Architecture Requirements Specification

For

Monstrosity Network

2/24/2020

ver. 1.0

Prepared by:

Ryan Shepherd, Andrew Taylor, Liam Floyd.

**Table of Contents**

[**REVISION HISTORY**](#_heading=h.32hioqz) 4

[**1**](#_heading=h.1hmsyys) **INTRODUCTION 5**

[**1.1**](#_heading=h.41mghml) **Overview 5**

[**1.2**](#_heading=h.2grqrue) **Goals and Objectives 5**

[**1.3**](#_heading=h.vx1227) **Scope 5**

[**1.4**](#_heading=h.3fwokq0) **Definitions 6**

[**1.5**](#_heading=h.1v1yuxt) **Document Conventions 7**

[**1.6**](#_heading=h.4f1mdlm) **Assumptions 7**

[**2**](#_heading=h.2u6wntf) **GENERAL DESIGN CONSTRAINTS 7**

[**2.1**](#_heading=h.19c6y18) **Product Environment 7**

[**2.2**](#_heading=h.3tbugp1) **User Characteristics 8**

[**2.3**](#_heading=h.28h4qwu) **Mandated Constraints 9**

[**2.4**](#_heading=h.nmf14n) **Potential System Evolution 9**

[**3**](#_heading=h.37m2jsg) **NONFUNCTIONAL REQUIREMENTS 9**

[**3.1**](#_heading=h.1mrcu09) **Usability Requirements 10**

[**3.2**](#_heading=h.44sinio) **Operational Requirements 10**

[**3.3**](#_heading=h.46r0co2) **Performance Requirements 11**

[**3.4**](#_heading=h.2lwamvv) **Security Requirements 11**

[**3.5**](#_heading=h.111kx3o) **Safety Requirements 11**

[**3.6**](#_heading=h.3l18frh) **Legal Requirements 12**

[**3.7**](#_heading=h.206ipza) **Other Quality Attributes 12**

[**3.8**](#_heading=h.4k668n3) **Documentation and Training 12**

[**3.9**](#_heading=h.2zbgiuw) **External Interface 12**

[**3.9.1 User Interface 1**](#_heading=h.1egqt2p)**3**

[**3.9.2 Software Interface 1**](#_heading=h.3ygebqi)**3**

[**4**](#_heading=h.2dlolyb) **SYSTEM FEATURES 13**

[**4.1**](#_heading=h.sqyw64) **Feature: Wireless Network 13**

[**4.1.1 Description and Priority 1**](#_heading=h.3cqmetx)**3**

**4.1.2.1 Use Case: Internet Connection for Employees 14**

[**4.1.2.2 Use Case:**](#_heading=h.1rvwp1q) **Internet Connection for Customers 15**

[**4.1.3 Additional Requirements 1**](#_heading=h.4bvk7pj)**5**

[**4.2**](#_heading=h.2r0uhxc) **Feature: Cloud Hosted Services 16**

[**4.2.1 Description and Priority**](#_heading=h.1664s55) **16**

[**4.2.2 Use Case:**](#_heading=h.3q5sasy)  **Redundancy and Support 16**

[**4.2.3 Additional Requirements**](#_heading=h.25b2l0r) **17**

[**4.3 Feature: Database System**](#_heading=h.2r0uhxc) **17**

[**4.3.1 Description and Priority**](#_heading=h.1664s55) **18**

[**4.3.2 Use Case:**](#_heading=h.3q5sasy)**Data Storage and Query 18**

[**4.3.3 Additional Requirements**](#_heading=h.25b2l0r) **19**

[**4.4 Feature: Security**](#_heading=h.2r0uhxc) **19**

[**4.4.1 Description and Priority**](#_heading=h.1664s55) **19**

[**4.4.2 Use Case:**](#_heading=h.3q5sasy) **Proper Security and Access Control 20**

[**4.4.3 Additional Requirements**](#_heading=h.25b2l0r) **20**

**5****OPTIONAL FEATURES 20**

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Name** | **Description** |
| 1.0 | 4/28/2020 | RS, AT, LF | Baseline Requirements Specification |
|  |  |  |  |

# **Introduction**

## 1.1 ***Overview***

This document outlines the requirements that will need to be implemented in the design of the information technology infrastructure for Monstrosity Inc., its employees and customers. The purpose of this document is to present the needs that this infrastructure shall satisfy in an understandable way so that the affected stakeholders can verify its accuracy and architects can refer to this document when making design decisions. This document will focus primarily on the hardware implementation of this system.

