CEDAR DESIGN REPORT

Revision 9

5/29/2023

Group 15: Bilal, Gent, Met, Thomas, Oluwatosin

Table of Contents

1 EXECUTIVE SUMMARY

To address the outdated IT infrastructure at CEDAR's Lombard, Oakbrook, and Waukegan locations, a comprehensive upgrade and overhaul plan has been put together by our team. The primary objectives were to improve operational efficiency, enhance CEDAR’s network security, and provide state-of-the-art hardware and software solutions that are relevant to today’s applications.

Our proposed plan involves replacing obsolete servers with advanced models such as Dell PowerEdge R750x’s and Oracle SPARC T-Series T8-1 rack servers. Lenovo ThinkStation P920 workstations are meant to replace the obsolete workstations currently at all locations. Network connectivity is also upgraded using Cisco ISR4461/K9 routers. Security measures were strengthened through dual-layer firewall configurations with a DMZ, Cisco Catalyst C9300 switch arrays, and the implementation of modern payment processing systems in Lombard.

Physical security was also enhanced by installing CCTV systems, biometric scanners, RFID systems, intrusion alarms, and more. All hardware will undergo thorough installation and testing, and a comprehensive security assessment will be conducted.

The estimated total cost of the implementation is **$5,975,691.36**, covering hardware, software licensing, cabling infrastructure, physical security systems, and other miscellaneous costs. The implementation will go down through a multi-phased approach, beginning with the Oakbrook location, then proceeding to Waukegan, and concluding at Lombard. This strategy minimizes the risk of service disruption. The entire process, from hardware installation to final testing and configuration, will take approximately **6 months**. Throughout the implementation, we will ensure minimal disruption to CEDAR's essential services, prioritizing a smooth transition into their new infrastructure.

We have also ensured that everything within our proposal from start to finish is compliant with NERC CIP. This ensures that no conflict will arise between CEDAR and the regulatory boards. Below you will find our proposed solution.

2 PROPOSED DESIGN CONSIDERATIONS

CEDAR's infrastructure design requires a handful of considerations of CEDAR’s network, physical, and operational aspects. The organization aims to establish an independent network infrastructure, distinct from its parent company, PLUNC, to ensure enhanced security measures. Below is what we had to take into consideration as we designed our proposal.

2.1 Location Setup

CEDAR operates in three distinct locations:

- **Oakbrook and Waukegan**: These locations mirror each other with one acting as a backup location (Waukegan). They house the Power Grid Control Center, comprising of a Solaris server and a Windows server, alongside a dedicated computer room.

- **Lombard**: This site serves as the customer service and repair dispatch center, equipped with standby trucks to promptly address customer needs.

2.2 Critical System Protection

To strengthen CEDAR’s critical systems, particularly the Supervisory Control and Data Acquisition (SCADA) system, comprehensive protection against malware attacks is essential. Notable malware threats, such as Stuxnet, BlackEnergy, and Havex, highlight the need for tight security measures. In 2022, the Department of Energy, FBI, and CISA warned of a specialized malware created by unidentified hackers. This malware allows attackers to scan, compromise, and gain complete control over targeted systems, leveraging vulnerabilities in ASRock motherboard drivers on Windows workstations. Therefore, careful component selection and proactive security tools are imperative.

2.3 System Upgrades

To ensure optimal functionality, the following upgrades are planned:

- **Solaris 10 server**: Considering CEDAR’s request to keep this system as it is. We have chosen to maintain the Solaris 10 server in adherence with CEDAR’s requests but on much newer hardware. The Oracle SPARC T-Series T8-1 rack server is the server that can run Solaris 10.

- **Windows 2008 server**: Upgrade to the latest Windows 2022 server to overcome end-of-life limitations and meet CEDAR's operational and security requirements effectively. The upgrade offers multi-layered security, secure connectivity, virtualization capabilities, and enhanced accessibility for operators.

- **SQL server**: Upgrading from an outdated version to the 2022 SQL server ensures compatibility and reinforces security measures.

- **Workstations**: Currently running on the obsolete Windows XP Pro, an upgrade to the latest Windows 11 OS is vital. This upgrade ensures compliance with the latest security updates and harnesses the advanced features available in the market.

- **Customer Relation Management (CRM) system:** Replacing the existing custom CRM with Microsoft Dynamics 365, an all-encompassing suite of business tools, ensures seamless compatibility and enhances customer relationship management capabilities.

2.4 Access Control Considerations

To safeguard data and physical resources, robust access control measures are paramount. Access control encompasses two key aspects:

- **Physical access control**: Implementing a comprehensive set of measures to secure operational locations, including locks, keys, employee access cards, biometric authentication, security personnel, surveillance systems, and environmental controls (e.g., temperature and humidity regulation). These measures are particularly crucial for rooms housing the SCADA system, ensuring optimal performance under ideal conditions.

- **Technical access control**: Deploying a range of security structures, such as Next-Generation Antivirus (NGAV), Endpoint Detection and Response (EDR), Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and Security Information and Event Management (SIEM) tools across all identified technical assets. Moreover, implementing discretionary, role-based, rule-based, and time-based access control mechanisms strengthens security layers and restricts unauthorized access, ensuring controlled information dissemination on a need-to-know basis.

By implementing comprehensive access control measures, CEDAR strives to protect its infrastructure from external threats and potential exploitation.

With these enhancements, CEDAR's infrastructure design prioritizes security, functionality, and efficiency, paving the way for seamless operations across its locations while mitigating potential risks.

3 WAN TOPOLOGY OVERVIEW

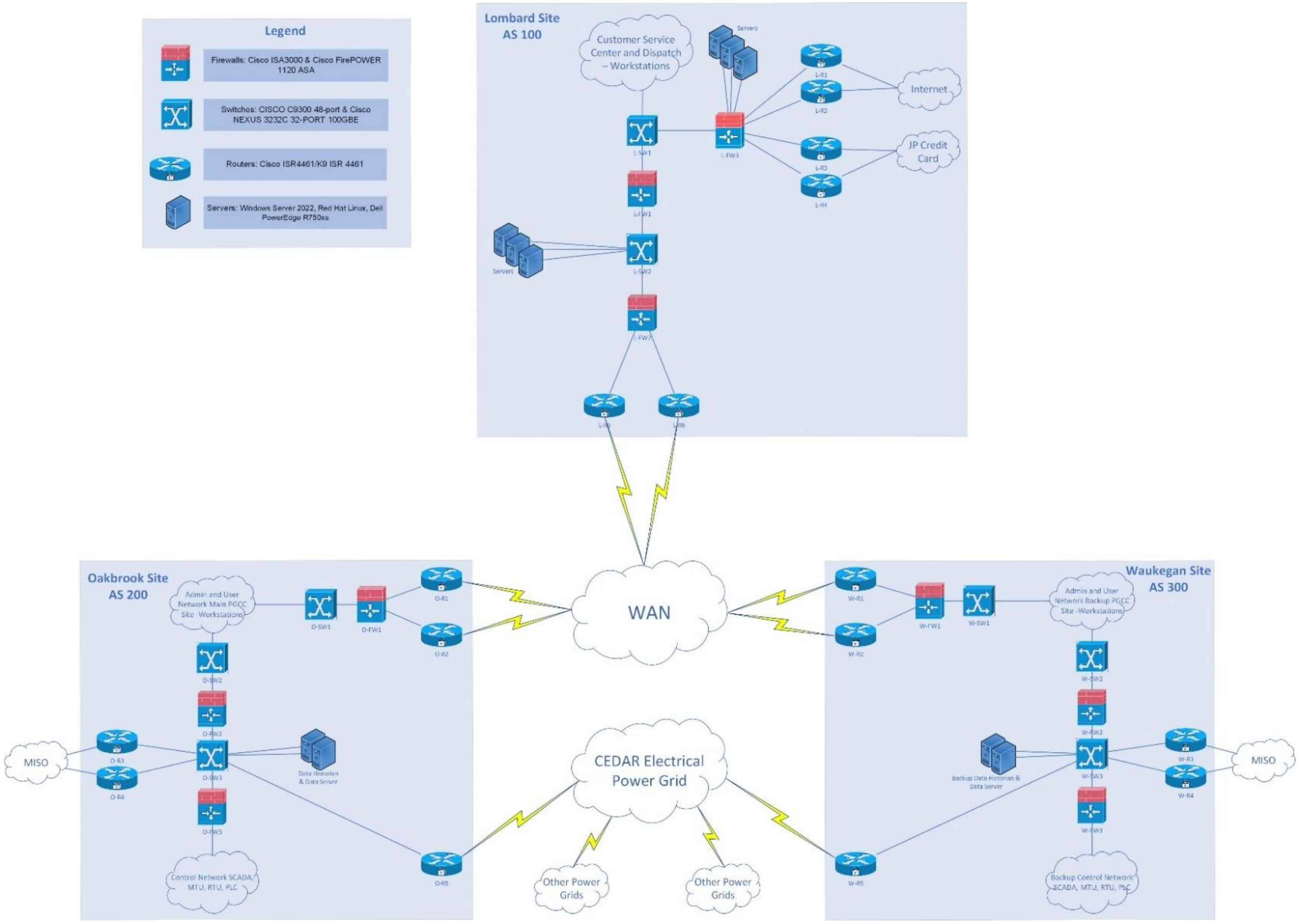

Legend
Firewalls: Cisco ISA3000 & Cisco FirePOWER 1120 ASA
Switches: CISCO C9300 48-port & Cisco NEXUS 3232C 32-PORT 100GBE
Routers: Cisco ISR4461/K9 ISR 4461
Servers: Windows Server 2022, Red Hat Linux, Dell PowerEdge R750xs
Lombard Site
AS 100
Customer Service Center and Dispatch – Workstations
Servers
L-R1
L-R2
Internet
L-SW1
L-FW3
L-R3
L-R4
JP Credit Card
L-FW1
Servers
L-SW2
L-FW2
L-R5
L-R6
WAN
Oakbrook Site
AS 200
Admin and User Network Main PGCC Site Workstations
O-SW1
O-FW1
O-R1
O-R2
O-SW2
O-FW2
MISO
O-R3
O-R4
O-SW3
Data Historian & Data Server
O-FW3
Control Network SCADA, MTU, RTU, PLC
O-R5
CEDAR Electrical Power Grid
Other Power Grids
Other Power Grids
Waukegan Site
AS 300
W-R1
W-R2
W-FW1
W-SW1
Admin and User Network Backup PGCC Site -Workstations
W-SW2
W-FW2
Backup Data Historian & Data Server
W-SW3
W-R3
W-R4
MISO
W-FW3
W-R5
Backup Control Network SCADA, MTU, RTU, PLC

FIGURE 1: CEDAR WAN TOPOLOGY

3.1 Routing Protocols

Border Gateway Protocol will be used as the primary protocol for routing traffic between the Oakbrook, Waukegan, and Lombard Autonomous Systems. The two variants of BGP we will use are:

- **eBGP**: External BGP will be used to routing between different sites. This will allow each CEDAR site to communicate with one another. Each will have their own AS number such as Lombard will have AS #100, Oakbrook will have AS #200, and Waukegan will have AS #300.
- **iBGP**: Internal BGP will be used for communication within a single AS. Therefore, routing information and maintaining network consistency will be done by iBGP.

4 IP ADDRESSING

Below, you will find our IP addressing scheme for each CEDAR location:

4.1 Oakbrook

TABLE 1: OAKBROOK IP ADDRESSING

Device	IP Address Block	Description
R1, R2 ⟶ WAN	128.1.1.0/29	R1 and R2 WAN
R3, R4 ⟶ MISO	128.1.1.8/29	R3 and R4 to MISO
R5 ⟶ CEDAR Electrical Grid	128.1.1.16/29	R5 to CEDAR Electrical Grid
FW1 ⟶ R1, R2	192.168.2.0/29	FW1 to R1 and R2
FW1 ⟵⟶ FW2	192.168.1.1 - 192.168.1.2	FW1 to FW2
⟶ 60 Workstations	192.168.1.1/24	Employee Workstations
DMZ (FW2 ⟵⟶ FW3)	192.168.2.32/27	
⟶ Microsoft/SQL Server	192.168.2.33	
⟶ Solaris Server	192.168.2.34	
⟶ Ivanti Patch Management Server	192.168.2.35	
⟶ Logging Server	192.168.2.36	
⟶ Varonis Server	192.168.2.37	
⟶ DHCP Server	192.168.2.38	
⟶ AD DS Server	192.168.2.39	
⟶ Centralized Video Recording Server	192.168.2.40	
FW3 → Control Network	192.168.3.0/24	For the use of PLCs

4.2 Waukegan

TABLE 2: WAUKEGAN IP ADDRESSING

Device	IP Address Block	Description
R1, R2 → WAN	128.1.1.24/29	R1 and R2 WAN
R3, R4 → MISO	128.1.1.32/29	R3 and R4 to MISO
R5 → CEDAR Electrical Grid	128.1.1.40/29	R5 to CEDAR Electrical Grid
FW1 → R1, R2	192.168.2.0/29	FW1 to R1 and R2
FW1 ←→ FW2	192.168.1.1 - 192.168.1.2	FW1 to FW2
→ 60 Workstations	192.168.1.1/24	DHCP
DMZ (FW2 ←→ FW3)	192.168.2.32/27	
→ Microsoft/SQL Server	192.168.2.33	
→ Solaris Server	192.168.2.34	
→ Ivanti Patch Management Server	192.168.2.35	
→ Logging Server	192.168.2.36	
→ Varonis Server	192.168.2.37	
→ DHCP Server	192.168.2.38	
→ AD DS Server	192.168.2.39	
→ Centralized Video Recording Server	192.168.2.40	
FW3 → Control Network	192.168.3.0/24	

4.3 Lombard

TABLE 3: LOMBARD IP ADDRESSING

Device	IP Address Block	Description
R1 & R2 ⟶ Internet	128.1.1.48/29	R1 and R2 to Internet
R3 & R4 ⟶ JP Credit Card	128.1.1.56/29	R3 and R4 to JP Credit Card
R5 & R6 ⟶ WAN	128.1.1.64/29	R5 and R6 to WAN
DMZ (FW2 ⟵⟶ FW1)	192.168.2.0/28	
⟶ Logging Server	192.168.2.1	
⟶ Varonis Server	192.168.2.2	
⟶ Ivanti Patch Management Server	192.168.2.3	
⟶ Email Server	192.168.2.4	
⟶ File/Print Sharing Server	192.168.2.5	
DMZ (FW1 ⟵⟶ FW3)		
⟶ 150 PC's	192.168.1.0/24	Employee Workstations
⟶ DHCP Server	192.168.3.1	
⟶ AD DS Server	192.168.3.2	
⟶ Credit Card Server	192.168.3.3	
⟶ 3 x CRM Windows 2022 Server	192.168.3.4, 192.168.3.5, 192.168.3.6	
⟶ Red Hat Web Server	192.168.3.7	
⟶ Centralized Video Recording Server	192.168.3.8	
R3 & R4 ⟶ JP Credit Card	128.1.1.56/29	R3 and R4 to JP Credit Card
R5 & R6 ⟶ WAN	128.1.1.64/29	R5 and R6 to WAN

5 OAKBROOK – MAIN PGCC

The Oakbrook location houses the main control center for the electrical grid, responsible for primary electric outputs in the Chicagoland area. It has a power grid controller center, considered an asset for CEDAR. Operators will access the grid application and communicate with the new Oracle Solaris server.

