COMPANY X

Network Infrastructure Upgrade Plan

Network Improvement Team

Contents

Report Purpose *3*

Company Overview *3*

IT Governance Structure *3*

Enterprise Architecture *3*

Project Scope *5*

Physical Network *5*

Logical Network *6*

Summary of Findings and Next Steps *6*

Needs Assessment *6*

Risk Assessment *7*

Enterprise Architecture (Revised) *8*

Gap Analysis *8*

SWOT Analysis 9

Migration Planning 9

Detailed Budget *11*

Conclusion 11

1. CONTACTS *14*

1.1 IT Management Team 14

2. INTRODUCTION *14*

2.1 Plan purpose and scope 14

2.2 Risk Assessment 14

3. INCIDENT MANAGEMENT *15*

3.1 Incident flow chart 15

3.2 Fault detection 15

3.3 When to invoke the plan 16

3.4 Standard incident meeting agenda 16

4. ROLES & RESPONSIBILITIES DURING A DISRUPTIVE INCIDENT *16*

5. DISASTER RECOVERY PROCEDURES 18

5.1 Critical System 1: Network Infrastructure (FortiGate, FortiSwitch, Cisco Catalyst) 18

5.2 Critical System 2: Servers (vCenter ESXi) 18

5.3 Critical System 3: Firewall (FortiGate 101F) 19

6. COMMUNICATIONS 20

6.1 Internal Staff: Template Informing Staff of Priority 20

6.2 External Customers: Template Informing Customer Support 20

6.3 Use of Workarounds: Template Advising Affected Users 21

6.4 Issue Has Been Resolved: Template Advising Affected Users 21

7. TESTING / TRAINING 22

7.1 Testing and Review: 22

7.2 Training and Awareness: 23

7.3 Document control and plan distribution 24

Appendix A – IT Governance Diagram 25

Appendix B – Enterprise Architecture Diagram 26

Appendix C – Physical Network Diagram 27

Appendix D – Logical Network Diagram 28

Appendix E – Enterprise Architecture Diagram (Revised) 29

Appendix F – GAP Analysis Forms 30

Appendix G – SWOT Analysis 32

Timeline 33

Appendix I – Risk Assessment Worksheets 33

Appendix J – Revised Physical Network Diagram 37

Report Purpose

Our team will be providing consultation services in order to assist Company X in upgrading network infrastructure to improve connectivity and enhancing end user and systems security. Network infrastructure upgrades will improve 10 Gbit connections between on-property facilities by converting MPLS to ELAN. End user and systems security will be enhanced through EDR/MDR/SIEM, awareness training, MFA/MDM, and email security.

The purpose of this report is to detail the relevant current network infrastructure of Company X, detail the scope of the project, and identify key next steps. The current network infrastructure will be outlined through an enterprise architecture report and a Logical and Physical Network Diagram. We will end with a summary of our findings and identify key next steps for our team.

Company Overview

Company X is a prestigious country club that was founded by soda fountain magnate James Walker Tufts in 1895 as a health and wellness resort. The famous Company X was opened in 1907 and has since hosted 3 US Opens, 1 Ryder Cup and 1 PGA Championship. Today Company has 10 18-hole golf courses, 4 hotels, a spa, and several remote/satellite locations within the Company. Company is currently staffed by a mix of seasonal, part-time, and full-time positions for a rough total of 1500 employees. The IT department has a current team of 11 people maintaining the network. Within the next 12 months Company will become a spotlight in the world of golf, hosting the 2024 US Open, among other tournaments, and is an anchor site (rotational property) for future US Opens.

IT Governance Structure

See Appendix A for the breakdown of Company governance structure.

Although Company offers a wide variety of golf courses, hotels, spas, and employs roughly 1,500 personnel, the corporation does not currently consist of a strict IT governance structure. The current Director of Information Technology is Ed Nickelson, who leads the company's IT department as well as 10 additional employees who make up the company's IT department. Therefore, these 11 employees are responsible for determining if Company information technology is being used efficiently and effectively to execute the corporation's operational goals.

The chain of command for maintaining existing information systems and implementing new systems to execute company goals begins with the Director of Information Technology which oversees the entire IT department. Then depending on the nature of the system, the Applications and Infrastructure/Projects managers would implement action. Then the Applications Engineers and Security Engineer would be next to take action. Finally, the helpdesk and network technicians would conclude logistical tactics for maintaining and/or implementing new systems.

Enterprise Architecture

See Appendix B for Enterprise Architecture Diagram

The company’s business architecture is a well-structured framework designed to deliver rich history, world-class golf courses, luxurious accommodations, and a wide range of amenities. The company's business model involves SWOT analysis to help them assess their internal strengths and weaknesses and external opportunities and threats to make informed decisions. The company’s process model includes Business Process Modeling (BPMN) to map out guest’s check-in/check-out processes, reservation management, and other operation workflows. Company has taken steps to promote sustainability and environmental responsibility, including conservation efforts on the golf courses. This commitment to eco-friendliness is an attractive feature for guests who appreciate environmentally conscious practices. By embracing digital technology, personalized services, and loyalty programs, Company’s business architecture reinforces its competitive advantage within the luxury golf and leisure industry, making it a destination of choice for many travelers and golf enthusiasts.

Regarding the company’s information architecture, it is a comprehensive system ensuring the seamless flow and management of data and information. The company currently uses MFA (Multi-Factor Authentication) for their RDP (Remote Desktop Protocol) Windows login to add an extra layer of protection to the process of logging into their computers or servers remotely. VMware Horizon via Duo is used for remote access. The company is currently working on adding PAM (Privileged Access Management) and NAC (Network Access Control) likely from Fortinet which is their current firewall provider. Their firewall device is FortiGate 101F and provides security and network protection for the company by offering firewall protection, intrusion prevention, antivirus, and VPN capabilities. Some other practices that Company implement involve regular security audits and testing, backing up data, data minimization, and ongoing employee training with ArticWolf for managed SOC and security awareness as well as knowbe4 for phishing/security awareness. By implementing these security and data management measures, Company can protect guest information and preferences, ensuring that guests' personal data is kept secure and used to provide enhanced and personalized experiences while also complying with data privacy regulations.

Company’s application architecture is designed to deliver seamless and efficient services to guests and manage their robust operations. They currently leverage Agilysys, a technology provider that offers a wide range of hospitality solutions to enhance operations and secure data. Visual One/Versa, solution developed by Agilysys Company, includes Property Management System (PMS), reservation and booking system, mobile solutions, and security and compliance with industry standards including Payment Card Industry Data Security Standard (PCI DSS) and General Data Protection Regulation (GDPR). Their Point of Sale (POS) solution is InfoGenesis, another platform developed by Agilysys to enhance the efficiency and accuracy of food and beverage service operations. Other applications to mention are YellowDog for resort inventory needs and Revinate/Navis for sales CRM tool. Revinate/Navis is the only software solution that is SAAS, all other solutions are hosted on premises in fear of information exposed to the cloud. Company’s application architecture is a vital component in the delivery of exceptional guest experiences and the successful management of a high-end resort.

Company’s technology architecture is a dynamic framework that encompasses the hardware, software, security, and network infrastructure necessary to support its hospitality operations. Its

network security is configured of a network involving a FortiGate 101F appliance and a switch (FortiSwitch 1048) with two 10G uplinks. This configuration is a redundant setup where two FortiGate devices are connected to a switch for high availability and load balancing. The FortiGate devices work together to provide network security and traffic management. Company uses multiple network providers, a CenturyLink VLAN and Spectrum VLAN, both connected via 1G fiber runs. There is an MPLS (Multiprotocol Label Switching) in use, and it's connected via a 10G fiber run. MPLS is used to secure their wide-area networking. Data routing into the network enters via Layer 3 routing/switching onto the FortiSwitch 1048 “dirty” VLAN and then distributed to the production network on a “clean” VLAN. This architecture is designed for scalability and reliability, enabling the management and delivery of services across their network.