Monstrosity Inc. has contracted with our firm to design an infrastructure package that will provide high speed wireless internet connectivity, access to apps such as secure email, and a database system to manage the real estate companies information. This system will be used by approximately 200 employees of Monstrosity Inc. as well as its customers and will have to be implemented in 5 satellite offices and 1 corporate office.

This document doesn’t address *project* issues such as schedule, cost, development methods, development phases, deliverables and testing procedures. Those are addressed in a separate project document and quality assurance test plan. Additionally, this document does not address detailed user interface implementation which would be accomplished at the software level.

## 1.2 ***Goals and Objectives***

Our goals and objectives are to research, design, and propose the infrastructural solution to the technical needs of Monstrosity Inc which includes:

1. secure network with intrusion detection, as well as wireless internet services for employees and customers,
2. cloud services hosting for secure email,
3. onsite database hosting infrastructure.

We will complete this over the course of 5 planning and design iterations that will end with the final proposal being presented by May 4, 2020.

## 1.3 ***Scope***

The Monstrosity Inc network setup will provide secure corporate network access for one corporate office and five satellite offices. In addition to employee access, customers will be able to access a guest wifi with no access to corporate file share, resources, etc. The infrastructure will also cover cloud hosted company applications, such as email. On-prem database hosting will also be outlined along with considerations for security parameters such as web filtering, intrusion detection, and secure access for corporate users. These features will be outlined and detailed for implementation, however no actual financing, front-end (user interface) software development, database build-out, physical infrastructure construction, or key business decisions will be made.

## 1.4 ***Definitions***

This section defines potentially unfamiliar or ambiguous words, acronyms and abbreviations.

**On-Prem** - “on premises”, infrastructure that is on-prem will be hosted physically on site at the physical location opposed to hosted in the cloud through a third party provider.

**TBD** - To be determined. When used in this document, this refers to material facts or decisions that will need to be made at a later date and will be added to this document as an addendum.

**Use case** – describes a goal-oriented interaction between the system and an actor. A use case may define several variants called scenarios that result in different paths through the use case and usually different outcomes.

**Actor** – user or other system that receives value from a use case.

**Product** – what is being described here; the system specified in this document.

**Project** – activities that will lead to the production of the product described here. Project issues are described in a separate project plan.

**Shall** – adverb used to indicate importance; indicates the requirement is mandatory. “Must” and “will” are synonyms for “shall”.

**Should** – adverb used to indicate importance; indicates the requirement is desired but not mandatory.

**May** – adverb used to indicate an option. For example, “The system may be taken offline for up to one hour every evening for maintenance.” Not used to express a requirement, but rather to specifically allow an option.

**ISP** - Internet service provider, a third party company that will provide the infrastructure needed to access and utilize internet capabilities

**IT Professional** - It is assumed that Monstrosity INC will not have a full time IT manager on staff to maintain the system and that this will be contracted out to a third party who will be on-call.

**Cloud Service Provider** - A third party provider who maintains and manages their own data center who provides cloud services to the public

**Network** - refers to the physical infrastructure of a group of two or more computer systems linked together. There are many types of computer networks, including Local Area Networks (LAN), Wireless Internet (wifi), and Wide Area Networks (WAN).

**SLA** - Service Level Agreement. A service-level agreement is a commitment between a service provider and a client. Particular aspects of the service – quality, availability, responsibilities – are agreed between the service provider and the service user. As used in this document, SLA’s refer to agreements between the cloud service provider and Monstrosity Inc.

**UI** - User interface. Any number of front-end software that will allow the users to interact with the system.

## 1.5 ***Document Conventions***

Portions of this document that are incomplete will be marked with TBD. Each TBD item will have an addendum added to this document once material facts are uncovered that result in changes or additions to this document at a later time.