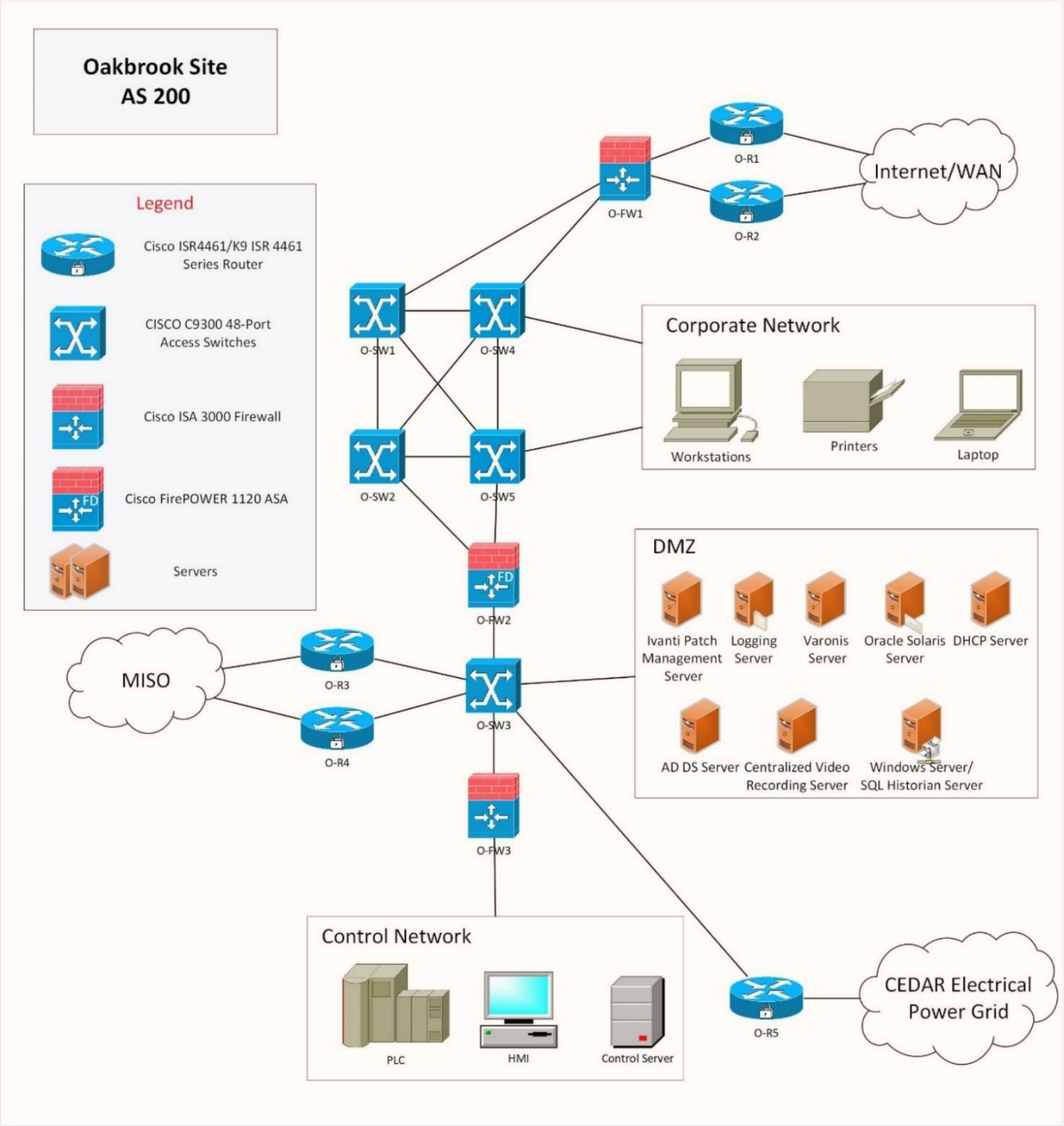


FIGURE 2: OAKBROOK LOGICAL TOPOLOGY

5.1 Servers

All the servers are Dell PowerEdge R750xs rack servers except for the Solaris Server which will be a SPARC T-Series T8-1 rack server. The SPARC server is the most up-to-date server that can run Solaris 10. At Oakbrook, we have 8 total servers:

TABLE 4: OAKBROOK SERVERS

Server	Description	Count
Ivanti Patch Management Server	Automated Patch Management	1
Centralized Logging Server	Log Data Storage	1
Varonis Server	Data Protection	1
Oracle Solaris Server	Runs SCADA Software	1
DHCP Server	Site Dynamic IP Configuration	1
AD/DS Server	User Access Management	1
Video Recording Server	Surveillance Footage Storage	1
Windows Server/SQL Historian Server	Data Archiving and Historian	1

5.2 Switches

CEDAR did not have any switches present in any of their locations prior. We have added switches for improved security, scalability, and overall better performance. We chose to use the catalyst C9300 switches because of its redundant hardware (fans and power supplies), built-in intrusion detection and prevention systems, anti-DDOS protection, easy management, and its ability to work with our security cameras. The switches are connected to the Solaris server and firewalls. We have 5 total switches at Oakbrook, all of them being CISCO C9300 48-Port Access Switches.

5.3 Workstations

We have replaced 60 workstations with Lenovo ThinkStation P920 running Windows 11 and HMI application. These workstations have better hardware than what CEDAR currently has and will be easier for CEDAR staff to work with them.

5.4 Routers

We chose Cisco ISR4461/K9 ISR 4461 Series routers due to their enhanced security and optimized network traffic, IDS/IPS systems, support for encryption, scalability, and performance. At Oakbrook, we have 5 total routers:

- 2 Cisco ISR4461/K9 ISR 4461 routers for WAN connection to other CEDAR locations.
- 2 Cisco ISR4461/K9 ISR 4461 routers for MISO power grid information transmission.
- 1 ISR 4461 router for connection to electrical grid.

5.5 Firewalls

We decided to choose two different models of firewalls in an effort to have better security in the event one of the models has any sort of vulnerabilities. Each firewall has enhanced security, redundancy, failover capabilities, performance, and scalability. They also have improved network security with built-in intrusion prevention and rule-based traffic blocking. Firewalls are configured in a dual layer configuration with DMZs. At Oakbrook, we have 3 firewalls:

- 2 Cisco ISA3000
- 1 Cisco FirePOWER 1120 ASA

5.6 Software

The software used amongst the servers at this location includes Varonis, Ivanti, EventLog Management, and Crowdstrike. Varonis helps organizations protect and manage their valuable data by monitoring and analyzing how that data is accessed and shared across the network. It will be utilized to make sure that the right people have access to CEDAR’s data, especially pertaining to customer data. It will also be used for monitoring. Ivanti is a patch management software, which makes sure that all the programs and software on all of CEDAR’s devices are up to date and don’t have any vulnerabilities. EventLog Mangement is a tool used to collect, analyze, and manage event logs generated by various systems and applications within CEDAR. All logs collected will be stored on the logging server. Crowdstrike Endpoint Protection is software that provides endpoint protection, threat detection, and threat response for all devices within CEDAR. This software will be installed on every endpoint within CEDAR.

5.7 Physical Security

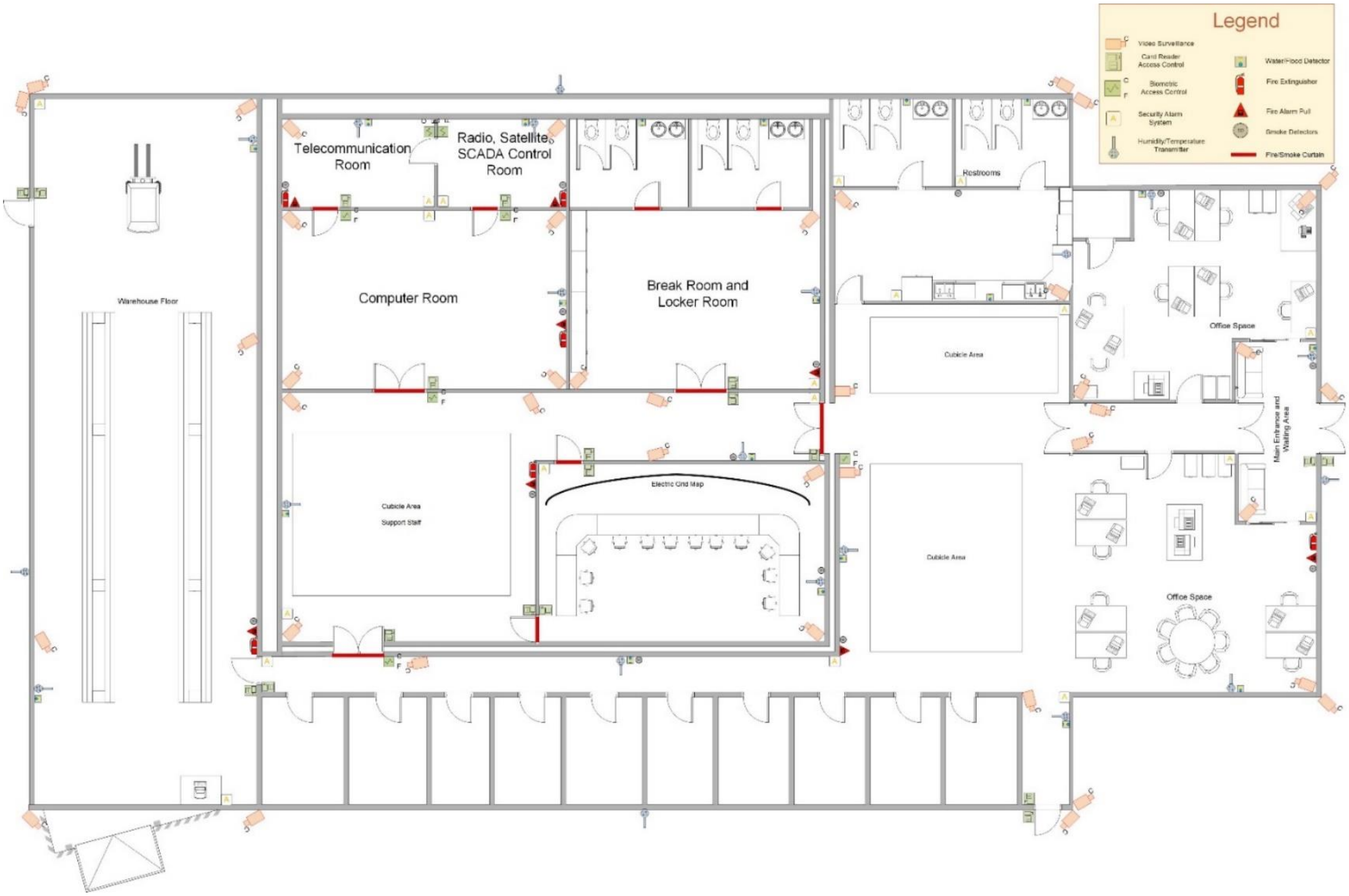


FIGURE 3: OAKBROOK PHYSICAL TOPOLOGY

Oakbrook is CEDAR’s most important location since the main PGCC is located at Oakbrook. Due to that, we have taken high physical security measures:

- **Video Surveillance:** The building is heavily equipped with cameras on the interior and exterior. Each part of the building is being monitored by cameras so no threat actor can go in a specific room without being detected. These video surveillance cameras will serve as a deterrent as well as detection security measure.
- **Card Reader/Biometric Access Controls**: We have implemented access controls in each room of the building. In the control center rooms we have implemented biometric access controls where employees who enter need to provide biometric identification, pin/password, and bypass a card reader. This way, we can make sure no-one enters a room they shouldn’t. Biometric access controls have been mainly put in important rooms such as control rooms, computer rooms, and so on.