Project Scope

As Company LLC is currently undergoing an infrastructure update to improve its current on-site connection systems, the scope of this report is to address how the company will transition from a packet transferring system (MPLS) to a more modern approach of grouping various LANs throughout Company Resort. Additionally, we will evaluate firewall and switch enhancements. There are five core concepts we will focus on enhancing while conducting our gap analysis, risk assessment, needs assessment and SWOT analysis further along in the project for Company LLC. These concepts include systems security, awareness training, multi-factor authentication, mobile device management solutions, and email security. We will identify any risks that come up throughout the course of our study and provide recommended solutions for each with documentation to back them up.

Physical Network

See Appendix C for Physical Network Diagram

Company’s physical network is large, spanning several hotels, several off-site restaurants, a clubhouse, and seven remote locations. Due to this size, we have chosen to focus on the PBX Datacenter, the Front Desk Rack Room, and Couse 8, a satellite location. Company’s network is fed by three one-gigabit circuits, two from CenturyLink/BrightsSpeed and one from Spectrum. These three circuits are fed into a Layer 3 Fortinet 1048 FortiSwitch and tagged with a dirt VLAN. This dirty VLAN is then routed to the Fortinet 101F FortiGate firewall where it passes through firewall rules. After inspection it is passed to the production network via a clean VLAN back to the 1048. The 1048 pair acts as the main distribution switches for the property.

Connected to the 1048 is a Cisco Catalyst 9500. The C9500 acts as a second distribution switch, connecting the remaining Cisco parts of the property to the 1048 as well as serving as the connection switch for vCenter ESXi and Storage traffic and the landing point for the remaining MPLS circuits. Course 8 is one of the satellite locations fed by MPLS. This MPLS circuit connects to a Fortinet FortiGate 80F on the satellite side to provide local firewall routing and DHCP. This 80F then feeds two Cisco Catalyst 2960 switches for the clubhouse and golf course maintenance facility. As for the Front Desk, three Fortinet 148F FortiSwitches connect to a main 148F that has a 10-gigabit connection back to the 1048. This allows for Fortinet FortiLink to

manage the switches. Company is currently undergoing a conversion of the remaining Cisco switches to Fortinet switches to broaden its 10-gigabit connections.

Logical Network

See Appendix D for Logical Network Diagram

The logical diagram of the Company Resort and Country Club network, including its connections, components, and communication protocols, is usually shown in the logical diagram. Servers, switches, routers, firewalls, and the several subnetworks inside the country club are possible components. The graphic would highlight data protection, security protocols, and access control systems while illuminating the flow of data across various places. It is also possible to illustrate subnets and their connections for other departments, including facilities management, member services, and administration. In essence, the logical diagram offers a high-level depiction of the network's organizational structure and operating framework.

Summary of Findings and Next Steps

Company currently has a very robust network infrastructure; however, they have areas for improvement. Company is working on increasing bandwidth between sites from 1 Gigabit to 10 Gigabit connections. Alongside this project they are also replacing older Cisco equipment with newer Fortinet equipment to provide better insight and management of the network through FortiLink. Regarding this route, we agree with Company's goals and methods. Another area where Company is lacking is in the control of their network. Currently Company does not have any form of Risk or Role Based Access Control (RBAC), no Network Access Control (NAC), and no Privileged Access Management (PAM). Regarding this, we recommend potential solutions such as FortiNAC or Cisco ISE for NAC and Delinea or FortiPAM for PAM solutions. Regarding Security Awareness Training, Company currently is using KnowBe4 and just brought on ArcticWolf for managed security awareness. The current use of KnowBe4 has been limited to phishing tests with minimal training being issues to users for security awareness. Therefore, we recommend Company work on utilizing KnowBe4's library of content to deliver training alongside the rollout of ArcticWolf's training.

Needs Assessment

Company LLC currently has a robust network spanning much of the Company area with 4 hotels and 5 clubhouses. Currently much of the backbone network, internally and between sites, is gigabit fiber. To provide a better employee experience, and futureproofing to provide a better guest experience, Company is aiming to replace most of the backbone with 10 gigabit fiber, and 10 gigabit-compatible switches accordingly. To provide a better connection with satellite sites, Company is transitioning from MPLS to ELAN to provide better Layer 2 connectivity and bandwidth scalability. Lastly, to meet requirements by cyber insurance, Company is evaluating Privileged Access Management solutions to migrate from spreadsheets and common-knowledge credentials to secure role-based access on-demand credential access.

To facilitate the network upgrade, new switches and firewalls will need to be acquired. Potential firewall hardware would be Cisco 3100/4100 series firewalls or Fortinet FortiGate 400Fs or

600Fs. The new switching hardware could be Cisco Catalyst 9300/9400 series switches or Fortinet FortiSwitch148Fs. Currently Company has a broad rollout of both Cisco and Fortinet equipment, with a focus on migrating away from Cisco towards Fortinet. The aforementioned equipment would be capable of ingesting, managing and processing 10 gigabit traffic with ease.

To meet the PAM requirements for cyber insurance, solutions from Delinea or Fortinet are strong options. Delinea Secret Server and Privilege Manager is a strong product for its price point. Meanwhile, Fortinet's FortiPAM product is new to the market, and although it lacks some features it is cost-effective and has integration with the Fortinet Security Fabric. Both of these products feature role-based access control to privileged credentials as well as session monitoring.

Risk Assessment

See Appendix I for Risk Assessment Worksheets

In June of 2024 Company LLC will be the spotlight of televised Golf across the world as they host the 2024 US Open Golf Championship. This kind of publicity puts a target on Company's back by bad actors. There are several areas of risk that must be considered: financial, reputation, productivity and legal. During each day of the Open millions of dollars' worth of transactions will occur. Any disruption to the event would harm Company's reputation and potentially put Company in legal contest if the disruptions affect third party entities. The scope of such disruption would impact varying levels of productivity. Therefore, in measuring the impacts of risk, financial and reputational risks are of the highest level.

There are several points along Company's IT infrastructure that can be identified as potential vulnerabilities. These areas are: the FortiGate firewalls, VisualOne (the Property Management System (PMS)), the employees, and malware. The FortiGate firewalls are central to Company's routing, is where the ISP connections land and the default gateways live. To mitigate outages, the firewalls are in a high-availability (HA) pair. However, the current firewalls barely meet the current network demands, and an unexpected shift of load can lead to overloading. Agilysys VisualOne is the core PMS product at Company. Most of Company's systems connect back to VisualOne to manage a guest's itinerary as well as guest financials. VisualOne is a legacy product that is currently undergoing an upgrade by the vendor. Until the modern replacement is generally available, VisualOne is prone to latency. It is also reliant on a singular app and database server.

Like many institutions, the employees are a potential liability. Employees can be careless or willingly become threat actors. Either situation can lead to data loss and exposure of confidential information or even the introduction of malware into the environment. These activities can lead to degradation of business or even a complete halt in business activities. Lastly, malware can cause major disruptions to business activities as well as data confidentiality. Malware can pop instantly or be dormant for weeks or even years waiting until it is well engrained and is able to gain the access it needs. In the event of an infection, typically the anti-malware solution can resolve the event. However, if the malware is more complex like ransomware, it can require an exhaustive effort to recover with an adequate backup with acceptable losses of data.

Enterprise Architecture (Revised)

See Appendix E for Enterprise Architecture Diagram (Revised)

In Company's existing technology architecture, the switch serves as a pivotal component in the network infrastructure, functioning as the entry point for internet-bound traffic. The switch, specifically identified as the FortiSwitch 1048, plays a crucial role in directing and managing data flows within the network. Positioned at the forefront of Company's connectivity framework, this switch is designed to efficiently route incoming and outgoing data, ensuring that information is transmitted securely and swiftly between various devices and network segments. The FortiSwitch 1048 is an integral part of the redundant setup, working together with the FortiGate 101F appliances to provide network security, load balancing, and high availability. It operates at both Layer 2 and Layer 3 of the OSI model, facilitating effective data routing and switching. As Company evolves its enterprise architecture to enhance security measures, the proposed introduction of an Internet Entry Firewall will further fortify this switch entry point, bolstering the overall resilience and protective capabilities of the network against potential cyber threats from the internet.

Gap Analysis

See Appendix F for GAP Analysis Forms

In this section we will assess where Company LLC's current information technology and systems are, where the corporation would like them to be, and how our team recommends the company to implement this transition by performing a GAP analysis. Company LLC currently operates with 1 Gigabit connections, uses Cisco equipment, and uses KnowBe4 as their security awareness tool, while mainly focusing on phishing threats. Additionally, Company LLC currently lacks role-based access controls which grant access privileges based on employee roles. Company also lacks network access controls, which increases network visibility and reduces risk. The organization also does not utilize privileged access management which identifies which users require privileged access controls.