## 1.6 ***Assumptions***

* It is assumed that Monstrosity Inc is a local real estate company with all offices residing in the same state, managing several properties that are for sale to the public and businesses.
* Monstrosity Inc is being considered a small to medium sized business.
* It is assumed that Monstrosity has a limited budget, characteristic of a small/medium real estate company. For example they may look more to hosted services instead of building extensive in house applications and on-prem infrastructure..
* It is assumed that this project will be treated as a simulation of the “real-world”, making decisions based on considerations of likely consequences in a practical implementation.
* Due to the technical nature of physical infrastructure (hardware configurations), the average user (customers, managers, employees) will not be able to manage this system should problems arise and that Monstrosity Inc will likely need to contract with a third party IT support professional who will be on-call to provide maintenance and assistance with operations.

# 2. **General Design Constraints**

## 2.1 ***Product Environment***

Monstrosity Inc. is a real estate company that operates 6 offices throughout the state. Each site will have its own wireless internet network. These networks will require an ISP to provide the internet backbone that will allow connectivity to the internet, cloud hosting service provider, as well as to connect each site to the database system being hosted at the corporate office. This infrastructure will also require electricity to operate and will therefore need to be connected to each office's power infrastructure. End-user hosts at each site will operate on their own operating systems (Windows, iOS, Android, Oracle, etc) which will handle the front-end connectivity to the system including system login, network interface handling, internet/network resources navigation, manipulation of database information, etc. User authentication and other front-end considerations will also take place at the end-user host level. Security and TCP/IP protocols, which have been widely established within the IT industry, will be utilized and implemented within the system to allow for interoperability with IT systems extending beyond the systems at Monstrosity Inc..

Note the user interface, which characterizes an interface between the system and its environment, is described below in its requirements, but does not go into detail about its implementation, which is beyond the scope of this project.

## 2.2 ***User Characteristics***

For this project, we will have three main actors involved. Each actor will have a different level of control over the system and be allowed different privileges.

1. customers - Priority Low
   1. customers are people who will be in the offices that are seeking to purchase home through the realtors at Monstrocity and wish to get on the internet for various uses.
   2. can access a guest wifi network that is seperate from the main network
   3. will be able to access the internet and surf the web
   4. customers are the general public and will have varying technical experience in navigating the internet from the novice to very experienced
2. employees - Priority High
   1. will have access to wifi that grants different permissions
   2. website monitoring is desired by corporate office to protect the nature of secure data but also to maintain productivity of employees
   3. can access database read and query access
   4. can alter tables in the database
   5. will have access to secure email hosted by the selected cloud service provider
   6. employees will consist of managers and real estate agents.
   7. employees will have varying experience in using the IT systems and some will require training in how to use the system to complete their tasks
   8. Managers will need to be very fluent in the systems as they will be required to help the more novice users in navigating system resources
3. IT professionals managing the system - Priority High
   1. will have access to the database servers for maintenance
   2. will have access to the network for maintenance

The end product will be used by many different people in many different ways. The network and database physical infrastructure will need to be maintained by an IT professional. The secured emails will be used by all Monstrosity Inc. employees, so they need to be able to be used by inexperienced users. The wifi will be used by all workers as well as customers, so we need the wifi to be easily accessible to those inside of the various buildings. The highest priority users would be the workers because they need to be able to access all the information easily in order to do their job and keep the business running. The next highest priority users, which it could be argued that they are at the same priority level as the workers, is the IT professional because they will be protecting and maintaining all of the systems to make sure they all run as smoothly as possible. The lowest priority user would be the customer because they are just accessing the wifi and do not actually require it.

## 2.3 ***Mandated Constraints***

* We are designing a network layout for a purely hypothetical company with no actual finances, existing infrastructure, or offices.
* With no offices we must rely heavily on assumptions developed by the team.
* We are also operating as a group for a school project, giving limited time with schedules involving work, other courses, and more.
* Operating with no defined financial constraints of the infrastructure. In general, we will try to keep the costs to a minimum as to what we feel would be logical costs/budget constraints of a business of this size.
* As students, we have limited experience and knowledge in applying architectural design and will require research to complete this project. All variables that would affect a real-world design such as this may not be considered due to inexperience.
* As a hypothetical company with no ability for physical implementation, testing designs is limited.
* The database system will be based on MySQL.
* The system will need to be accessible from a variety of devices (desktops, laptops, tablets, phones, etc) that run on various operating systems (Windows, Mac, Android, etc).
* Due to the technical nature of physical infrastructure (hardware configurations), the average user (customers, managers, employees) will not be able to manage this system should problems arise.