- **Security Alarm Systems**: We also have implemented alarm systems so in case of a breach, the alarm system will turn on and alert everyone in the building.
- **Humidity/Temperature Transmitters:** The building is equipped with humidity/temperature transmitters on the interior and exterior. They will help CEDAR operators have a full understanding of humidity/temperature levels in each room; therefore, giving them the ability to monitor suspicious rises of temperature levels and respond swiftly. For example, if the temperature levels rise in the telecommunication room, CEDAR staff will notice that immediately and can take appropriate action.
- **Water and Flood Detectors**: The Oakbrook building has been equipped with water and flood detectors. These detectors will be essential in detecting and preventing water-related incidents such as leaks, pipe bursts, or floods. Each room of the control center does have a water/flood detector as well as other parts of the Oakbrook building.
- **Smoke Detectors**: Smoke detectors have been implemented at the Oakbrook location to detect smoke and take immediate action in case of a fire.
- **Fire Extinguishers**: Fire extinguishers will be present in the building so CEDAR staff can take immediate action in case of a small fire and not let it spread to other sensitive areas of Oakbrook building.
- **Fire Alarm Pulls**: Fire alarm pulls will also be present so in case of a fire, CEDAR employees can use these fire alarm pulls to allow immediate activation of the security alarm system.
- **Fire and Smoke Curtains**: These curtains will be present at each door of the control room, so the smoke and fire is contained, and other equipment is protected. For example, in case of a fire on the telecommunication room, fire/smoke curtains will be dropped when an employee pulls the switch, and the fire/smoke will be contained in that room for a long enough period so emergency procedures can take place.

5.8 Rack Diagrams

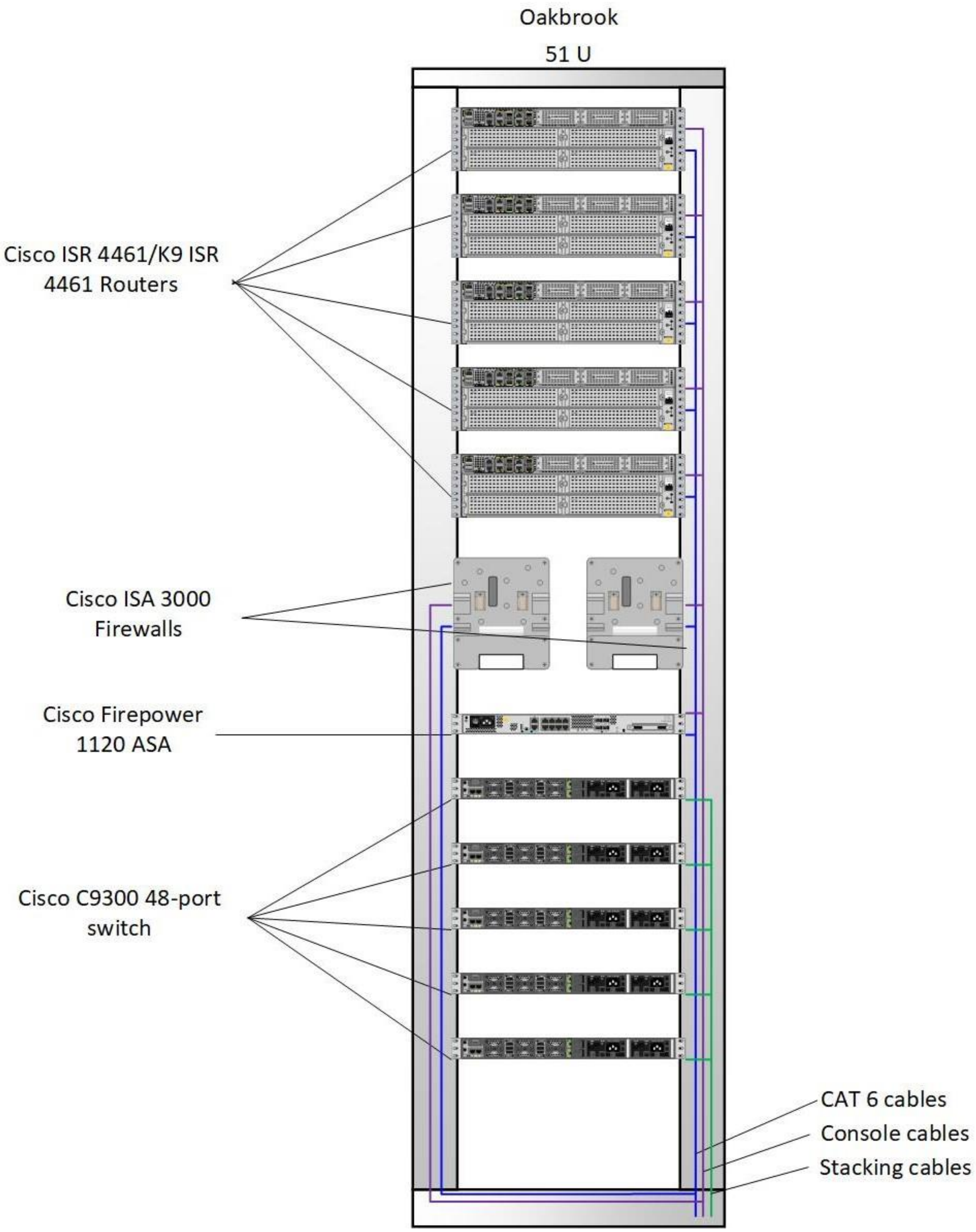


FIGURE 4: OAKBROOK RACK 1

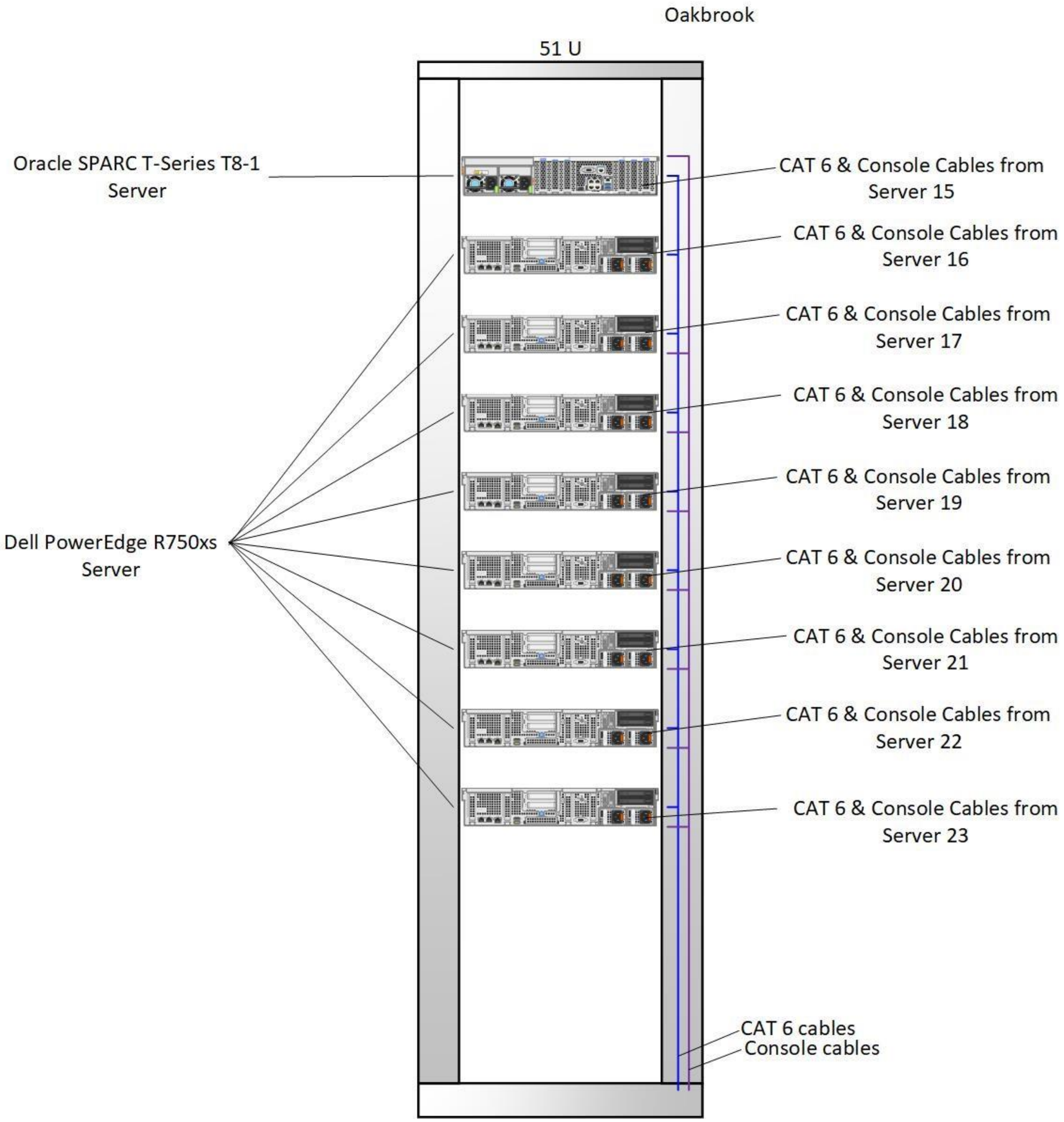

Oakbrook
51 U
Oracle SPARC T-Series T8-1 Server
Dell PowerEdge R750xs Server
CAT 6 & Console Cables from Server 15
CAT 6 & Console Cables from Server 16
CAT 6 & Console Cables from Server 17
CAT 6 & Console Cables from Server 18
CAT 6 & Console Cables from Server 19
CAT 6 & Console Cables from Server 20
CAT 6 & Console Cables from Server 21
CAT 6 & Console Cables from Server 22
CAT 6 & Console Cables from Server 23
CAT 6 cables
Console cables

FIGURE 5: OAKBROOK RACK 2

6 WAUKEGAN – BACKUP PGCC

The Waukegan location houses the backup control center for the electrical grid in the event that the Oakbrook location goes down. The design and hardware of this location is exactly the same as the one located in Oakbrook. It has the power grid controller center, considered an asset for CEDAR. Operators will access the grid application and communicate with the new Oracle Solaris server.

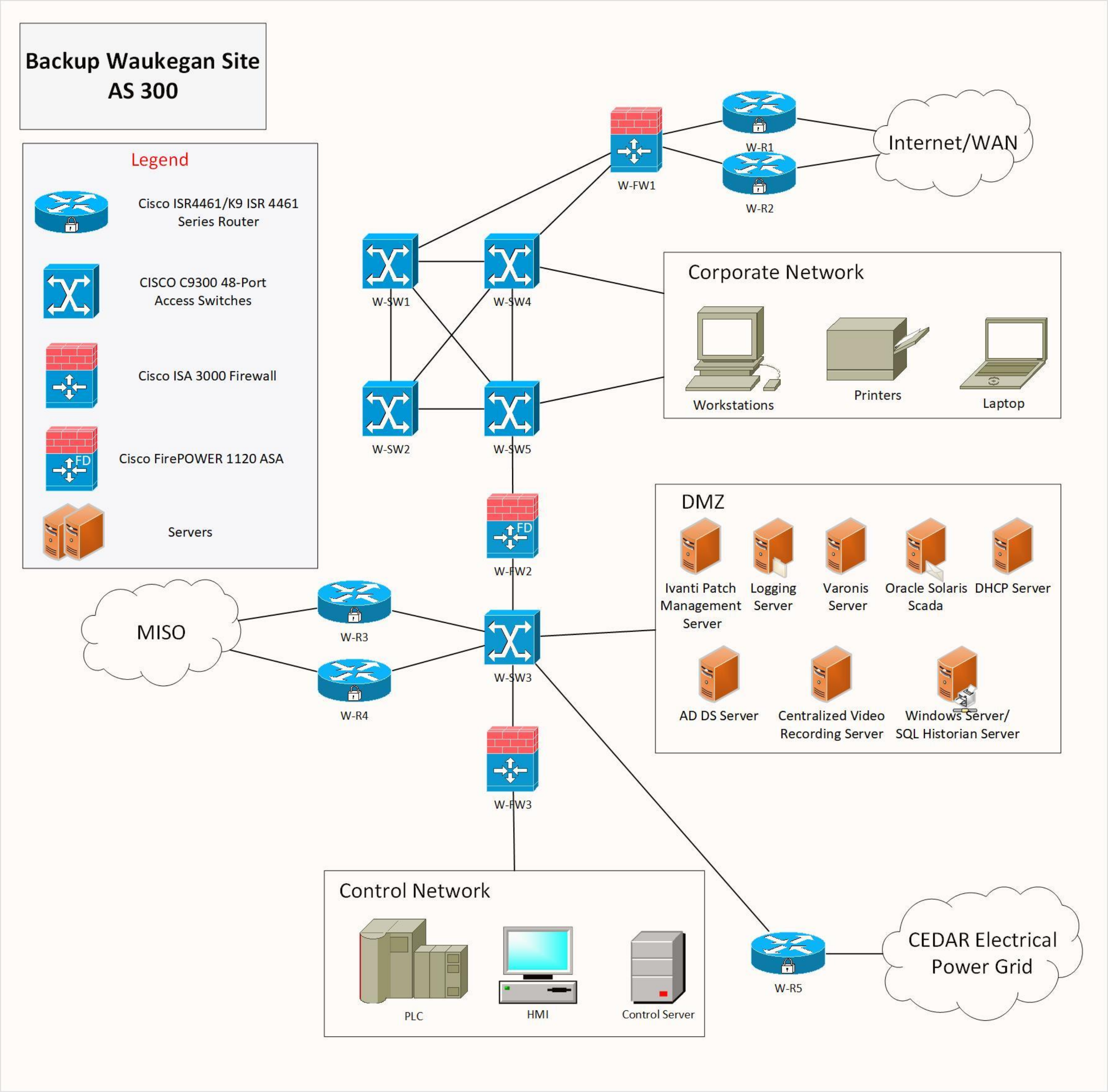


FIGURE 6: WAUKEGAN LOGICAL TOPOLOGY

6.1 Servers

All the servers are Dell PowerEdge R750xs rack servers except for the Solaris Server which will be a SPARC T-Series T8-1 rack server.