Company LLC wishes to transition to 10 Gigabit connections as well as integrate Fortinet equipment in with any Cisco equipment that they will utilize after the upgrades. The organization also wishes to implement heightened security awareness tools and expand their focus from phishing threats to prevent other security threats. Additionally, the company will need to install new firewalls and switches to accommodate their network upgrade.

To bridge this gap between where Company Resort's technological infrastructure currently is and where it needs to be improved, we will suggest some recommendations for how to facilitate the upgrade process. First off, our team recommends transitioning to 10 Gigabit fiber connections. Next, we recommend Company LLC to expand on KnowBe4's security awareness training by implementing ransomware and social engineering features as well. We also recommend that the organization continues using Arctic Wolf security operations. Our team believes Cisco 3100/4100 series firewalls or Fortinet FortiGate 400Fs or 600Fs are great firewall options for the organization. Additionally, we suggest acquiring Cisco Catalyst 9300/9400 series switches or Fortinet FortiSwitch148Fs for switch upgrades. The goal of these combined

recommendations is to allow Company LLC to implement maximum security awareness, facilitate much needed network upgrades, and reach desired system performance standards.

SWOT Analysis

See Appendix G for SWOT Analysis Diagram

The purpose of this S.W.O.T analysis is to detail Company Resort's strengths, weaknesses, proposed opportunities, and threats to provide insight into a feasible solution for undergoing the suggested upgrades and transitions.

Company LLC currently emphasizes a strong business architecture and competitive advantage through its multifaceted customer amenities and core values. The organization excels in utilizing a well-structured framework as well as implementing security awareness through different security operations. Although Company LLC has a well-designed framework, the company has a few core weaknesses. Please see Appendix G for detailed weaknesses. After assessing these shortcomings, we are able to identify possible opportunities for the organization. Outdated equipment could be upgraded by acquiring new firewalls and switches. Additionally, Company should expand their IT governance, security training, and assign NAC, PAM, and RBAC tools.

Some possible threats Company LLC faces are security breaches such as phishing, malware, ransomware, and social engineering. The organization is also susceptible to physical and online theft. Unauthorized access, data loss, and natural disasters are all feasible potential threats for the company as well.

Migration Planning

See Appendix H for Timeline

Phase I: Upgrade Connections

The first phase is upgrading Company's current 1 Gbit connections. The company should begin with 10 Gbit installation at the main site with applicable network gateways, clients, and cables. The organization should then implement 10 Gbit connectivity to remote/satellite locations. Once these connections are installed, troubleshooting and observation should follow.

Phase II: Transition from MPLS to ELAN

In the next phase, Company will transition from MPLS to ELAN to improve network connectivity and bandwidth scalability. To facilitate this transition, acquisition of new firewall hardware (Cisco 3100/4100 series firewalls or Fortinet FortiGate 400Fs or 600Fs) and switches (Cisco Catalyst 9300/9400 series switches or Fortinet FortiSwitch148Fs) would need to take place.

Phase III: Cisco to Fortinet Transition

To accommodate the new 10 Gbit connectivity, Company will need to transition from Cisco equipment to Fortinet to adequately ingest, manage, and process the new amount of traffic. In this phase, Company would also establish PAM, NAC, and RBAC.

Phase IV: Implement Heightened Security Awareness Measures

In the final phase, after the new connections and equipment have been established, Company will continue to use KnowBe4 security operations for phishing security measures. The organization will also expand on their limited usage of Arctic Wolf security operations for heightened security measures. This phase would also be used to monitor any errors or threats that could arise from implementation of the new equipment installations and upgrades.

Detailed Budget

y

Description	Quantity	Purchase Price	Subtotal	Rationale	Features		Vendor	Asset Class
Fortinet FortiSwitch 148F Switch	2	$ 895.58	$ 1,791.16	The 148F has more total network interfaces, a high switching capacity, quadruple the packets per second, and more Mac Address Storage	Total Network Interfaces:	48x GE RJ45 and 4x 10GE SFP+	AV Firewalls	Computer & Network Equipment
					Switching Capacity:	176 Gbs		
					Packets per Second (Duplex):	260 Mpps		
					Mac Address Storage:	32 K		
QuickTreX Multimode 10 Gigabit Fiber Optic Network Extension (RJ45 to Fiber to RJ45) Conversion Kit w/ 500FT 2 Strand MM OM4 Indoor/Outdoor	1	$959.24	$959.24	This QuickTreX Multimode 10 Gigabit Fiber Optic Network Extension is perfect for any enterprise looking to expand their LAN connection and speed. It comes with two 500 ft strands that can connect the entire network. This will bring the speed and connectivity that Pinehurst is looking for.	Link Length:	550 meters (10Gb/s@850nm) x 2	LAN Shack	Computer & Network Equipment
					Bandwidth (EMB High Performance):	4700MHz.km@850nm		
					Wavelength:	850/1300nm		
					ndoor/Outdoor UV Rated Distribution Jacke	YES		
Fortinet FortiGate 600F	1	$14,219.00	$14,219.00	The Fortinet FortiGate 600F supports 10.5 Gbps threat protection throughput and 9 Gbps SSL Inspection throughput. This will be compatible with the existing network of Fortinet switches and support a 10 Gigabit Fiber network.	NGFW Throughput:	11.5 Gbps	Network Devices Inc	Computer & Network Equipment
					Threat Protection Throughput:	10.5 Gbps		
					SSL Inspection Throughput:	9 Gbps		
					Concurrent Sessions:	7800000		
Fortinet FortiPAM 1000G	1	$53,100.00	$53,100.00	The Fortinet FortiPAM is a Privaleged Access Management Server that can handle up to 50 users. This is ideal for the LAN that Pinehurst is focusing on improving. It also easily integrates with the new and existing Fortinet hardware that Pinehurst relies on. This is the best choice for price, security and compatibility with existing hardware.	Local + Remote Users (Base):	50	AV Firewalls	Computer & Network Equipment
					Secrets:	5000		
					Folders:	2000		
					Secret Requests:	5000		

Conclusion

The purpose of this report is to provide recommendations for Company's Network improvement project. The goals of the network improvement are to improve network speed, increase satellite location connectivity, and increase network security. We recommended improvements to network speed through 10 gigabit fiber optic cable and 10 gigabit compatible switches. In order to improve satellite location connectivity, transition from MPLS to ELAN is recommended. Finally, in order to improve network security, we recommend the implementation of a FortiPAM Privileged Access Management Server.

The next steps will be the migration and implementation of the network to the new hardware. The team recommends implementing the hardware solutions in a multi-step process starting with connection upgrades. Next, the Cisco hardware should be upgraded and finally, the recommended firewall and switches should be implemented The recommended hardware solutions should be supplemented with Security Training and awareness. We are confident the

implementation of these hardware solutions will satisfy the needs of the Company network improvement project.

Company

COMPANY DISASTER RECOVERY PLAN

This plan will be reviewed once annually and immediately after any major changes to the delivery of the service.

1. CONTACTS

1.1 IT Management Team

Ref	Name	Role during a disruptive incident	Contact Numbers (O) Office desk phone (M) Work Mobile
1.	**Ed Nickelson**	Director of Information Technology	(O) (M)
2.	**Kevin Biegger**	Security Engineer	(O) (M)
3.	**Nick Wolcott**	Directory Service Manager	(O) (M)

2. INTRODUCTION

2.1 Plan purpose and scope

The purpose of this disaster recovery plan is to ensure the continuity of Company Resort and Country Club's critical IT systems in the event of a disaster.

Scope

The plan focuses on minimizing downtime, protecting data integrity, and facilitating a swift recovery of IT services.