## 2.4 ***Potential System Evolution***

Potential considerations will be taken into account to allow for extensibility in the future. Such expansions could include Monstrosity Inc. wanting to develop a mobile app for their services, which will need to be hosted. Additionally, the company may wish to take advantage of additional services that the cloud provider may have available in the future. The wireless internet network will need to evolve as the business grows, which includes increases in bandwidth needs, allowing for additional concurrent users on the system, increased data storage needs, and hardware upgrades as technology develops over time. The infrastructure will need to be adaptable should the external environment change such as changes in IT management companies, ISP providers, or other changes beyond the control of Monstrosity Inc. which might affect operability of the system. As the company grows and adds more employees (or terminates employees), user profiles will need to be able to be managed quickly so as to not cause delays in business operations.

# 3. **Nonfunctional Requirements**

Nonfunctional requirements are properties the system must have relating to quality of the system; how usable the system is, how well it operates, and performance requirements.

## 3.1 ***Usability Requirements***

The system’s components shall be easy to use. “Easy” is defined as end-users being able to complete 99% of tasks without the assistance of more skilled users such as managers or other experienced users. Additionally, ease of use will be measured by the amount of help desk tickets or calls issued to the IT professionals seeking assistance or repairs/maintenance to the system. The target for this type of contact would be less than 75 calls and/or tickets within a year. Complaints to management about the difficulty of using the system shall be promptly raised with the IT professionals with the intention to make the system easier to use or help the users understand how to use the system more efficiently. The front-end usability of the system shall be intuitive with limited “advanced” options or complicated screens to navigate so that the novice can use system resources without frustration or difficulty in knowing what to do and how to do it.

As part of usability, the system shall be reliable. Unreliable systems would not meet the expectation of being usable. The IT professional should be able to limit the amount of downtime to 0.002% of the time that employees are working without disruptions. Customers should be able to log into the wifi within 30 seconds of entering the building 99% of the time. Workers should be able to complete any task within one minute 98% of the time in order to keep things from backing up for them. 0.1% of emails that reach the employee will be spam emails.

We will not be producing the front end, however we would make sure to have this requirement fulfilled by the front end developers. add downtime constraint, and uptime requirements.

## 3.2 ***Operational Requirements***

The user environment will be a typical small office building. The on premise servers to handle locally hosted programs, the database, VPN server, etc will require a server room that is arid and cool. Temperature should be strictly regulated in the room. The power to the room should also be able to rely on an auxiliary generator in the event of a power loss. The system should operate quietly as this will be in use within an office environment and the system should not disturb the work being conducted in the office. Contracted IT support professionals to maintain the system should be available 24 hours a day, 7 days a week and should have a response time from call being initiated to IT professional to when work is started of no more than 12 hours while work completion should be less than 24 hours on average. Any hardware will need to be out of sight, hidden behind doors, ceiling tiles, walls, etc so as to not be a visual distraction or appear unprofessional. The system will need to be logically organized, for example cabling being bundled and appropriately labeled, and server racks being kept organized and with a “clean” appearance.

## 3.3 ***Performance Requirements***

The network should be able to maintain consistent internet connectivity meeting a target of 99.998% uptime reliability. Any downtime for updates, upgrades, and repairs would need to be scheduled during times the offices are closed to minimize impact on business operations. Scheduled downtime would need to be effectively communicated to employees and customers. Cloud hosted applications should maintain uptime targets of 99.998%. Database systems should maintain 99.99% uptime reliability. Response time targets of .1-.5 seconds on average from the point where the host initiated the request to when the response received at the host should be maintained 99.9% of requests of resources. Data integrity and data recovery systems should have a 99.999% reliability with no more than 1 hours difference in current data and the data that is stored in data recovery/backup storage. The system will need to be able to accommodate increased workloads during peak times of business operations as determined by usage history and should be adaptable to accommodate unexpected increases in system demands. The system will need to be able to handle concurrent users each needing equal, reliable, and speedy access to system resources. At most, the system will need to be able to accomodate 250-300 concurrent users if all employees and a large number of customers were all using resources at the same time. This is an extreme case if the system were at maximum utilization. A minimum target for concurrent users with equal access to resources without degradation of user experience would be approximately 200 users. SLA’s with the contracted cloud hosting provider and ISP would need to closely mirror these targets. The database should be able to maintain an active-active data accessibility through the cluster so as to avoid data conflicts.