TABLE 5: WAUKEGAN SERVERS

Server	Description	Count
Ivanti Patch Management Server	Automated Patch Management	1
Centralized Logging Server	Log Data Storage	1
Varonis Server	Data Protection	1
Oracle Solaris Server	Runs SCADA Software	1
DHCP Server	Site Dynamic IP Configuration	1
AD/DS Server	User Access Management	1
Video Recording Server	Surveillance Footage Storage	1
Windows Server/SQL Historian Server	Data Archiving and Historian	1

6.2 Switches

CEDAR did not have any switches present in any of their locations prior. We have added switches for improved security, scalability, and overall better performance. We chose to use the catalyst C9300 switches because of its redundant hardware (fans and power supplies), built-in intrusion detection and prevention systems, anti-DDOS protection, easy management, and its ability to work with our security cameras. The switches are connected to Solaris servers and firewalls. We have 5 total switches at Waukegan, all of them being CISCO C9300 48-Port Access Switches.

6.3 Workstations

We have replaced 20 workstations with Lenovo ThinkStation P920 running Windows 11 and HMI application.

6.4 Routers

We chose Cisco ISR4461/K9 ISR 4461 Series routers due to their enhanced security and optimized network traffic, IDS/IPS systems, support for encryption, scalability, and performance. At Waukegan, we have 5 total routers:

- 2 Cisco ISR4461/K9 ISR 4461 routers for WAN connection to other CEDAR locations.
- 2 Cisco ISR4461/K9 ISR 4461 routers for MISO power grid information transmission.
- 1 ISR 4461 router for connection to electrical grid.

6.5 Firewalls

We decided to choose two different models of firewalls to have better security in the event one of the models has any sort of vulnerabilities. Each firewall has enhanced security, redundancy, failover capabilities, performance, and scalability. They also have improved network security with built-in intrusion prevention and rule-based traffic blocking. Firewalls are implemented in a dual layer configuration with DMZs. We have 3 firewalls at Waukegan:

- 2 Cisco ISA3000
- 1 Cisco FirePOWER 1120 ASA

6.6 Software

The software used amongst the servers at this location includes Varonis, Ivanti, EventLog Management, and Crowdstrike. Varonis helps organizations protect and manage their valuable data by monitoring and analyzing how that data is accessed and shared across the network. It will be utilized to make sure that the right people have access to CEDAR’s data, especially pertaining to customer data. It will also be used for monitoring. Ivanti is a patch management software, which makes sure that all the programs and software on all of CEDAR’s devices are up to date and don’t have any vulnerabilities. EventLog Mangement is a tool used to collect, analyze, and manage event logs generated by various systems and applications within CEDAR. All logs collected will be stored on the logging server. Crowdstrike Endpoint Protection is software that provides endpoint protection, threat detection, and threat response for all devices within CEDAR. This software will be installed on every endpoint within CEDAR.

6.7 Physical Security

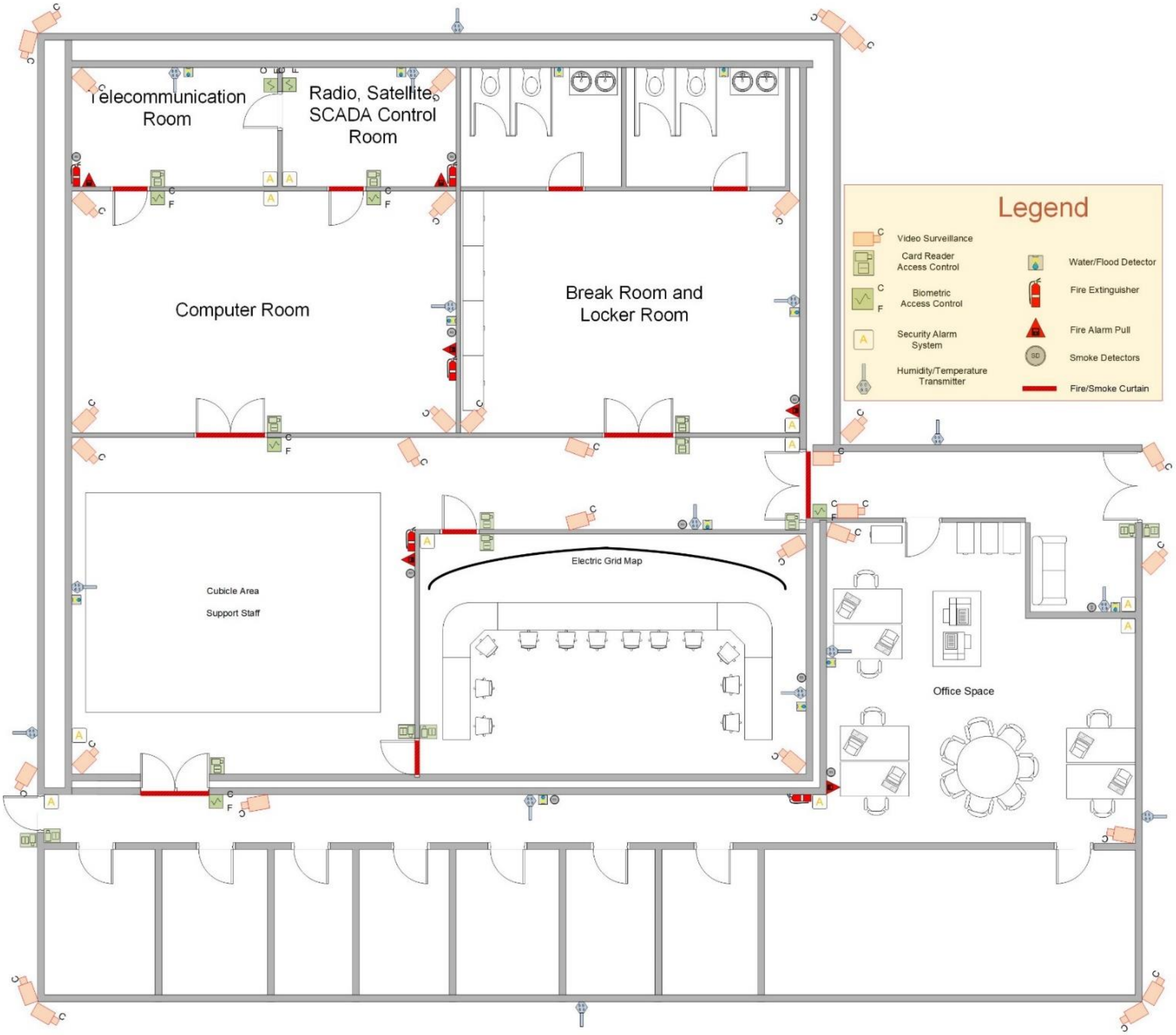


FIGURE 7: WAUKEGAN PHYISCAL TOPOLOGY

Waukegan is the backup PGCC location of CEDAR. This location also needs to be heavily secured at the same level as Oakbrook. At Waukegan, we have also taken high physical security measures:

- **Video Surveillance:** There are numerous cameras both inside and outside of the building. Cameras are placed throughout the building to ensure that no threat actor can enter a particular room without being noticed. Both a deterrent and a detection security measure will be provided by these video surveillance cameras.

- **Card Reader/Biometric Access Controls**: At every room throughout the building, access controls have been put in place. In the control center rooms we have implemented biometric access controls where employees who go into need to provide biometric identification, pin/password, and bypass a card reader. We can ensure that nobody enters a room they shouldn't on this basis. Most key areas, such control rooms and computer rooms, have biometric access restrictions installed.
- **Security Alarm Systems**: We also installed alarm systems, which will activate in the event of a breach and notify everyone inside the building.
- **Humidity/Temperature Transmitters:** On the inside and outside of the building are transmitters for humidity and temperature. They will aid CEDAR operators in fully comprehending the humidity/temperature levels in each room, enabling them to watch for suspicious temperature rises and act quickly. For instance, CEDAR workers will be alert and able to respond instantly if the temperature in the telecommunications room starts to increase.
- **Water and Flood Detectors**: Water and flood detectors have been installed in the Waukegan building. These detectors will be crucial in identifying and stopping incidents involving water, such as leaks, burst pipes, and floods. There are water/flood detectors in every room of the control center and throughout the Waukegan building.
- **Smoke Detectors**: To detect smoke and act quickly in the event of a fire, smoke detectors have been installed at the Waukegan building.
- **Fire Extinguishers**: There will be fire extinguishers in the building so CEDAR staff can put out a minor fire right away and prevent it from spreading to other sensitive areas of the Waukegan building.
- **Fire Alarm Pulls**: Additionally, fire alarm pulls will be available so that CEDAR staff members can use them in the event of a fire to enable prompt activation of the security alarm system.
- **Fire and Smoke Curtains**: At the control room's doors, there will be fire/smoke curtains to keep the fire and smoke under control and safeguard other power grid equipment. For instance, if a fire breaks out in the telecommunications room, fire/smoke curtains will be opened when a worker flips a switch, keeping the fire/smoke isolated in that space for long enough for emergency measures to be carried out.