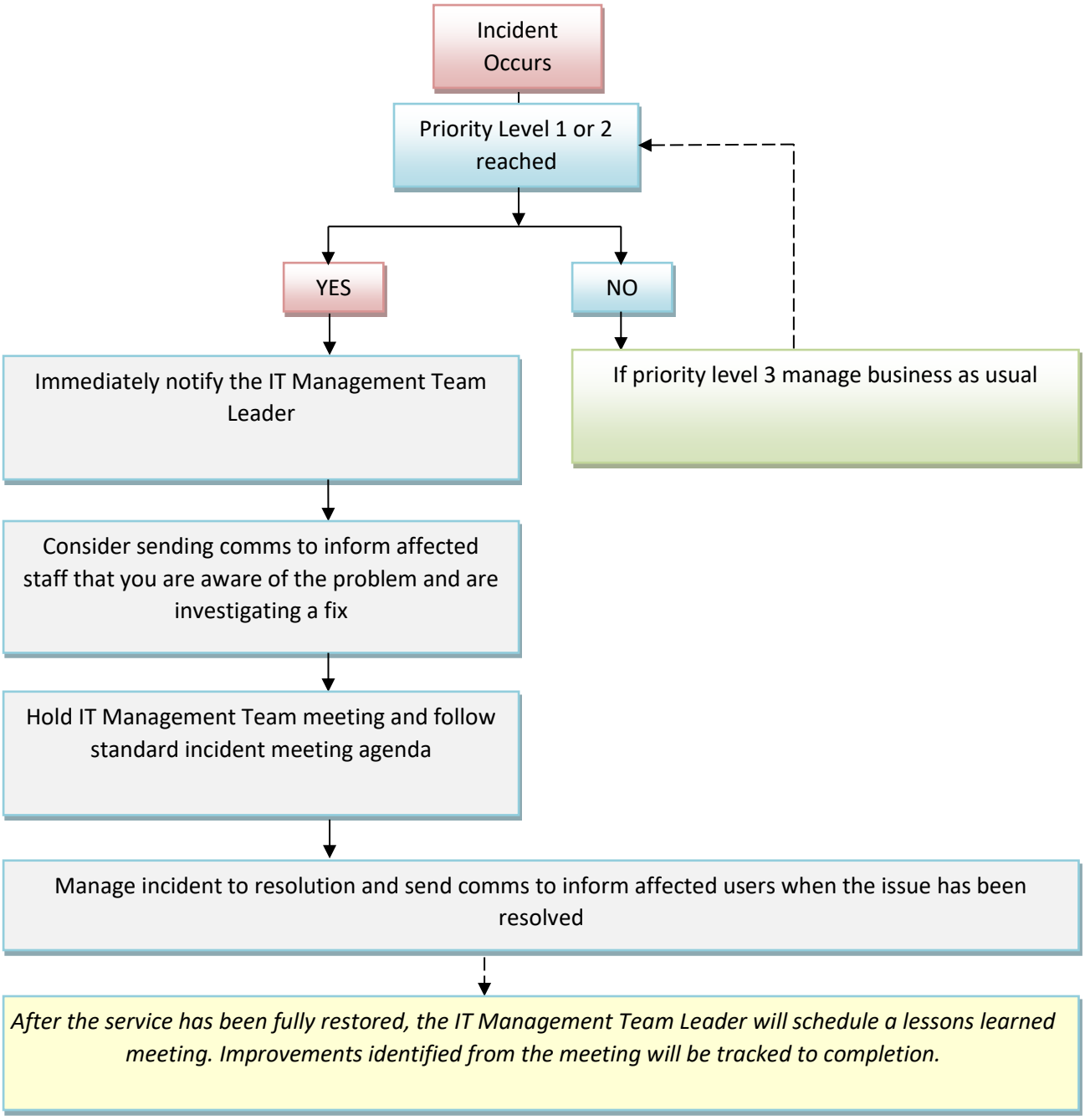
2.2 Risk Assessment

Identified Risks:

- Natural disasters (e.g., hurricanes, floods)
- Cybersecurity incidents (e.g., ransomware attacks)
- Equipment failures (e.g., server, networking hardware)
- Human errors (e.g., accidental data deletion)

3. INCIDENT MANAGEMENT

3.1 Incident flow chart



3.2 Fault detection

Company Resort and Country Club employs advanced health monitoring systems to ensure the continuous health and functionality of its critical IT systems. Health monitoring covers network infrastructure, servers, firewalls, and security systems. The monitoring systems track metrics such as network traffic, server performance, firewall logs, and security event data.

3.3 When to invoke the plan

The IT Management Team will invoke this plan if any of the following circumstances are met:

Priority Level	Circumstances
1	Website Unavailable; Critical System Failure
2	Percentage of Users Affected Exceeds Defined Threshold
3	General IT Issues Managed as Business as Usual

3.4 Standard incident meeting agenda

Ref	Agenda item	Responsible
1.	Situation report *What happened, when, do we know the cause, what actions have been completed.*	Technical Recovery Team Leader
2.	Impact assessment *Start an issues and actions log if it is the first incident management meeting. If it is not the first meeting, review the status of actions to address issues and whether any new issues have arisen.*	All
3.	Stakeholders and communications plan: • Do we need to issue internal comms? • Do we need to issue external comms?	All
4.	Confirm date, time and location of next incident meeting	IT Management Team Leader

4. ROLES & RESPONSIBILITIES DURING A DISRUPTIVE INCIDENT

Ref	Incident Role	Responsibility

1.	IT Management Team Leader	Oversee and manage the broader business impact of the disruptive incident.
2.	Technical Recovery Team leader	Disseminate crucial information to affected staff regarding the incident and provide updates, including temporary workarounds if applicable.
3.	Member of staff who receives fault alert	Promptly inform the IT Management Team and Technical Recovery Team upon receiving fault alerts, ensuring swift communication of incident details.

5. DISASTER RECOVERY PROCEDURES

In the event of a disruptive incident, the following detailed step-by-step recovery procedures have been established to ensure the swift restoration of each critical system at Company Resort and Country Club. These procedures encompass initiation of recovery, data restoration, and systematic verification of system functionality.

5.1 Critical System 1: Network Infrastructure (FortiGate, FortiSwitch, Cisco Catalyst)

Initiation of Recovery:

Ref	Actions
1.	Notify the IT Management Team Leader and Technical Recovery Team Leader of the incident.
2.	Identify the root cause of the network disruption.
3.	Begin recovery by isolating affected components and initiating failover processes if necessary.

Data Restoration:

Ref	Actions
1.	Restore network configurations from the latest backup.
2.	Verify the integrity of restored configurations to ensure alignment with security protocols.
3.	Implement redundancy measures for critical components, such as FortiGate and FortiSwitch.

Verification of System Functionality:

Ref	Actions
1.	Conduct thorough testing of network connectivity across different segments.
2.	Monitor network traffic for anomalies and potential security breaches.
3.	Collaborate with security personnel to ensure the integrity of the restored network.

5.2 Critical System 2: Servers (vCenter ESXi)

Initiation of Recovery:

Ref	Actions
1.	Alert the IT Management Team Leader and Technical Recovery Team Leader about the server incident.
2.	Identify the affected servers and assess the extent of the disruption.
3.	Begin recovery by isolating affected servers and initiating the restoration process.

Data Restoration:

Ref	Actions
1.	Restore server configurations and critical data from backups.

2.	Verify the consistency of restored data to maintain data integrity.
3.	Implement failover mechanisms for critical server functions.

Verification of System Functionality:

Ref	Actions
1.	Execute comprehensive tests on server functionality, including critical applications.
2.	Monitor server performance metrics to ensure optimal operation.
3.	Collaborate with application owners to validate application-specific functionalities.

5.3 Critical System 3: Firewall (FortiGate 101F)

Initiation of Recovery:

Ref	Actions
1.	Notify the IT Management Team Leader and Technical Recovery Team Leader about the firewall incident.
2.	Identify the nature of the firewall disruption and assess its impact.
3.	Begin recovery by isolating the firewall and initiating recovery processes.

Data Restoration:

Ref	Actions
1.	Restore firewall configurations from backups, considering security policies.
2.	Validate the restored configurations to align with security protocols.
3.	Implement additional security measures, such as rule validation and intrusion prevention.

Verification of System Functionality:

Ref	Actions
1.	Conduct penetration testing to ensure the resilience of the firewall.
2.	Monitor firewall logs for any unusual activity.
3.	Collaborate with security teams to validate the effectiveness of the restored firewall.