Employees will be able to login to the system within a minute of turning on their client machines 99% of the time. Employees should be able to receive an email within 30 seconds of it being sent and the recipient should receive an email within a minute of the employee sending it 99% of the time.

## 3.4 ***Security Requirements***

No one shall have access to the server room except for the contracted IT professionals. IT professionals and trained managers may have access to elements of the network should routers need to be rebooted from time to time. Email services will be secured with spam and phishing filters to avoid having workers accidentally click on a contaminated link, and virus detectors to prevent malicious code from infecting the system. Guest wifi access will be in a secluded environment so as to not allow access to secure system resources. Network resources will require authentication, only allowing specific users to edit data, and limiting read permissions of various information to those that need it. Websites shall also be filtered to prevent customers and workers from accessing various sites that could be harmful or could cause a decrease in productivity, as well as those that are not appropriate for work. Intrusion detection infrastructure will be utilized to prevent unauthorized access to the system. The system will keep logs of activity that takes place on the network and its resources, which will be stored for a period of time established by business protocols TBD by management.

## 3.5 ***Safety Requirements***

There is a potential for electrical fires with the server hardware, thus proper fire containment measurements and procedures for the building are important. The wifi could cause possible radio interference with the surrounding environment. The electrical system would need to follow standardized safety protocols including but not limited to proper shielding of cables and wiring, grounded outlets, circuit breakers, use of power distribution units, etc.

## 3.6 ***Legal Requirements***

System resources will need to maintain licensure and adhere to end-user agreements in order to be legally operated. These licenses include the MySQL operating system of the database, Windows operating systems, and any firmwares or software requirements of the hardware. Any data stored and expressly used by Monstrosity Inc will need to adhere to copyright protections. Customers, when logging onto the guest wifi, will need to agree to an end-user agreement to access the wifi network. In order to use system resources, employees will need to agree to company legal requirements governing the use of the system and any needs for confidentiality. There will be a legal duty to maintain confidential and secure data about customers including but not limited to bank account information, personally identifiable information, etc. Wifi and the network will need to adhere to government regulations, for example commercial use of radio frequencies. Web filtering will need to be implemented so as to protect the company from liability of how users will use the internet.

## 3.7 ***Other Quality Attributes***

The server will have a backup power source that will grant enough time, should the power go out, for the system to save everything that is occuring, preventing data loss. Backups of the database will be made by automated processes. The data stored in the cloud will be backed up as well.. The company providing the cloud hosting service will be easily reachable for help with their services. The IT staff members will be easily reachable, and they will take turns being available overnight should a problem arise that needs their attention.

## 3.8 ***Documentation and Training***

For IT staff to manage, most applications will be third party, thus have their own documentation. The structure of the network, security protocols, firewall configuration and spam/filter configuration should all be documented for the IT staff to effectively respond to issues and rectify them. The database and hosted website will require documentation on structure by the software engineers so that developers can properly construct queries and maintain integrity of the data.

Company documentation for users to connect to the network, connect to VPN, and access file share would be needed to mitigate IT help desk tickets. Users would also need to be trained on best practices in regards to cyber security to reduce likelihood of employees accidentally leaking data or credentials.

## 3.9 ***External Interface***

The infrastructure being designed for Monstrosity Inc will require some front-end interface in order to gain access to the system and to utilize the company resources residing within the system. This architecture design will not go into the details of front-end user interface implementation at the software level, but will give requirements that will require consideration in order to make the hardware infrastructure usable at end-user level. Please note, this is not an exhaustive list.