6.8 Rack Diagrams

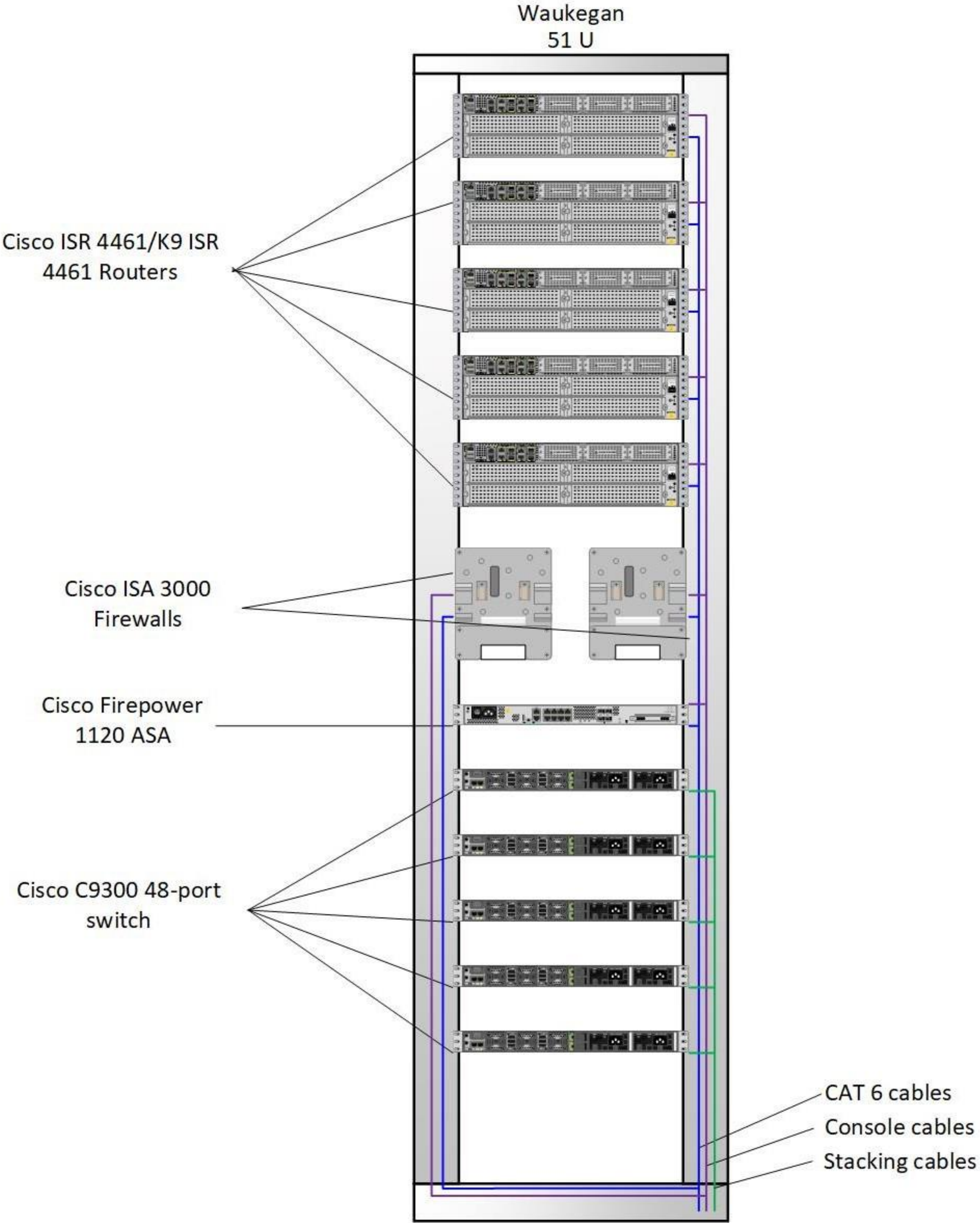


FIGURE 8: WAUKEGAN RACK 1

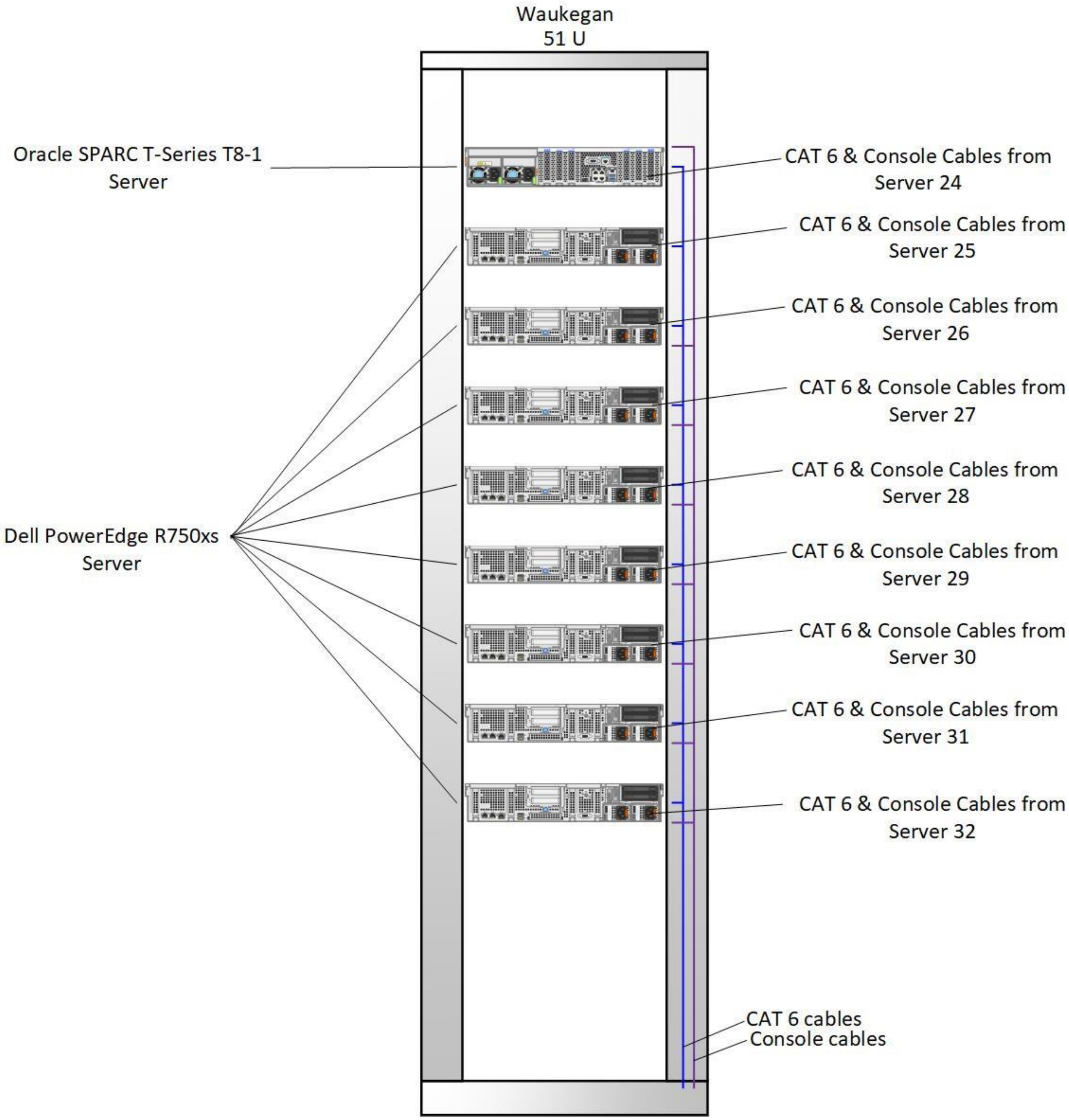

Waukegan
51 U
Oracle SPARC T-Series T8-1 Server
Dell PowerEdge R750xs Server
CAT 6 & Console Cables from Server 24
CAT 6 & Console Cables from Server 25
CAT 6 & Console Cables from Server 26
CAT 6 & Console Cables from Server 27
CAT 6 & Console Cables from Server 28
CAT 6 & Console Cables from Server 29
CAT 6 & Console Cables from Server 30
CAT 6 & Console Cables from Server 31
CAT 6 & Console Cables from Server 32
CAT 6 cables
Console cables

FIGURE 9: WAUKEGAN RACK 2

7 LOMBARD – DATA CENTER

The Lombard location is the largest, housing customer service center and repair dispatch team. The work trucks will be equipped with mobile hotspots for the service team to use.

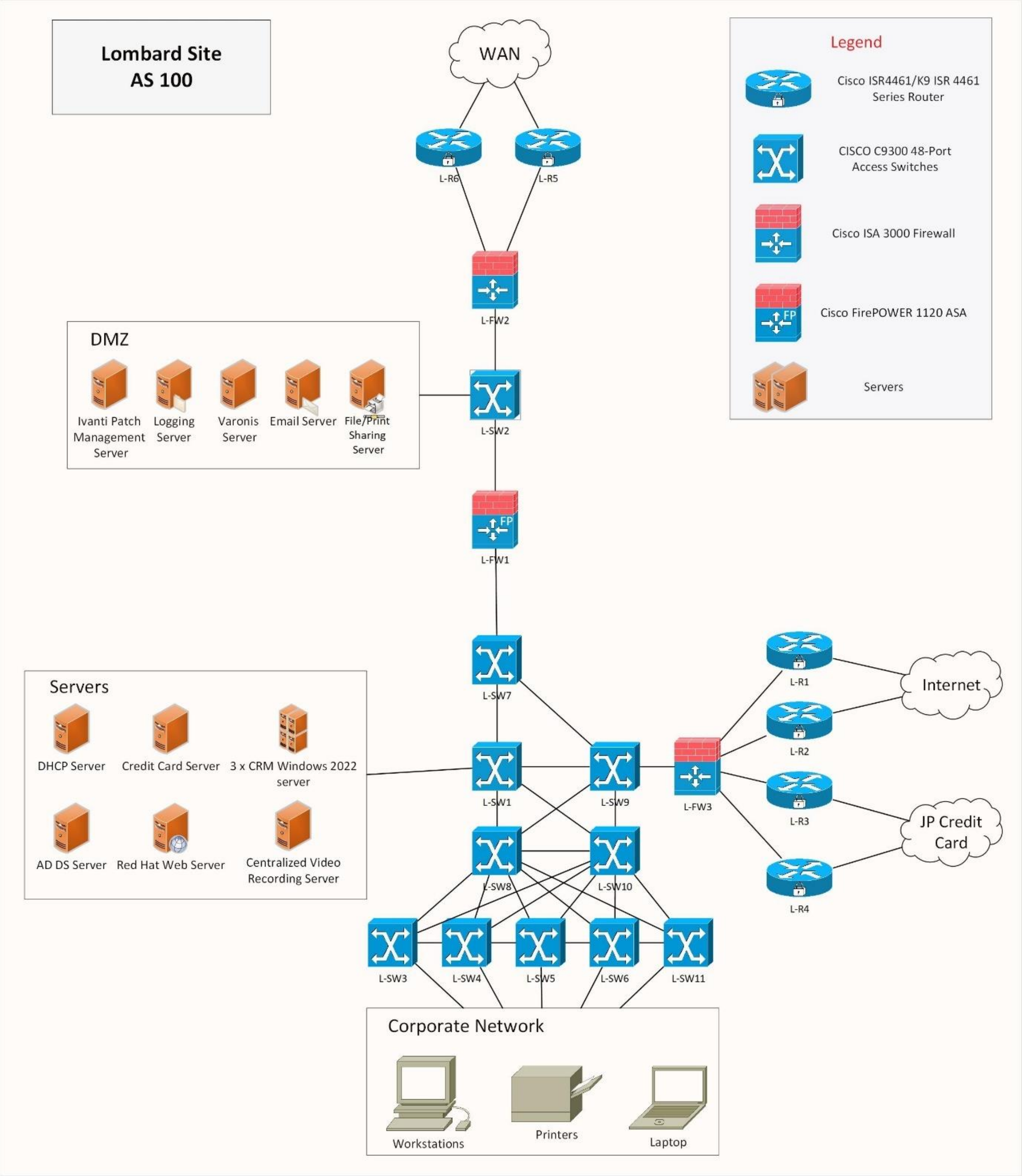


FIGURE 10: LOMBARD LOGICAL TOPOLOGY

7.1 Servers

The servers have been upgraded to Dell PowerEdge R750xs. We have a total of 13 servers at Lombard Data Center:

TABLE 6: LOMBARD SERVERS

Server	Description	Count
CRM System	Customer Relationship Management service	3
DHCP Server	Site Dynamic IP Configuration	1
AD/DS Server	User Access Management	1
Credit Card Server	Payment Authorizations	1
Red Hat Web Server	Forward Facing Web Server	1
Centralized Video Recording Server	Surveillance Footage Storage	1
Ivanti Patch Management Server	Automated Patch Management	1
Centralized Logging Server	Log Data Storage	1
Varonis Server	Data Protection	1
Email Server	Email Services	1
File/Print Sharing Server	Storing and Sharing Files	1

7.2 Switches

CEDAR did not have any switches present in any of their locations prior. We have added switches for improved security, scalability, and overall better performance. We chose to use the catalyst C9300 switches because of its redundant hardware (fans and power supplies), built-in intrusion detection and prevention systems, anti-DDOS protection, easy management, and its ability to work with our security cameras. We have a total of 11 switches at Lombard, all of them being CISCO C9300 48-port access switches.

Spanning Tree Protocol (STP) has been implemented at the switches located in Lombard Data Center. By implementing STP, we have taken a step towards ensuring network reliability and preventing loop within the network infrastructure.

7.3 Workstations

We have replaced 150 Windows XP workstations with Lenovo ThinkStation P920 running Windows 11 for customer service. Furthermore, we have provided 100 mobile support staff with Dell Latitude 5430 rugged laptops running Windows 11.

7.4 Routers

We chose Cisco ISR4461/K9 ISR 4461 Series routers due to their enhanced security and optimized network traffic, IDS/IPS systems, support for encrpytion, scalability, and performance. We have implemented 6 Cisco ISR4461/K9 ISR 4461 Series routers for redundant internet connection.

- 2 Routers for WAN Connectivity
- 2 Routers for Internet Connection
- 2 Routers for JP Credit Card Clearing
    - Responsible for payment processing with a T1 connection to JP Credit Card Clearing.

7.5 Firewalls

We decided to choose two different models of firewalls in an effort to have better security in the event one of the models has any sort of vulnerabilities. Each firewall has enhanced security, redundancy, failover capabilities, performance, and scalability. They also have improved network security with built-in intrusion prevention and rule-based traffic blocking. Firewalls in a dual layer configuration with DMZs. There is DMC connection to routers, JP Credit Card Clearing, and Internet/WAN routers. We have 3 firewalls at Lombard:

- 2 Cisco ISA3000
- 1 Cisco FirePOWER 1120 ASA

7.6 Physical Security

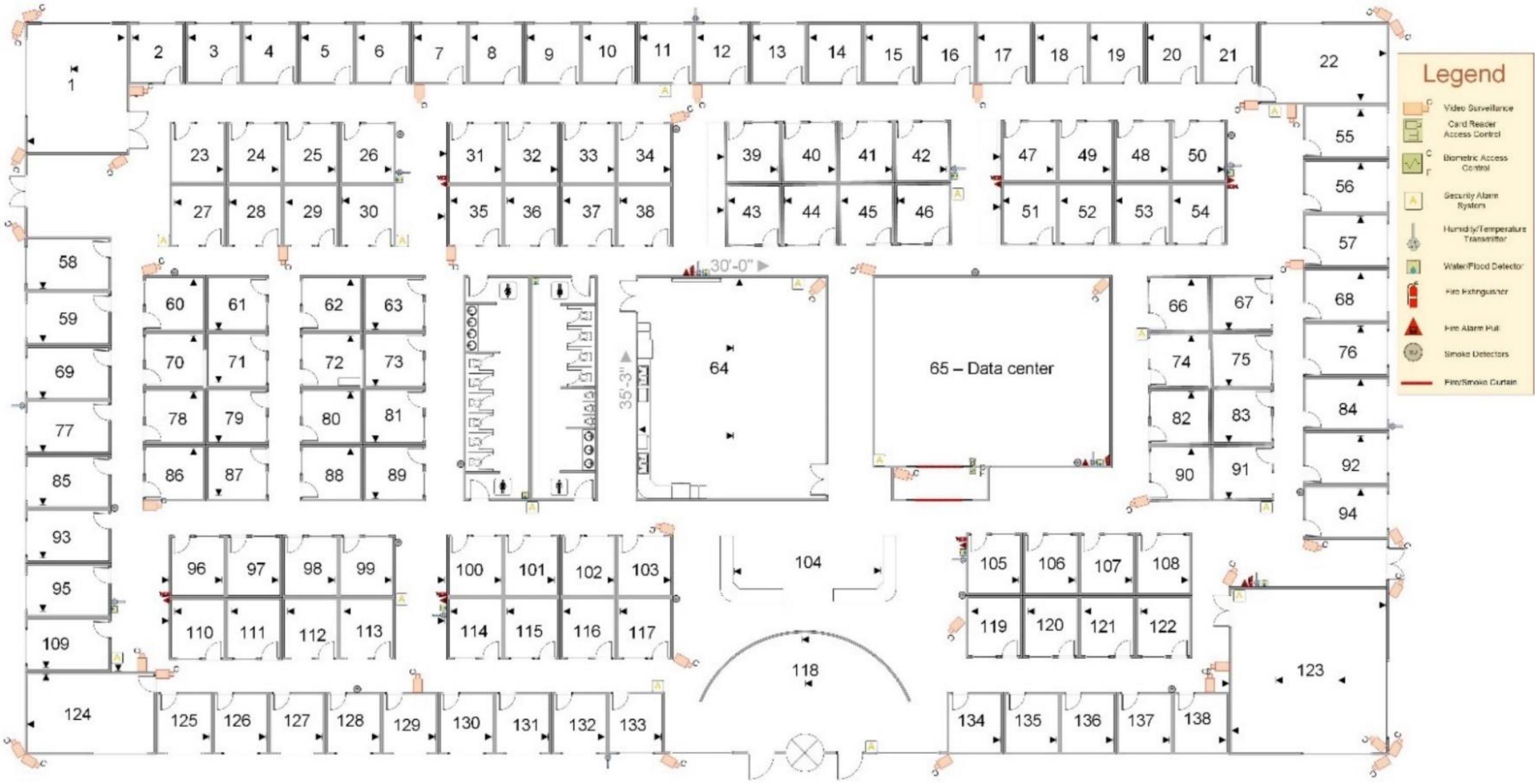


FIGURE 11: LOMBARD PHYSICAL TOPOLOGY

High security measures will be implemented at the Lombard data center. These will include:

- **Video Surveillance:** Numerous cameras have been installed both inside and outside the Lombard building. No threat actor will be able to go inside/outside the building without being detected.
- **Card Reader/Biometric Access Controls**: Access controls have been put in place to make sure no unauthorized entry is done to the data center.
- **Security Alarm Systems**: An alarm system has been implemented which will be activated in the event of a breach and alert everyone in the building.
- **Humidity/Temperature Transmitters:** These transmitters will monitor humidity/temperature levels so CEDAR operators can take immediate action in case of humidity/temperature levels being too low or too high.
- **Water and Flood Detectors**: These detectors will protect the Lombard center from water-related incidents by notifying CEDAR staff in case of an incident.
- **Smoke Detectors**: Will detect smoke and alert the whole building so CEDAR staff can take swift action.
- **Fire Extinguishers**: Fire extinguishers will be provided so CEDAR staff can take immediate action against small fires.