6. COMMUNICATIONS

Below are the communications templates to use during disruption to the application.

6.1 Internal Staff: Template Informing Staff of Priority

Subject: Urgent: Disruption to IT Services - Action Required

Dear [Team/Department],

I hope this message finds you well. We want to inform you that we are currently experiencing a disruption in our IT services. Our team is actively working on resolving this issue as a top priority.

Current Status:

- [Brief description of the issue]
- [Any workarounds currently in place]

Next Steps:

- Our technical recovery team is actively addressing the problem.
- Regular updates will be provided.

Please bear with us as we work diligently to restore full functionality. Your patience and cooperation during this time are highly appreciated.

Best Regards,

[Your Name]
[Your Position]
Company Resort and Country Club IT Department

6.2 External Customers: Template Informing Customer Support

Subject: Important Notice: Temporary Disruption to Services

Dear Valued Customer,

We hope this message finds you well. Unfortunately, we are currently experiencing a disruption to our services that may impact your experience. Our technical team is actively addressing the issue, and we sincerely apologize for any inconvenience this may cause.

Current Status:

- [Brief description of the issue]
- [Any workarounds currently in place]

Next Steps:

- Our team is working diligently to resolve the problem.
- Updates will be provided regularly.

We appreciate your understanding and patience during this time. If you have any urgent inquiries, please contact our customer support team at [Contact Information].
Thank you for your continued trust in Company Resort and Country Club.

Best Regards,

[Your Name]
[Your Position]
Company Resort and Country Club Customer Support

6.3 Use of Workarounds: Template Advising Affected Users

Subject: Important: Temporary Workarounds for IT Service Disruption

Dear [User],

Due to the ongoing disruption to our IT services, we would like to provide you with temporary workarounds to minimize any impact on your work. Please follow the instructions below:

Workarounds:

1. [Detail of the first workaround]
2. [Detail of the second workaround]
3. [Any additional steps or precautions]

Our technical team is actively working on a comprehensive solution, and we appreciate your cooperation during this time.
If you have any questions or concerns, please do not hesitate to contact our IT support team at [Contact Information].

Thank you for your understanding.

Best Regards,
[Your Name]
[Your Position]
Company Resort and Country Club IT Department

6.4 Issue Has Been Resolved: Template Advising Affected Users

Subject: Update: Resolution of IT Service Disruption

Dear [User],

We are pleased to inform you that the disruption to our IT services has been successfully resolved. All systems are now operating as usual.

Summary:

- [Brief description of the resolution]
- [Any additional information or steps]

We appreciate your patience and understanding during this period. If you encounter any lingering issues or have further questions, please contact our IT support team at [Contact Information].

Thank you for your cooperation.

Best Regards,
[Your Name]
[Your Position]
Company Resort and Country Club IT Department

7. TESTING / TRAINING

A lessons learned meeting will be held after all P1 and P2 disruptions have been resolved in order to discuss whether health monitoring, alerting, response and recovery processes and procedures were effective.

7.1 Testing and Review:

Testing Schedule:

1. **Frequency:** Conduct a comprehensive test of the disaster recovery plan annually.
2. **Types of Tests:**
    - **Tabletop Exercises:** Simulate disaster scenarios in a controlled environment, allowing key personnel to discuss and validate their roles and responsibilities.
    - **Simulated Disaster Scenarios:** Execute realistic simulations of potential disasters to evaluate the effectiveness of the plan in a more dynamic setting.
    - **Technical Tests:** Verify the functionality of backup systems, recovery procedures, and communication protocols.

Review Process:

1. **Post-Test Evaluations:** Collect feedback from participants and stakeholders involved in the testing process.
2. **Incident Debriefs:** Analyze the performance of the disaster recovery plan during simulated scenarios, identifying strengths and areas for improvement.
3. **Documentation Review:** Assess the completeness and accuracy of the disaster recovery plan documentation.

Improvement Strategies:

1. **Feedback Implementation:** Use feedback gathered from post-test evaluations and incident debriefs to implement immediate improvements to the plan.
2. **Continuous Refinement:** Regularly review and update the disaster recovery plan based on emerging technologies, changes in infrastructure, and lessons learned from testing and real incidents.
3. **Training Adjustments:** Modify training programs based on feedback and identified areas of improvement.

7.2 Training and Awareness:

Training Program:

1. **Development:** Design a comprehensive training program to educate staff on their roles and responsibilities during a disruptive incident.
2. **Delivery:** Conduct regular training sessions for all staff, ensuring they are familiar with the disaster recovery plan.
3. **Role-Specific Training:** Tailor training modules for specific roles within the disaster recovery team, emphasizing their unique responsibilities.

Awareness Initiatives:

1. **Communication Campaigns:** Regularly communicate potential risks and the importance of reporting incidents promptly through internal channels.
2. **Awareness Materials:** Provide resources such as posters, email updates, and newsletters to keep staff informed about the disaster recovery plan and cybersecurity best practices.
3. **Interactive Sessions:** Host workshops and interactive sessions to engage staff in hands-on activities related to disaster recovery.

Ongoing Training:

1. **Regular Updates:** Keep staff informed about changes to the disaster recovery plan through periodic updates and refresher courses.
2. **New Employee Orientation:** Include disaster recovery plan training as part of the onboarding process for new hires.

7.3 Document control and plan distribution

Comprehensive Document Maintenance:

1. **Regular Updates:** Ensure that the disaster recovery plan is regularly updated to reflect changes in infrastructure, personnel, and technologies.
2. **Contact Information:** Keep contact information for key personnel, vendors, and stakeholders up-to-date.
3. **Procedures and Timelines:** Document detailed procedures and recovery timelines, and review them regularly to ensure accuracy.

Secure Storage:

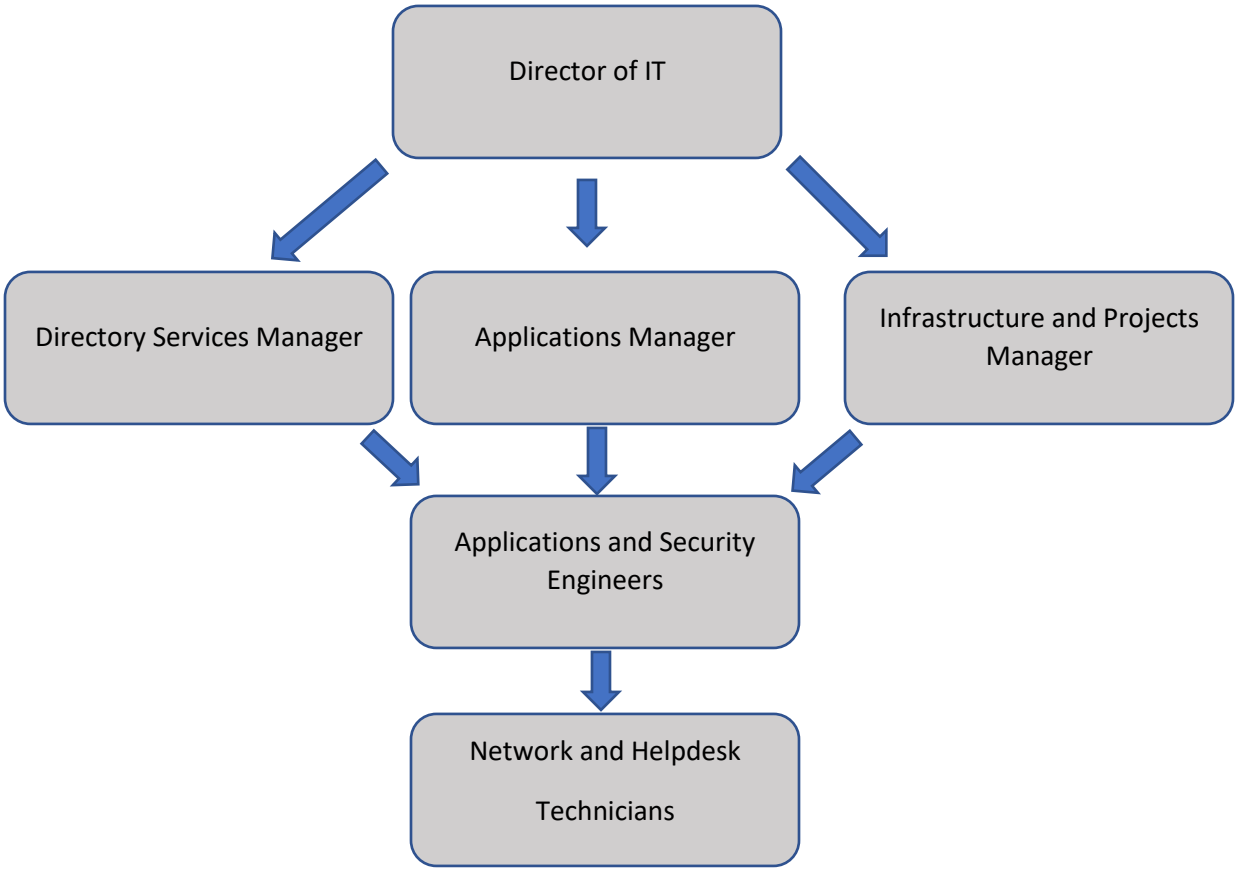
1. **Digital Storage:** Maintain digital copies of the disaster recovery plan in secure, password-protected locations accessible only to authorized personnel.
2. **Hard Copy Storage:** Keep hard copies in physically secure locations, such as a designated disaster recovery binder stored in a locked cabinet.