### 3.9.1 **User Interface**

For this project we are not detailing the specifics of the user interface design and implementation. We would pass that on to front end designers, however we would have some design requirements for them. Many user interface functions will take place at the operating system level and will not require custom software. The operating system will also manage back-end functionality such as TCP/IP and security protocols and displaying of relevant data on the monitor/screen. There will be several different user interfaces that users will interact with. Employees will have a login page to connect to system resources, a UI that allows them to navigate the database, and a UI or email client for email access. The UI should allow customers to be able to login to the guest wifi and agree to user-agreement/terms of service. The database interface should allow you to read, enter, and alter data. Additionally, the UI shall need to be able to query the database based on specified criteria and return results in an easy to read format that can be printed and given to the customer. There should be a corporate intranet that will allow employees to navigate resources and to find policies and procedures. Email will be accessible through an email client such as MS Outlook or similar, which will handle the management of email functionality.

### 3.9.2 **Software Interface**

For cloud hosted applications Monstrosity Inc's web development would use application provider's APIs to integrate data and functionality to the website, such as a single sign on. Employees will be likely using Windows 10 Professional thus using it's built in VPN connection tools (with the connection being preconfigured for them by IT) to connect to the VPN. The website will need to make queries to the database and handle them properly to avoid any injection from malicious actors.

# 4. **System Features**

The core requirements of the system are listed in this section. Features are system behaviors from the user’s point-of-view. The requirements of a feature are described by one or more use cases plus any additional narration that is necessary

## 4.1 ***Feature:*** Wireless Network

### 4.1.1 **Description and Priority**

Monstrosity Inc. will need to have internet networks setup for each of their satellite offices as well as for their corporate office. This network will be utilized by all of the employees, and the customers. The network will require 2 different SSIDs (open guest and secure employee); two for each of the buildings preventing the customers from being able to have access to the main network. This will also allow the customers and employees to have separate firewalls and web filtering blocking different sites.

Cost: medium

Priority: high

Risk: medium

Value: high

### 4.1.2.1 **Use Case:** Internet Connection for Employees

***Actors: Employees***

* As an employee I want to be able to use my tablet and laptop to show the customers our real estate listings.
* As an employee I want to be able to use the wifi to compare our listings to the listings of our competitors to better prepare myself for customer questions.
* As an employee, I want to be able to connect to the network infrastructure so that I can use system resources including but not limited to the database and email services

Basic path:

1. User clicks on internet icon of laptop or phone
2. System displays two SSIDs
3. User selects SSID for employees
4. System requests username and password
5. User correctly enters employee username and password
6. System notifies user that they are now connected
7. The employee is now connected to the network
8. User clicks on internet icon of laptop or phone
9. User selects current network
10. System asks is user wants to disconnect
11. User selects yes
12. System disconnects user
13. User is no longer connected to the system

Alternate path:

1. User clicks on internet icon of laptop or phone
2. System displays two SSIDs
3. User selects SSID for employees
4. System requests username and password
5. User incorrectly enters employee username and password
6. System notifies user that they are not connected
7. The employee either re-enters credentials or stops trying

### 4.1.2.2 Use Case: Internet Connection for Customers

***Actors: Customers***

* As a customer I want to be able to access the wifi to compare the houses listed by Monstrosity Inc. with other listings.
* As a customer I want to be able to access the wifi so that I am not bored while I wait for my parents.

Basic path:

1. User clicks on internet icon of laptop or phone
2. System displays two SSIDs
3. User selects SSID for customers’ guest network
4. System requests username and password
5. User correctly enters customer password
6. User will be prompted to go to a web page that will display a end user agreement that they will need to accept in order to continue using the resource
7. System notifies user that they are now connected
8. The customer is now connected to internet
9. When user wishes to disconnect, user clicks on internet icon of laptop or phone
10. User selects current network
11. System asks is user wants to disconnect
12. User selects yes
13. System disconnects user
14. User is no longer connected to the system

Alternate path:

1. User clicks on internet icon of laptop or phone
2. System displays two SSIDs
3. User selects SSID for customers’ guest network
4. System requests username and password
5. User incorrectly enters customer password
6. User will be prompted to go to a web page that will display a end user agreement that they will need to accept in order to continue using the resource
7. System notifies user that they are not connected
8. The customer either re-enters password or stops trying

### 4.1.3 **Additional Requirements**

Employees and customers will login to two different SSIDs separating customers from the main network, protecting it from attacks, unauthorized access to system resources, and giving different website restrictions.