- **Fire Alarm Pulls**: Fire alarm pulls will be available so that CEDAR employees can use them in an event of a fire and alert the whole building.
- **Fire and Smoke Curtains**: These will be installed mainly in the data center room, so the fire doesn't spread inside or outside of it. 7.7 Software

7.7 Software

The software used amongst the servers at this location includes Varonis, Ivanti, EventLog Management, and Crowdstrike. Varonis helps organizations protect and manage their valuable data by monitoring and analyzing how that data is accessed and shared across the network. It will be utilized to make sure that the right people have access to CEDAR's data, especially pertaining to customer data. It will also be used for monitoring. Ivanti is a patch management software, which makes sure that all the programs and software on all of CEDAR's devices are up to date and don't have any vulnerabilities. EventLog Mangement is a tool used to collect, analyze, and manage event logs generated by various systems and applications within CEDAR. All logs collected will be stored on the logging server. Crowdstrike Endpoint Protection is software that provides endpoint protection, threat detection, and threat response for all devices within CEDAR. This software will be installed on every endpoint within CEDAR.

7.8 Rack Diagrams

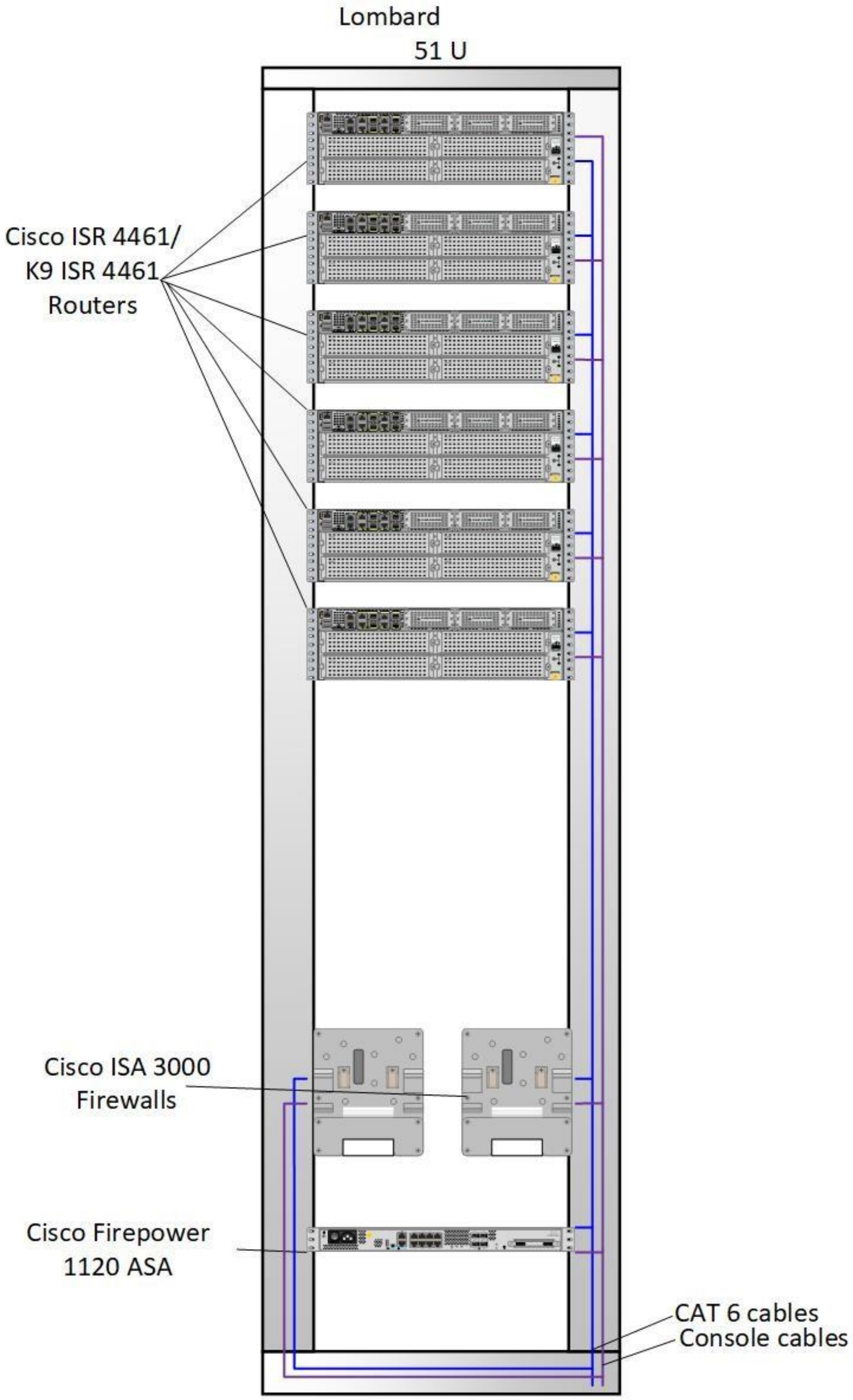


FIGURE 12: LOMBARD RACK 1

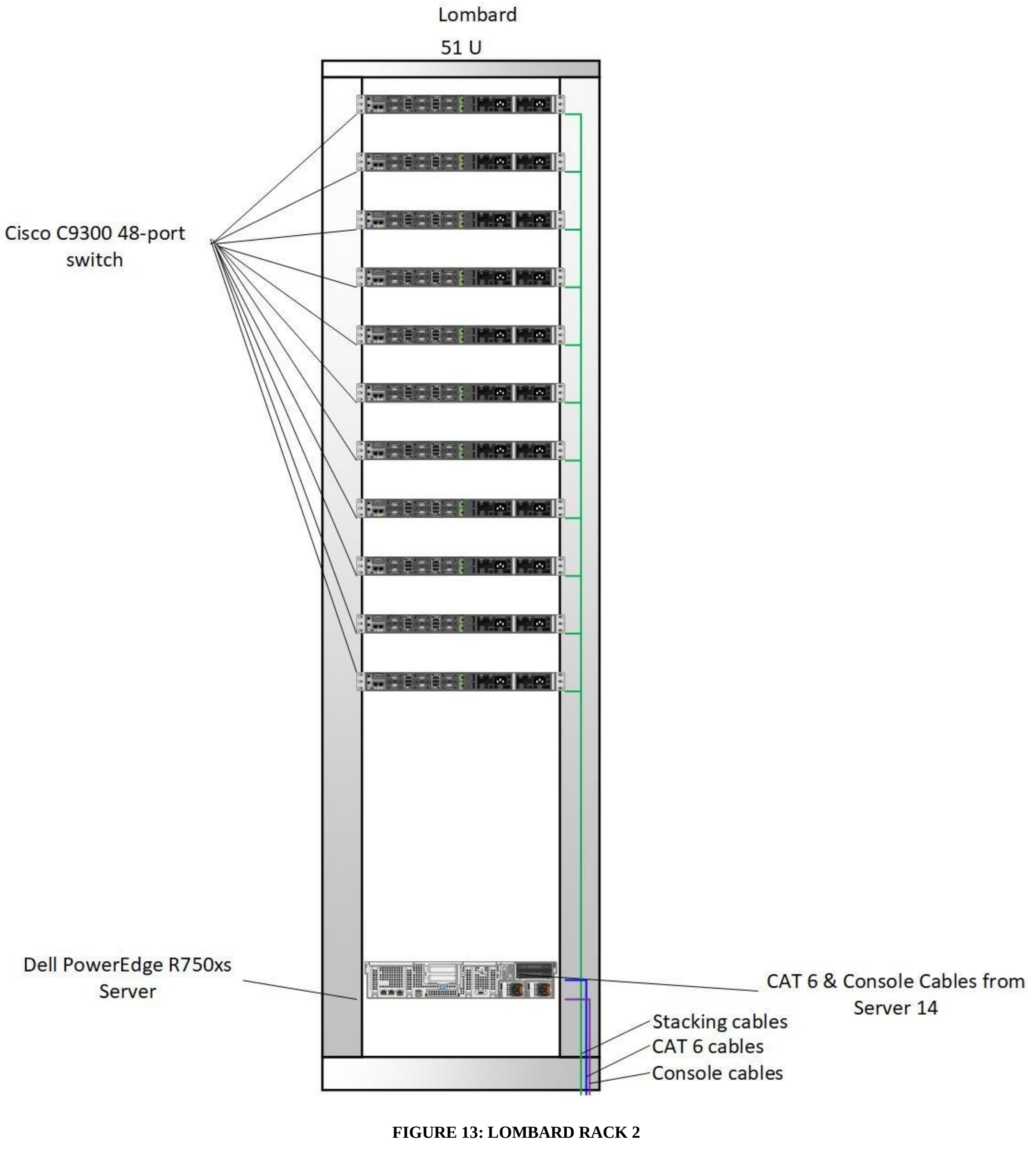

Lombard
51 U
Cisco C9300 48-port switch
Dell PowerEdge R750xs Server
CAT 6 & Console Cables from Server 14
Stacking cables
CAT 6 cables
Console cables

FIGURE 13: LOMBARD RACK 2

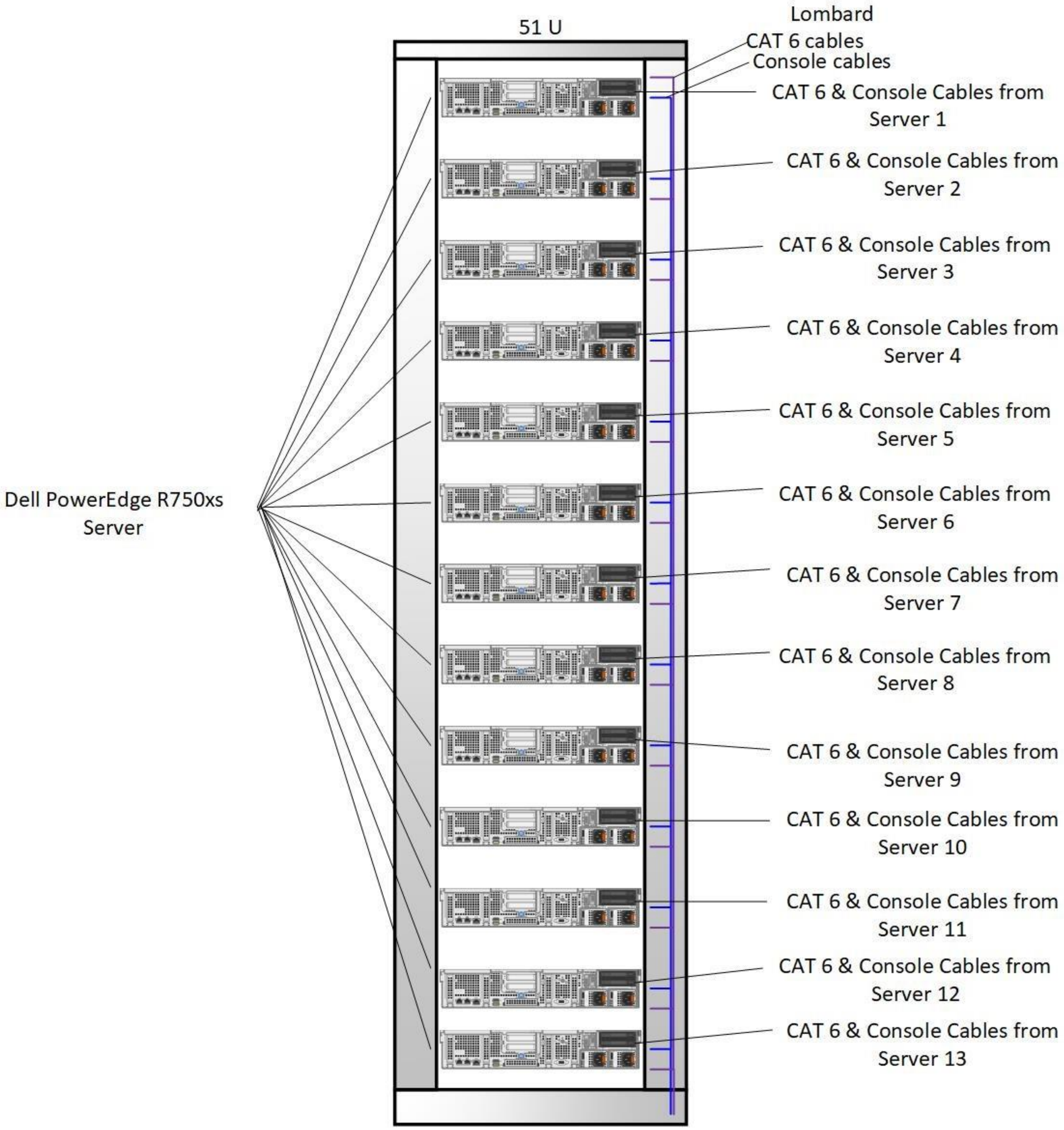

51 U
Lombard
CAT 6 cables
Console cables
CAT 6 & Console Cables from Server 1
CAT 6 & Console Cables from Server 2
CAT 6 & Console Cables from Server 3
CAT 6 & Console Cables from Server 4
CAT 6 & Console Cables from Server 5
CAT 6 & Console Cables from Server 6
CAT 6 & Console Cables from Server 7
CAT 6 & Console Cables from Server 8
CAT 6 & Console Cables from Server 9
CAT 6 & Console Cables from Server 10
CAT 6 & Console Cables from Server 11
CAT 6 & Console Cables from Server 12
CAT 6 & Console Cables from Server 13
Dell PowerEdge R750xs Server

FIGURE 14: LOMBARD RACK 3

8 PHYSICAL SECURITY

8.1 Risks Associated with Inadequate Physical Security

As of now, not one CEDAR location has any physical security measures put in place. This poses high security risks since anyone can easily walk inside the building, go into the control room, and have access to information and systems that they shouldn't. Furthermore, threat actors can physically attack critical systems of CEDAR which can result in the whole shutdown of the power grid. Due to the lack of physical security measures, our team has been designing physical security measures that will be implemented on all CEDAR locations.