Accessibility:

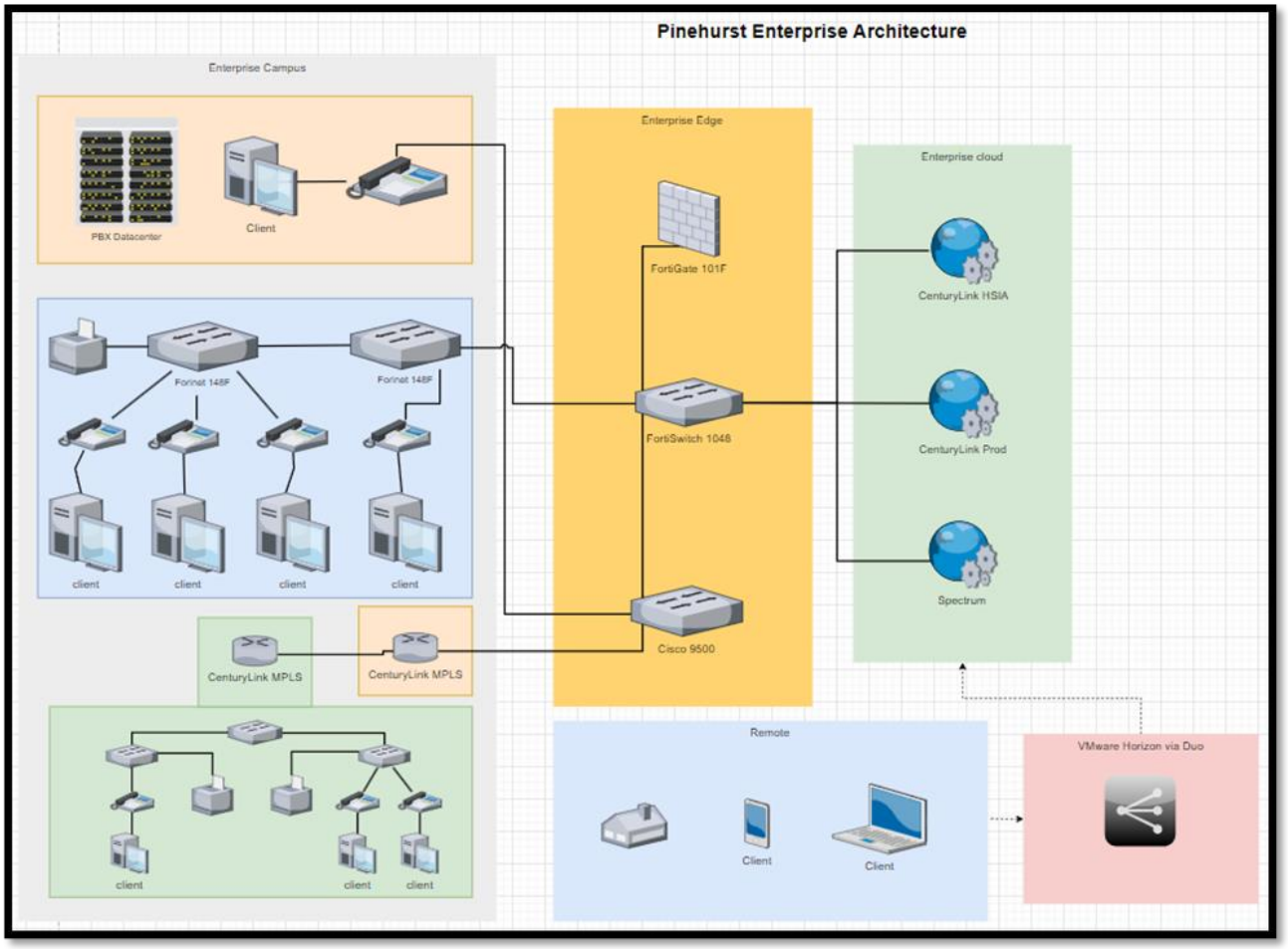
1. **Distribution:** Ensure that all relevant staff members have access to the latest version of the disaster recovery plan.
2. **Training on Access:** Educate staff on where to find the disaster recovery plan and how to access it when needed.

By implementing these strategies, Company Resort and Country Club aims to maintain a dynamic and resilient disaster recovery plan that evolves with technological advancements and organizational changes.