## 4.2 Feature: Cloud Hosting

### 4.2.1 Description and Priority

To reduce strain on internal servers, internal maintenance and risk of failure, catastrophe, or else hosting applications in the cloud through third party providers will be used for Monstrosity Inc. This also frees up use of local server resources. This will likely include services such as Exchange Online through Office 365 to help manage user software and email needs. To help manage users, Azure, AWS, or Google Cloud could be used on its own or in a hybrid environment with a local active directory server to provide redundancy and local level control. The use of cloud hosting alleviates strain on IT staff in terms of troubleshooting, as providers generally offer support for hosted apps. Most providers generally have multiple backup locations for redundancy. As a new network and system this will not require any migration. The requirements would be deciding optimal providers, financial and registering. For a hybrid environment, configuration will need to be done locally to merge the two.

Cost: medium-high

Priority: medium

Risk: low

Value: high

Primary and alternate paths for front-end operation is TBD as this would be implemented at the software design level instead of hardware function.

### 4.2.2 Use Case: Redundancy and Support

***Actors: Employees, IT Staff, Customers***

* As an employee I should be able to log into a single sign on between my computer and online resources such as Microsoft
* As an employee with access to my sign on and email I should then be able to access Microsoft office suite programs
* As an employee I should be able to view other employees I'm a global address book
* As an employee I should be able to send emails to other employees and internal email groups
* As an employee I should be able to send emails to external users and email groups
* As IT staff I should be able to reach out to the provider if there is an unexplained issue to resolve
* As IT staff use of cloud hosting should make our local server hosting more manageable
* As IT staff I should have adequate tools to administer users and setup across cloud hosted apps to reflect the standards of Monstrosity Inc
* As IT staff customers should not have to seek my help to get technical assistance with a cloud hosted application
* As IT staff if our local office experiences an outage then our cloud hosted apps should still be serving customers and employees
* As a customer I should be able to successfully email an employee
* As a customer if I am having technical difficulties then I should be able to get support for the providers tech support

### 4.2.3 Additional Requirements

* Backups for critical services will need to be in place in the event the provider is experiencing an outage
* Proper local configuration will need to be in place for a hybrid environment or for good flow between local and remote services
* Staff will need to be trained on use of newer hosted administration tools
* Security will have to allow for communication between internal services and external providers
* Records of required info for providers will have to be kept up to date in event of an audit as Microsoft occasionally does
* Proper permissions will need to be synced between local requirements and hosted applications
* With the use of third party hosted external apps, customers should be able to access the app in their own role
* With the use of third party hosted external apps, customers should be able to seek technical support from the provider support rather than internal IT staff

## 4.3 Feature: Database System

### 4.3.1 Description and Priority

Monstrosity Inc. has a database product that will require hosting. The purpose of this database is to store, maintain, and query information about the real estate properties that the company manages and sell through its realtors. This database will also store other company information relating to Human Resources, system authentication, user logs, and other information related to business operations. The database will require the database itself which will utilize MySQL architecture, but will also require the hardware to host and run services that will access the database. This will include a server cluster with 2 servers to provide redundancy and failover reliability, RAID storage to protect data against failures and data corruption, data backup, and cluster control systems. The cluster will need to operate in an active-active configuration to allow for data integrity and data accuracy when being accessed across many concurrent users.

Current requirements are to have the physical database infrastructure to be hosted on-prem. However, cost-benefit analysis (TBD) should be considered to determine if a cloud hosted database system would provide advantage over being on-prem. Also, considerations to the design of such infrastructure will take into consideration the size of Monstrosity Inc and potential concurrent user workloads when in peak usage. This means that the infrastructure will be limited and cost efficient to meet these requirements. For example, the infrastructure will be on a smaller scale than that which would be required for a large enterprise system that would be used in a large data center or for a global tech company.

Cost: High

Priority: Medium

Risk: High

Value: Medium

Primary and alternate paths for front-end operation is TBD as this would be implemented at the software design level instead of hardware function.