8.2 Overview of Key Physical Security Measures

Key physical security measures that will be implemented are video surveillance cameras, card reader access controls, biometric access controls and security alarm systems. Other measures to ensure the total safety of each CEDAR building that we implemented are humidity and temperature transmitters, water and flood detectors, smoke detectors, fire extinguishers, fire alarm pulls, and fire and smoke barriers.

These physical security measures will be implemented at three CEDAR locations: Oakbrook, Waukegan, and Lombard.

8.2.1 Video Surveillance Cameras

Video surveillance cameras are the most crucial physical security control there is. There are many reasons behind that, such as they provide:

- **Deterrence**: The presence of surveillance cameras is a deterrent security measure that will discourage potential criminals from carrying out their attack. Since people know their actions will be recorded and can be used against them, criminals will be discouraged for doing anything unlawful.

- **Detection**: Surveillance cameras will capture clear footage of everyone that enters and leaves the building and specific rooms. This makes it possible for the CEDAR staff to know who and when exactly a specific person entered or left a specific room. Therefore, cameras will detect and capture any type of unlawful activity and security personnel will be alerted through monitoring them.

- **Documentation**: In case of a security incident, video cameras will provide important documentation that can help the CEDAR employees figure out what went wrong. Furthermore, the footage can be used as evidence against potential criminals.

Therefore, video surveillance cameras will be implemented throughout all the CEDAR locations. We will be using NVR Security Cameras because they provide face recognition, UltraHD 4K resolution, full-time color night vision, and video & audio recording.

FIGURE 15: NVR SECURITY CAMERA SYSTEM

8.2.2 Card Reader and Biometric Access Controls

Access controls are important for physical security for many reasons:

- **Restricting access**: Access controls will allow CEDAR to limit who has access to buildings and specific rooms at each one of their locations. For example, in Oakbrook, not all employees will have access to the computer room; therefore, through access controls CEDAR can make sure that only authorized employees have access.

- **Monitoring access**: Access controls will provide the company with a detailed record of who has entered and exited a specific room at a specific CEDAR location. This information is useful as it can be used to investigate security incidents and identify potential security attacks.

- **Preventing insider threats**: Access controls will prevent insider threats by restricting access to CEDAR employees or contractors. By restricting access to sensitive areas such as the main control room, CEDAR can limit the risk of insider threats and protect confidential systems and information.

- **Flexibility**: Access controls can be easily customized to meet CEDAR's need and grant and restrict access to specific employees and contractors as needed.

Therefore, access controls are a crucial component of physical security that CEDAR will be implementing.

We have implemented two main access controls:

1. Card readers will be put in rooms where maximum security is not needed, such as break rooms. We will be implementing RFID NFC Card Readers which will be implemented at almost every

door at all CEDAR locations that also have built-in cameras. We will be using Geovision Camera Access Controls with built-in Reader.

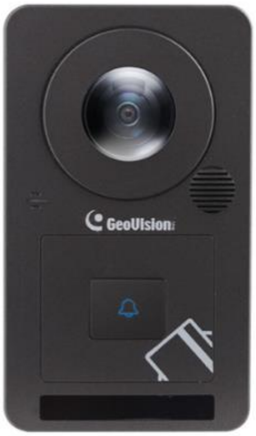


FIGURE 16: GEOVISION CAMERA ACCESS CONTROLLOER WITH BUILT-IN CARD READER

2. Biometric access controls will be put in places where maximum security is needed such as in the control room at Oakbrook and Waukegan. We will be implementing Suprema Biometric access controls. This control will provide three verification modes: Fingerprint Reader, Badge, and PIN/Password. This access control will satisfy the three human authentication methods:

    1. Something you know: PIN or Password

    2. Something you have: Smart Card

    3. Something you are: Fingerprint recognition.

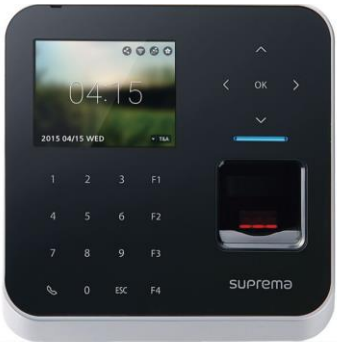


FIGURE 17: SUPREMA BIOMETRIC ACCESS CONTROLS

8.2.3 Security Alarm Systems

We will also be implementing security alarm systems throughout all CEDAR locations. These alarms will alert all security personnel whenever a security incident has occurred. Furthermore, these alarms will serve as a deterrent and detection security control. Security alarms will provide us with:

- **Deterrence**: The presence of alarms will discourage potential threat actors by signaling that the building is protected.

- **Intrusion Detection**: Alarms will detect and alert unauthorized entry.

- **Prompt Response**: Alarms will enable quick response, minimizing damage or theft of CEDAR equipment.

FIGURE 18: HONEYWELL SECURITY ALARM

8.2.4 Humidity and Temperature Transmitters

Throughout CEDAR’s locations, we also have implemented humidity and temperatures transmitters. These transmitters will help CEDAR operators monitor the humidity and temperature inside CEDAR locations and act when humidity/temperature levels are too high or too low. We have implemented humidity/temperature transmitters throughout every CEDAR building, in the interior and exterior of the buildings.

- **Interior**: A humidity/temperature transmitter has been implemented in most rooms at all three CEDAR locations, with more focus on the Oakbrook and Waukegan PGCC. This way, CEDAR operators will have a direct and specific understanding of temperature/humidity levels at each room, so in case a specific room is heating up more than usual, CEDAR operators will be notified and can take immediate action.
- **Exterior**: In most cases, humidity/temperature transmitters aren’t needed outside the building. However, to maximize the security of each CEDAR location, we decided that

humidity/temperature transmitters need to be placed outside the CEDAR buildings to monitor and assess environmental conditions. Assessing environmental conditions at all times is essential that CEDAR is aware first of any upcoming natural disaster at any CEDAR location.

FIGURE 19: DWYER HUMIDITY/TEMPERATURE TRANSMITTER

8.2.5 Water and Flood Detectors

Our team decided to also implement water and flood detectors throughout all CEDAR locations. Water and flood detectors play a crucial role in ensuring the physical security of every CEDAR building, most importantly the Oakbrook and Waukegan PGCC. These detectors will be essential in detecting and preventing damage caused by water-related incidents such as leaks, pipe bursts, or floods. Since Oakbrook and Waukegan PGCC house critical infrastructure and other sensitive equipment, these detectors will be crucial in protecting CEDAR equipment. Therefore, water and flood detectors will provide us with:

- **Early Detection:** Water and flood detectors will promptly identify the presence of water or abnormal moisture levels to CEDAR operators.
- **Damage Prevention**: Through alerting the CEDAR staff of water incidents, the staff will be able to take quick action to prevent as well as minimize damage to power grid equipment.
- **Risk Mitigation**: Water and flood detectors help mitigate risks by providing yet another layer of security through ensuring that water-related incidents are swiftly identified and taken care of.

FIGURE 20: WATER AND FLOOD DETECTORS

8.2.6 Smoke Detectors

We have implemented smoke detectors at all CEDAR buildings. Smoke detectors are extremely important in maintaining physical security of the PGCC. These detectors will be essential in providing early warning of fire and help prevent or mitigate the risks. Smoke detectors will play a crucial role in detecting smoke and allowing CEDAR operators to swiftly response to the fire and take the needed evacuation procedures. Therefore, smoke detectors will provide CEDAR with:

- **Early Warnings**: Smoke detectors will notify CEDAR staff of the presence of smoke, an early warning of a potential fire outbreak in the PGCC.
- **Fire Prevention and Mitigation**: Through alerting the CEDAR staff of the presence of smoke, smoke detectors allow swift action to prevent fires as well as potentially saving lives and minimizing damage to power grid equipment.

FIGURE 21: HONEYWELL SMOKE DETECTORS

8.2.7 Fire Extinguishers

We have supplied each CEDAR location with fire extinguishers. They are a critical component of physical security in a PGCC as they help prevent the spread of fires and protect CEDAR staff and equipment. These devices are essential for every building, let alone a power grid control center. Having readily accessible fire extinguishers is vital in maintaining a safe environment in a power grid control room where sensitive equipment is critical infrastructure are present. Therefore, fire extinguishers will provide us with:

- **Rapid Response**: Fire extinguishers allow for immediate action in the event of a small fire. This allows the CEDAR staff to quickly suppress small flames before they can spread to other rooms.
- **Fire Containment**: Fire extinguishers help contain and control flames. They will limit the damage and prevent the fire from spreading to the entire control room and other important areas.

- **Safety Assurance**: Fire extinguishers offer a sense of safety and security to CEDAR staff by letting them know of their ability to response to small fires and protect themselves.

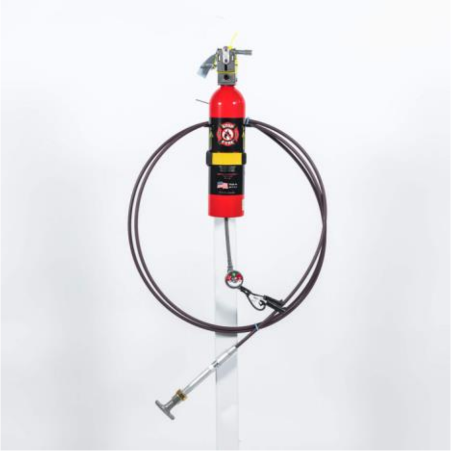


FIGURE 22: STOP-FYRE AUTOMATIC FIRE EXTINGUISHER

8.2.8 Fire Alarm Pulls

Fire alarm pulls have been implemented throughout every CEDAR building. These devices play an important role in notifying the rest of the building of a fire. They provide:

- **Immediate Activation**: Fire alarm pulls allow immediate activation of the security alarm system. Therefore, this will ensure swift response to fire emergencies to the PGCC.
- **Coordination of Response**: Fire alarm pulls also serve as a centralized means of initiating emergency response protocols. They allow for a coordination of response efforts such as the deployment of fire suppression systems, evacuation procedures, and other emergency services.

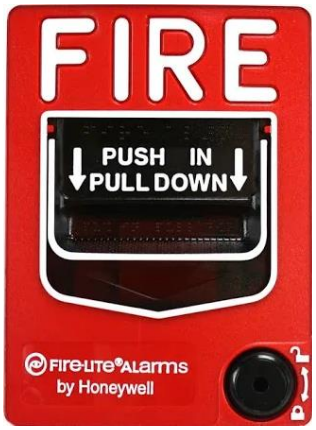


FIGURE 23: HONEYWELL PULL STATION

8.2.9 Fire and Smoke Curtains

Fire and smoke curtains have been implemented throughout all CEDAR buildings. These curtains will help prevent the spread of smoke and fire, providing additional time for evacuation procedures and fire response procedures. The fire/smoke curtains we have chosen will provide a 2-hour fire endurance rated system. These curtains provide:

- **Fire/Smoke Containment**: Fire/smoke curtains will create a barrier that restricts the movement of smoke/fire; therefore, preventing it from spreading to other important areas of the control room. This will help maintain clear evacuation routes and give staff more time to respond to fires.
- **Protection of Equipment and Infrastructure**: By limiting the spread of fire/smoke, these curtains will help protect critical equipment such as telecommunication equipment, electrical systems, and more. They will help minimize damage to critical infrastructure.

