to go with MySQL becuase it works hand and hand with Microsoft Azure and seems to be the best fit for the company.
7. Email Threat Prevention
   1. FireEye
   2. Inky
      1. Both of these will allow us to maintain secure functionality within our systems that we use. We will be able to block emails, IP address, and domains or even whitelist if we need to do that.
8. VPN
   1. FortiGate
      1. The forigate will allow the employess work from home and act as if they are in the office giving them secure connection.

### 3.1.2 Technical Considerations

1. Amazon AWS
2. EnGenius Switches
3. NordVPN
4. Oracle Database
5. EnGenius Access Ports
6. Cisco Firewalls

### 3.1.3 Selected Product(s)

1. FortiGate Firewall
2. Microsoft Azure
3. FireEye, Inky
4. FortiGate VPN
5. Meraki Switches & Access Ports
6. MySQL Database

### 3.1.4 Selection Rationale

1. The reasons for choosing these, from doing our research they seemed to fit our company the best, while being easy to use and seeming to work together the easiest. The ease of use for the users and IT team is another reason for using these products. Working with these before made it an easy choice as well and really enjoying the ease, we figured they would be good to use.

### 3.1.5 Architecture Risks

1. Possible architecture risks could include employees having emails get through that aren’t supposed to and getting their information taken. Some other architecture risk could be that the VPN tunnel goes down and employees working from cannot connect to the VPN. If our network goes down and people can’t work in the office, this could cause a chain of events if our database isn’t backed up properly then we could lose information if the network goes down that we can’t get back.

# Section 4: System Construction Environment

*The* ***System Construction Environment*** *section details the various environments necessary to enable system construction and testing.*

## 4.1 Development Environment

### *4.1.1* Developer Workstation Configuration

1. The Developers will have the same set up as the employees, while having more access to the database, the network, the switches, access ports, firewall and email threat prevention.

### 

### *4.1.2* Supporting Development Infrastructure Configuration

1. Development Hardware
   1. 13” Dell Latitude Laptop
   2. Dell Monitors x2
   3. Dell Docking Station
   4. Cell Phone
   5. Windows 10
   6. Office 365 E1, E3
   7. VPN
   8. Database Access
   9. Admin Privileges

## *4.2* QA Environment

1. We want to make sure we are giving out customers the best quality. So with that we must be able to protect our data, and prevent defects, and mistakes. The best way we are going to do that is to make sure the information and data is secure, and stored correctly while having the necessary backups in Azure, just in case something does happen.

### *4.2.1* QA Workstation Configuration

1. The Quality Assurance workstation will be the same as the developers, in case there will need to need to be changes made. The workstation needs to do the same thing that way they can monitor and have the correct permissions.

### *4.2.2* Supporting QA Infrastructure Configuration

1. QA Workstation Hardware
   1. 13” Dell Latitude Laptop
   2. Dell Monitors x2
   3. Dell Docking Station
   4. Cell Phone
   5. Windows 10
   6. Office 365 E1, E3
   7. VPN
   8. Database Access
   9. Admin Privileges

## *4.3* Acceptance Environment

*For each environment necessary for system construction (****Development, QA*** *and* ***Acceptance****), provide detailed specifications for the* ***Workstation*** *and* ***Supporting Infrastructure*** *that will be used (including hardware, network and operating system requirements, all necessary installed packages and tools, and needed directory structures**that will be utilized to store all construction components).*

### *4.3.1* Acceptance Workstation Configuration

1. For the workstations of all the employees, since they are in real estate they will each have a Dell Latitude 13” for easy travel. While in the office they will have Dell Monitors and a docking station to connect to the monitors. Each person will have a company phone since they will be talking to so many clients while each phone will be equipt to have hotspot.

### *4.3.2* Supporting Acceptance Infrastructure Configuration

1. Employees Hardware
   1. 13” Dell Latitude Laptop
   2. Dell Monitors x2
   3. Dell Docking Station
   4. Cell Phone
   5. Windows 10
   6. Office 365 E1, E3
   7. VPN
   8. Database Access
2. Office Components
   1. Switches
   2. Access Ports
   3. Firewalls
   4. Internet
   5. Azure