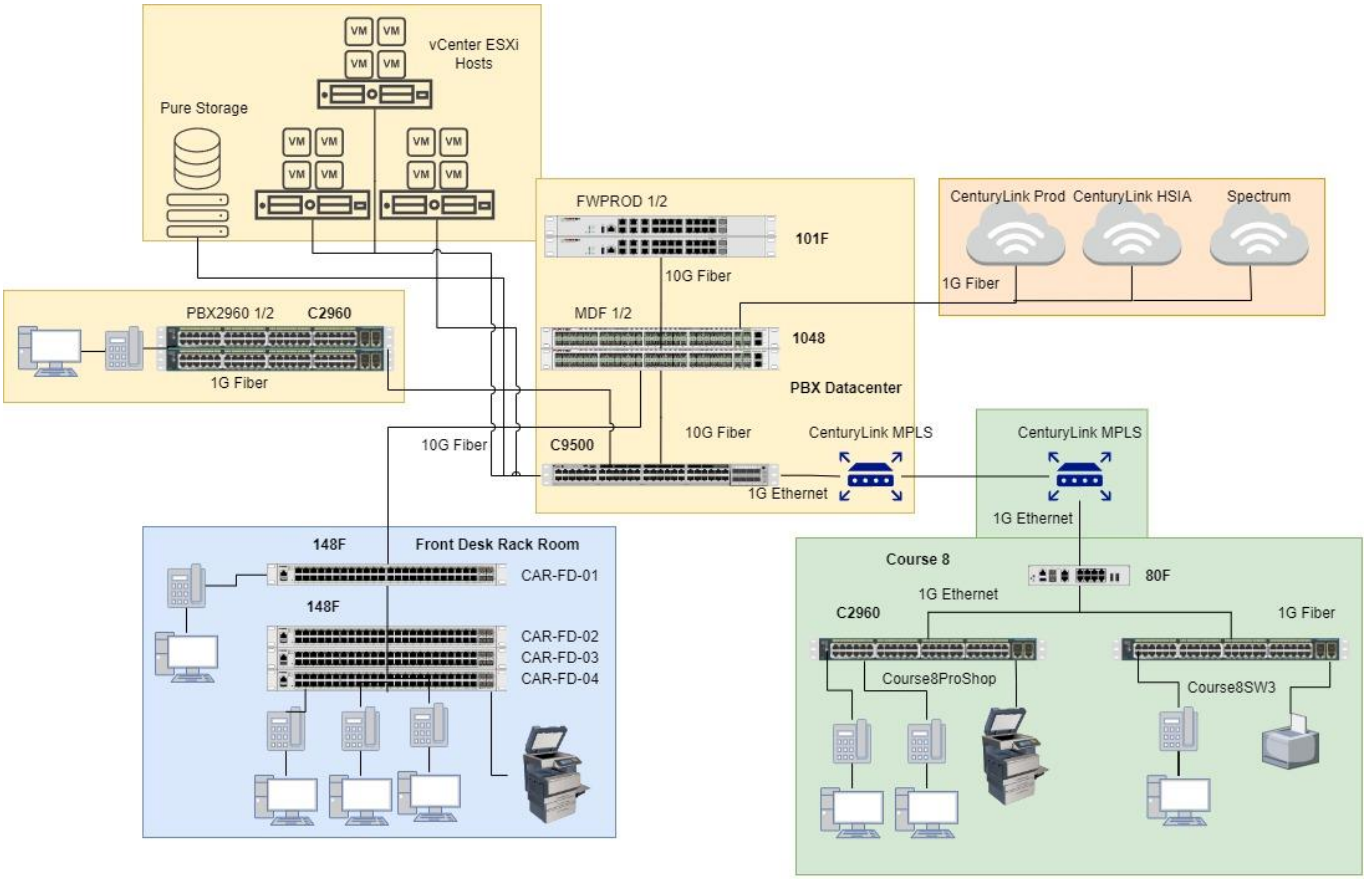
Appendix A – IT Governance Diagram



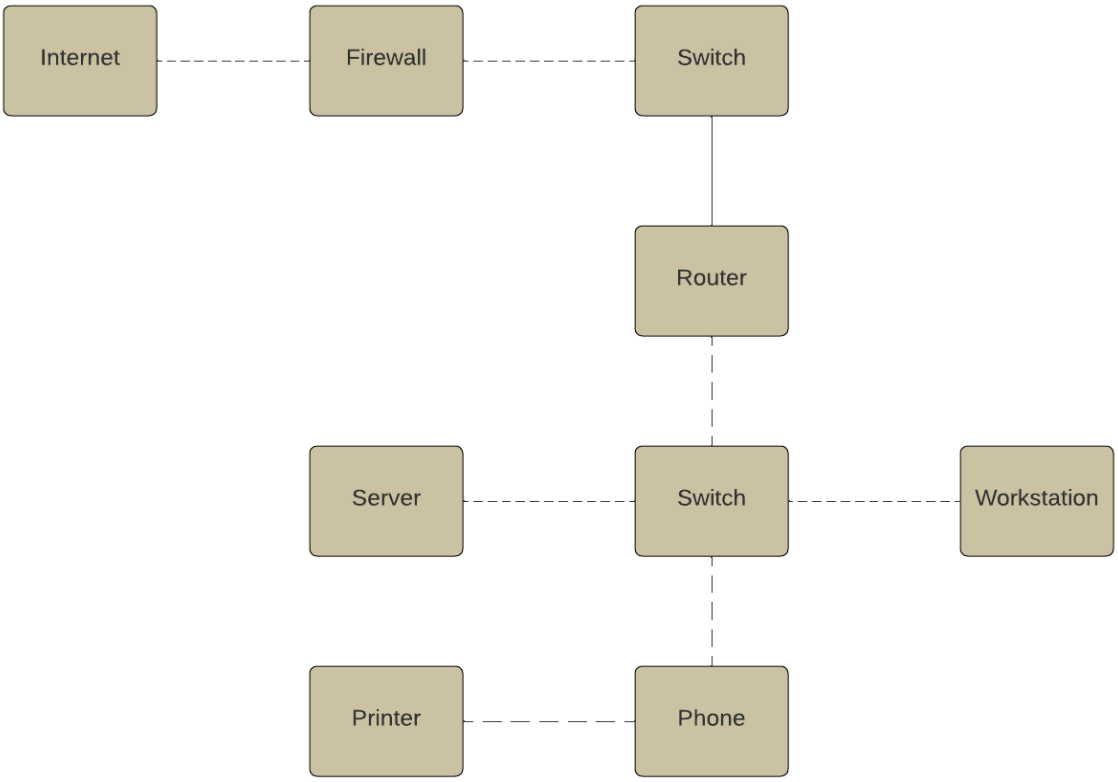
Appendix B – Enterprise Architecture Diagram



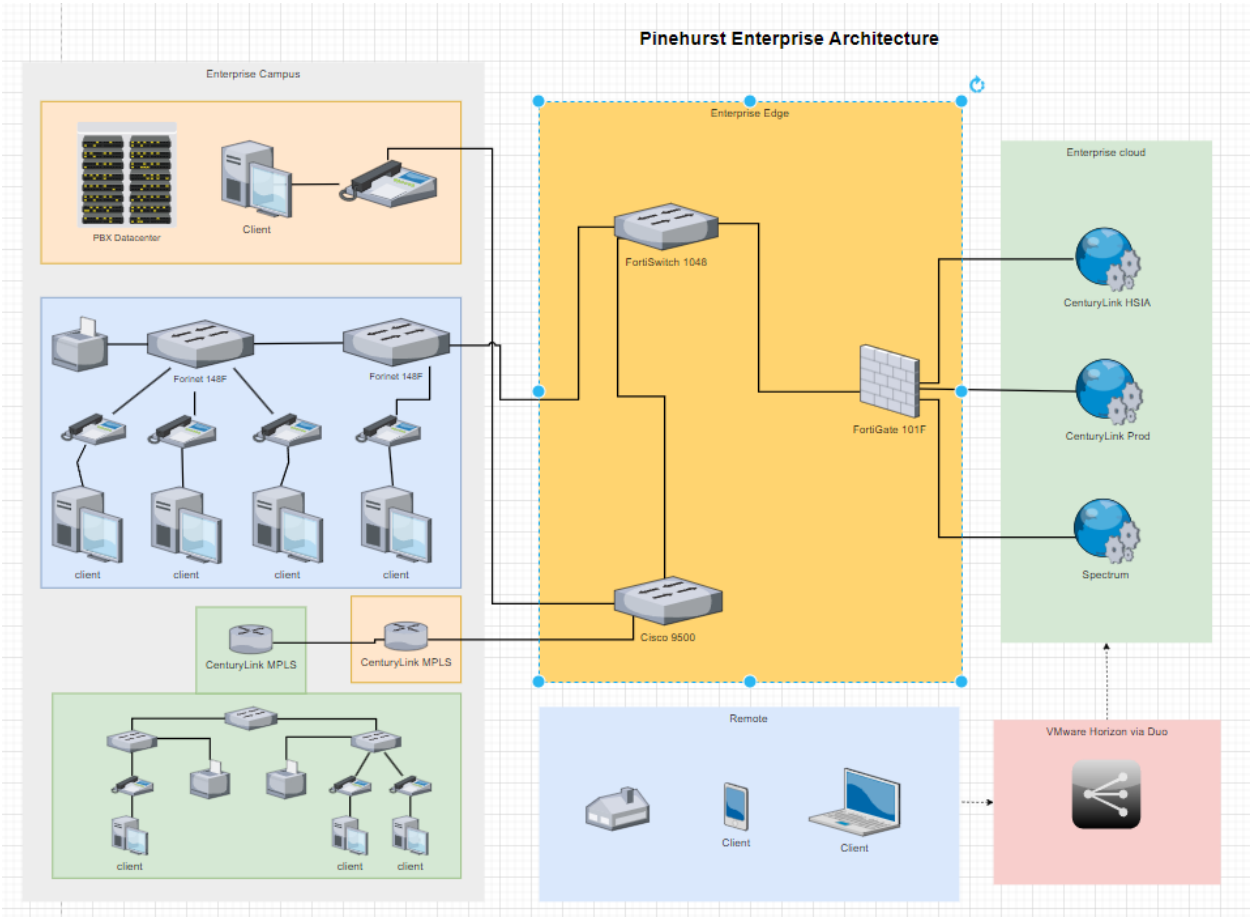
Appendix C – Physical Network Diagram



Appendix D – Logical Network Diagram



Appendix E – Enterprise Architecture Diagram (Revised)



Appendix F – GAP Analysis Forms

Business Unit Specific Gap Analysis

Business Unit:	Information Technology
Gap Analysis:	Upgrade connections at main site then followed by remote/satelite locations
Recommendations:	Prioritize bandwith enhancments to address capacity disparities, minimize downtime during the upgrades, and improve latency for better performance