### 4.3.2 Use Case: Data Storage and Query

***Actors: Employees, Customers, Company Operations***

* As an employee, I will need to be able to store information about real estate properties that are on the market and available for sale so that I can present these options to customers and complete a sale.
* As an employee, I will need to be able to query the information stored within the database so that I can search for properties based on criteria the customer desires in the property so that I can give them properties that they will be interested in purchasing.
* As an employee, I will need to be able to manage the data associated with a particular property so that I can record if it has been sold or to update information associated with the property.
* As a customer, I will rely on the information in the database as being accurate so that I can make informed decisions about properties I might be interested in purchasing and not waste any time looking at properties that will not suit my needs.
* As company operations, I will store and manage information related to company operations (such as human resources, financial information, and employee/customer profiles, etc) that will make business operations more efficient.

### 4.3.3 Additional Requirements

* Information within the database will need to follow security protocols to protect the data from unauthorized access.
* The database will require authorized access permissions to allow the data to only be changed by those with permissions to do so.
* The system will need physical protections (secure entry to server room) to prevent unauthorized access.
* Cyber Security protocols will need to be implemented to safeguard against attacks.
* The system will need to maintain data availability with failover systems, backup power, and data protection measures (data recovery and data backup) to ensure reliable access to the system and its data.
* The system will require a temperature controlled room to keep the servers cool as well as fire preventative measures for safety.
* The database will need to be user-friendly so that users without technical experience will be able to use the system without difficulty or the need to contact technical support, manager, or other employees to execute normal daily use

## 4.4 Feature: Security

### 4.4.1 Description and Priority

Monstrosity Inc will require security on both a digital and physical level to keep sensitive data safe. This will require specific network setup, laying a DMZ so that external users of company hosted applications such as the website will not have easy access to internal data such as file servers or active directory with them behind a properly configured firewall. The server room should also be separated from the main employee area, and locked physically with only access to IT and other select staff. There also needs to be security measures to protect users from themselves, such as email spam and web filtering to assure they don't go falling into traps. As part of security users would also need to be educated about security risks and how to spot suspicious emails and so on.

Overall security would consist part of network architecture to create secure networks for different access to different users and hosted (either on premises or cloud) applications to help monitor the network, and manage user anti-virus. This also includes security groups and access rights assigned to employees to ensure they have and only have access to files needed for the duties of their role.

Cost: medium

Priority: high

Risk: high

Value: high

Primary and alternate paths for front-end operation is TBD as this would be implemented at the software design level instead of hardware function.

### 4.4.2 Use Case: Proper Security and Access Control

***Actors: Employees, IT Staff, Customers, Malicious Actors***

* As an employee I should be able to log onto the network and access shared files needed for my job duties
* As an employee other employees or people should not be able to log on as me or view or modify files that are tied to my account for my role and not theirs
* As an employee I should be able to identify malicious emails and websites to avoid providing unauthorized access and promptly report the offending item to IT for review
* As an employee I should be able to identify phishing attempts to avoid them, preventing unauthorized use of my network credentials or access to sensitive company info
* As IT staff employees should not be able to modify files outside the scope of their role or permissions
* As IT staff I should have access to the server room to perform the duties associated with my role for any fixes or upgrades
* As IT staff I should have access rights to internal servers to perform the duties associated with my role for any fixes or upgrades
* As a customer I should not be able to access the internal file share
* As a malicious actor I should not be able to access internal servers
* As a malicious actor I should not be able to disrupt Monstrosity Inc services

### 4.4.3 Additional Requirements

* Users will require documentation of security protocols and proper handling of company files and computers
* Users will require documentation educating them on the threat of phishing and other malicious attacks
* Users should be assigned access based on roles and groups rather than assigning an individual user access to a file or directory
* Monitoring software should be implemented to warn of any suspicious logins or behavior
* Security should be seamless to users, if it does it's job they should never encounter a need for intervention
* A bastion should be in place to aid in external cyber attacks
* A DMZ sub network should be implemented to prevent access of internal data from an internet facing external use

# 5. Optional Features

Additional features that are not expressed as being requirements would be considered as optional features.

At this time, optional features are TBD and will be added to this requirements document as addendums.