Gap Analysis Metrics	Met	Somewhat Met	Not Met	Strengths	Weaknesses
Bandwith Discrepency			x		Network congestion, slow data transfer speeds, reduced overall eprformance hindering operational efficiency
Downtime Reduction			x		Extended source disruption negatively impacting productivity and causing financial loss
Latency Improvements			x		Delays in data transmission, affecting realtime communication colloboration and overall responsiveness of the network

Business Unit Specific Gap Analysis

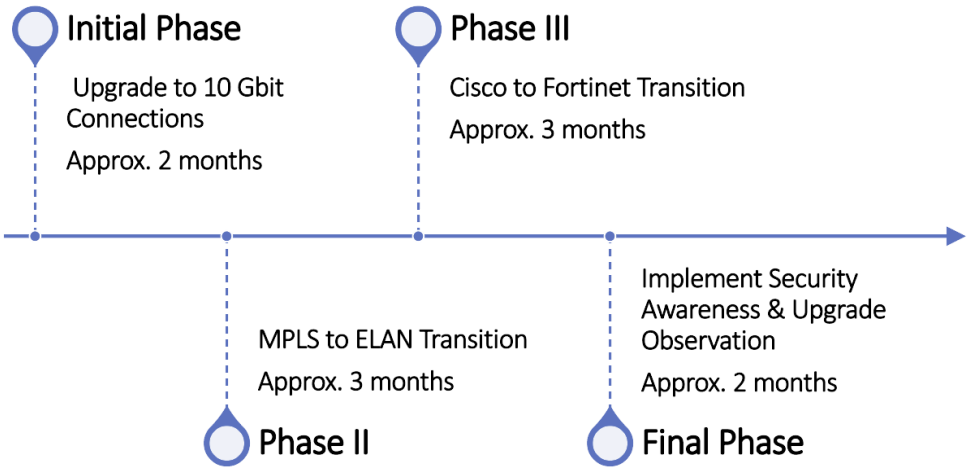
Business Unit:	Information Technology
Gap Analysis:	Secruity awareness/implementation within unit
Recommendations:	Updating training content with real wrold examples, increasing trianing frequencies, and diversifying methods
	Conduct regular assesments, establish clear communication plans, and ensure the content updating on secruity policies

Gap Analysis Metrics	Met	Somewhat Met	Not Met	Strengths	Weaknesses
Training Effectiveness			x		Absence of comprehensive follow up evaluation to guage the retention and knowledge of security practices over time
Policy Adherence			x		Inconsitent enforcment of secruity polocies leading to variation in adherence levels within unit.
Incident Response Time			x		Infrequent incident response stimulations.
Established Secruity awarness operations		x		Utilizing KnowBe4 platform	In addition should be utilizing Arctic Wolf

Appendix G – SWOT Analysis

Strengths	Weaknesses
• Strong business architecture and competitive advantage • Environmental sustainability practices • Well-structured framework • Large number of amenities/accommodations for customers to guarantee returning guests and ensure profitability • Utilization of MFA and RDP	• Outdated equipment • Limited IT governance • Narrow security training • Lack of NAC, RBAC, and PAM
Opportunities	**Threats**
• More reliable network connections • Heightened security awareness via Arctic Wolf and KnowBe4 • Implementation of NAC, RBAC, PAM • IT governance expansion • Utilization of EDR/MDR/SIEM • Upgraded firewalls and switches to facilitate the conversion from MPLS to ELAN	• Security breaches: phishing, malware, ransomware, social engineering • Unauthorized access to restricted material • Data loss • Natural Disasters • Theft

Timeline



Appendix I – Risk Assessment Worksheets

Vulnerability - Firewalls			
Asset	FortiGate 101Fs		
Asset Importance	HIGH		
Threat	Loss of HA pair, overloading		
Description	The current 101Fs are no longer suitable for surges in network changes.		
Likelihood	Low (1)		
Impact On	__ Confidentiality ___ Integrity _X_ Availability		
Impact Area	**Priority**	**Impact**	**Score**
Financial	High (3)	High (3)	9
Productivity	High (3)	High (3)	9
Reputation	Low (1)	Low (1)	1
Legal	Low (1)	Low (1)	1
		Impact Score	20
Risk Score (Likelihood x Impact)	20		
Adequacy of Existing Controls	High		
Risk Control Strategy	___ Accept _X_ Mitigate ___ Share ___ Defer		
Risk Mitigation Controls			

Replacement of Existing Equipment	Newer equipment is being sourced to provide resiliency against network surges and the addition of new networking equipment.

Vulnerability - Software			
Asset	VisualOne		
Asset Importance	HIGH		
Threat	Older system, single point of failure		
Description	VisualOne is the core PMS for Company. Any modification or loss of data could affect guest activity. Disruptions to the system would impact Company's ability to collect guest money.		
Likelihood	Low (1)		
Impact On	_X_ Confidentiality _X_ Integrity _X_ Availability		
Impact Area	**Priority**	**Impact**	**Score**
Financial	High (3)	High (3)	9
Productivity	High (3)	High (3)	9
Reputation	Low (2)	Low (2)	4
Legal	Low (1)	Low (1)	1
		Impact Score	23
Risk Score (Likelihood x Impact)	23		
Adequacy of Existing Controls	High		
Risk Control Strategy	_X_ Accept ___ Mitigate ___ Share ___ Defer		
Risk Mitigation Controls			
Anti-Malware and Backups	To protect guest and company data, anti-malware is deployed on all endpoints and backups are taken daily of the VisualOne database to ensure minimal loss of data.		
Replacement of Software	Agilysys is currently working on a modern replacement to VisualOne which will address potential performance concerns.		

Vulnerability - Employees	
Asset	Employees
Asset Importance	HIGH
Threat	Employees willingly or unwillingly expose Company to threat actors.

Description	Employees are a common point of vulnerability at any institution. They are common targets of phishing and are vulnerable to mistakes. This can lead to exposure of confidential data and a malware breakout.		
Likelihood	Medium (2)		
Impact On	_X_ Confidentiality _X_ Integrity _X_ Availability		
Impact Area	**Priority**	**Impact**	**Score**
Financial	High (3)	High (3)	9
Productivity	High (3)	High (3)	9
Reputation	High (3)	Low (2)	4
Legal	Low (2)	Low (1)	2
		Impact Score	24
Risk Score (Likelihood x Impact)	48		
Adequacy of Existing Controls	High		
Risk Control Strategy	_X_ Accept _X_ Mitigate __ Share _X_ Defer		
Risk Mitigation Controls			
Anti-Malware and Backups	To protect guest and company data, anti-malware is deployed on all endpoints and backups are taken daily of the VisualOne database to ensure minimal loss of data.		
Security Awareness Training	Every user with email goes through monthly or bi-weekly phishing tests to promote positive security culture.		
Managed Detection and Response	Company recently acquired a MDR solution to assist in detecting potential threats and receiving notifications and coordinated response.		

Vulnerability - Malware	
Asset	Corporate Infrastructure
Asset Importance	HIGH
Threat	Malware and Ransomware
Description	Malware possesses the ability to disrupt business activity and expose confidential information. In the event of ransomware, business operations would be crippled and severely disrupted due to loss of data.
Likelihood	Medium (2)

Impact On	_X_ Confidentiality _X_ Integrity _X_ Availability		
Impact Area	**Priority**	**Impact**	**Score**
Financial	High (3)	High (3)	9
Productivity	High (3)	High (3)	9
Reputation	High (3)	Low (3)	9
Legal	Low (2)	Low (2)	4
		Impact Score	31
Risk Score (Likelihood x Impact)	62		
Adequacy of Existing Controls	High		
Risk Control Strategy	___ Accept _X_ Mitigate ___ Share _X_ Defer		
Risk Mitigation Controls			
Anti-Malware and Backups	To protect guest and company data, anti-malware is deployed on all endpoints and backups are taken daily of the core systems to ensure minimal loss of data.		
Security Awareness Training	Every user with email goes through monthly or bi-weekly phishing tests to promote positive security culture.		
Managed Detection and Response	Company recently acquired a MDR solution to assist in detecting potential threats and receiving notifications and coordinated response.		

Appendix J – Revised Physical Network Diagram