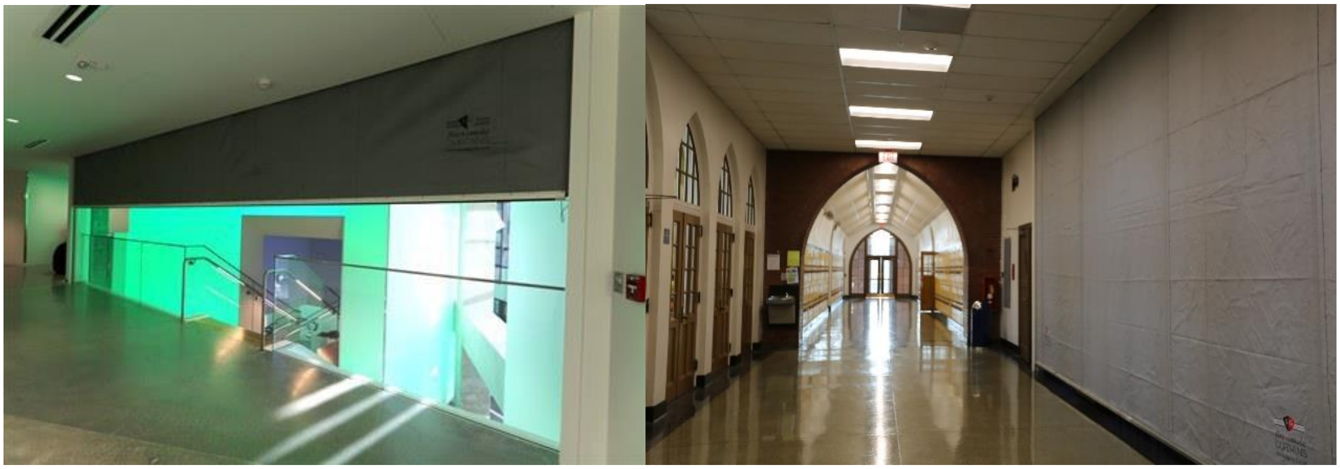


FIGURE 24: SMOKEGUARD FIRE AND SMOKE CURTAINS

8.2.10 Kensington Lock

In an effort to prevent CEDAR workstations from being stolen, all of workstations across CEDAR's three locations will be equipped with a Kensington lock. This will also be equipped in CEDAR's 100 service trucks that have service laptops. This ensures that confidential info within CEDAR's workstations do not leave CEDAR's premises.

FIGURE 25: KENSINGTON LOCK

8.2.11 GPS Location Tracking

In an effort to protect CEDAR's assets, GPS trackers will be installed in each work truck. This will ensure that in the event of theft, CEDAR can locate the work truck.

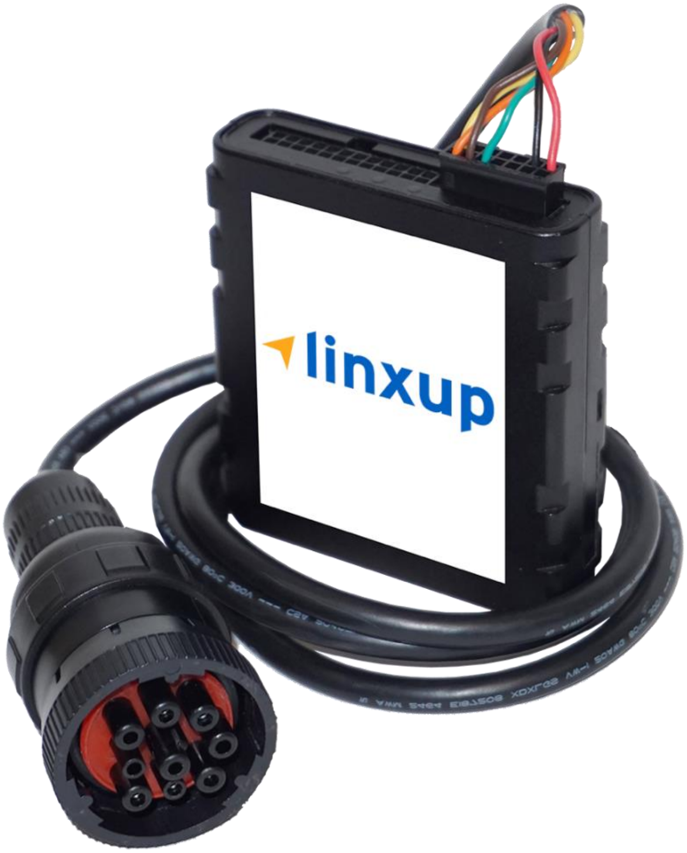


FIGURE 26: LINXUP GPS CAR TRACKER

9 RISK ASSESSMENT

This outline of how we are conducting our risk assessment (referenced from the *NIST SP 800-30* Risk assessment guideline). The risk will be based on a threat event, the likelihood of that threat happening, mitigating factors, and impact to our company.

TABLE 7: TOP 10 THREATS

TYPE OF THREAT SOURCE	DESCRIPTION
Malware • Rogue program. • Damages systems or files. • Unauthorized access. • Steal Sensitive Information • Conceals presence.	Malware has the potential to seriously disrupt operations and, in some situations, even result in physical harm. The risk of cyber-attacks rises as the energy sector's control systems and equipment become more interconnected.
Phishing • Steals employee information. • Access to unauthorized accounts • Hazardous attachments.	The goal of Phishing is to get private data that a bad actor can use to launch more serious assaults and acquire complete access to the CEDAR systems.
Distributed Denial of Service (DDOS) • Disrupts the online services used to control CEDAR equipment. • Clients lose access to systems. • Compromised machines.	DDoS attacks attempt to overwhelm and disrupt grid systems by bombarding them with a large volume of bogus traffic or requests. Attacks of this nature have the potential to take down crucial infrastructure systems.
Advanced Persistent Threat (APT) • Nation state actors and other sophisticated adversaries. • Gain unauthorized access to CEDAR network or/and systems. • Combination of attacks (Malware,	Advanced Persistent Threat (APT) attack, an attacker gets unauthorized access to a network or system with the goal of avoiding detection for a long time. The attacker's main goal is to obtain valuable information while simultaneously interfering with crucial

Phishing…)	infrastructure.
Insider • Selling corporate account information or admin privileges. • Insider sabotage. • Authorized breach.	An insider attack is when an employee harms the company by abusing their authority or stealing confidential information. Employees, contractors, or other trustworthy individuals with access to the grid run the risk of doing major harm to it.
Ransomware • Encrypts a large chunk or all of company data. • Takes advantage of a weakness in the company’s security. • Charges the company a sum of money for access to their data.	Ransomware can be classified as attacks that encrypt all the data on the gird’s servers and the perpetrators demand payment to possibly restore access and functionality.
Supply Chain • Difficult to detect. • Major goal is to maintain its presence. • Slowly disrupt services over time. • Compromises part of the build of an update or component.	Supply chain attacks are attacks that target the build process of a patch or piece of software, making them especially dangerous as the software is trusted by the company

TABLE 8: TOP 10 THREATS

TYPE OF THREAT SOURCE	DESCRIPTION
Supervisory Control and Data Acquisition (SCADA) • Disrupts the grid services. • Clients lose access to grid power. • Various forms (malware, phishing, supply chain). • Targets system processes e.g., temperature gage.	SCADA attacks are attacks that have unauthorized access into the SCADA systems in power grids. By having access to this system, they can sabotage pieces of equipment such as circuits or other parts of the actual grid.
Social Engineering • Gain unauthorized access to CEDAR network or systems. • Manipulate employees into doing malicious acts. • Leads to other types of attacks e.g., malware.	Social engineering are attacks that exploit human vulnerabilities, such as trust and stressful situations. When there are humans involved in the process the ability for error is dramatically increased.
Nation-state or Sponsored Attacks • Gain sensitive data for political or economic power. • Disrupt critical infrastructure. • Goal is to conceal identity. • Comprehensive approach e.g., threat intelligence, access controls.	Nation-state-sponsored cyber-attacks that aim to disrupt or disable critical infrastructure. These attacks are normally from specific nations to gain some sort of political or economic power.

The following table is from the NIST SP 800-30 Template and were used to describe impact and risk:

TABLE 9: ASSESSMENT SCALE – IMPACT OF THREAT EVENTS

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	The threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions. (ii) result in major damage to organizational assets. (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.
Moderate	21-79	5	The threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization can perform its primary functions, but the effectiveness of the functions is significantly reduced.

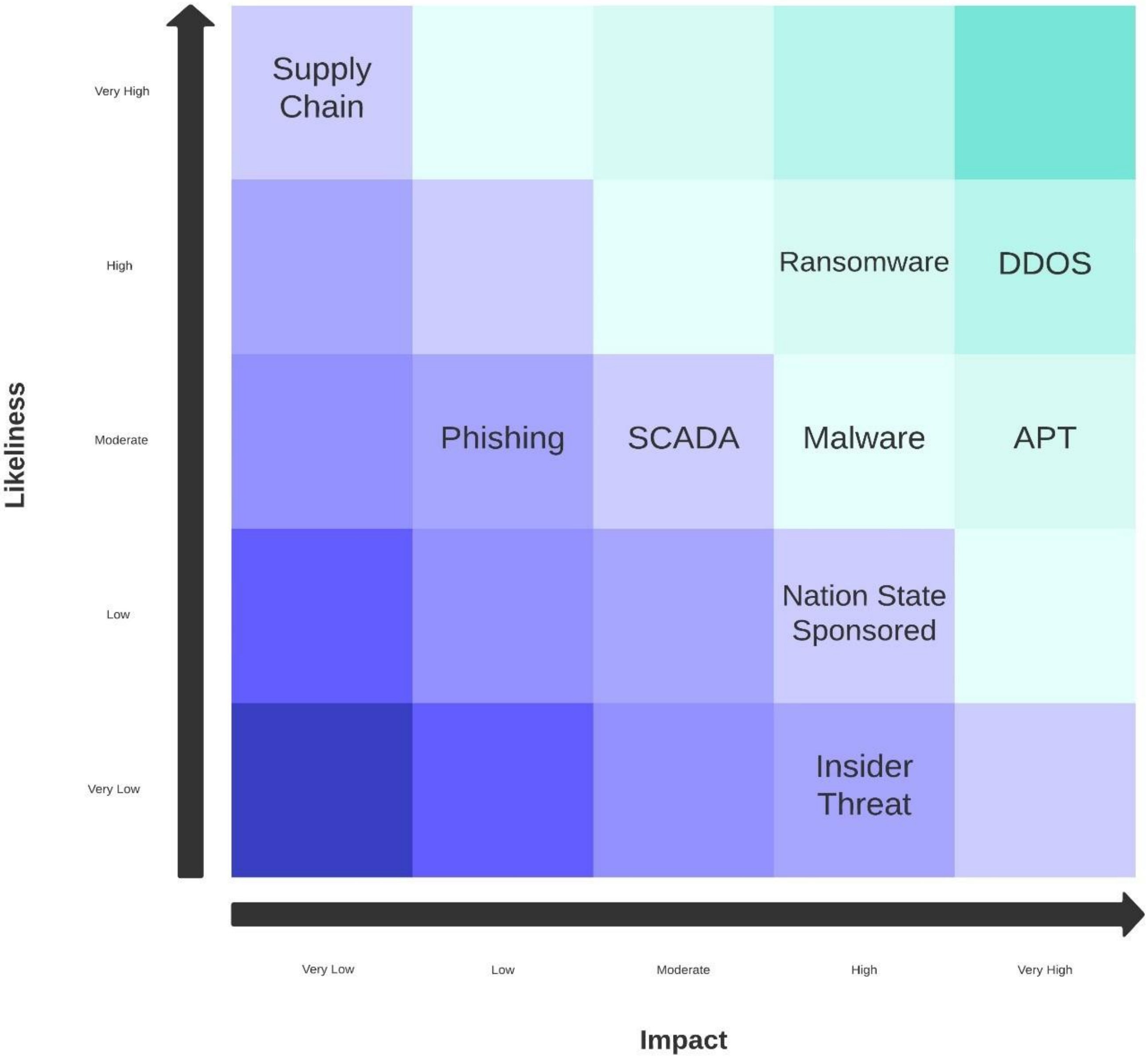
			(ii) result in significant damage to organizational assets. (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.
Low	5-20	2	The threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced. (ii) result in minor damage to organizational assets. (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Very Low	0-4	0	The threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

TABLE 10: ASSESSMENT SCALE – LEVEL OF LIKELIHOOD

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	Threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Moderate	21-79	5	Threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Low	5-20	2	Threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Very Low	0-4	0	Threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

TABLE 11: RISK ASSESSMENT RESULTS

Threat Event	Vulnerabilities / Predisposing Characteristics	Mitigating Factors	Impact	Likelihood
Phishing	Naïve Employee	Changing important info	Low	Moderate
Malware	System Vulnerability	Intrusion Detection	High	Moderate
DDOS	Outdated Technology	SIEM Monitoring	Very High	High
APT	Rogue Employees	Access Controls	Very High	Moderate
Insider Threat	Rogue Employees	Separation of Power	High	Very low
Ransomware	System Vulnerability	Backups/Disasters Recovery plan	High	High
Supply Chain	Malicious Code	Analysis Division	Very High	Low
SCADA	Outdated Software	Limit Functionality	Moderate	Moderate
Nation State Sponsored	Zero Day Exploits	Contact FBI	High	Low



	Very Low	Low	Moderate	High	Very High
Very High	Supply Chain				
High				Ransomware	DDOS
Moderate		Phishing	SCADA	Malware	APT
Low				Nation State Sponsored	
Very Low				Insider Threat	

FIGURE 27: RISK ASSESSMENT RESULTS

10 THREAT ASSESSMENT

A handful of threats against electrical grid companies like CEDAR have been identified and we have come up with proposed solutions to each kind of threat.

10.1 Malware

This threat increases as we further develop technology that is interconnected in many different ways. Using network monitoring tools like SIEM, which can identify and notify us of potential security events is imperative and a huge part of our approach to secure CEDAR. To find and stop any network intrusions, we will also install IDS and IPS systems. Encryption and multi-factor authentication will be employed to strengthen our security, and stringent physical security measures will be implemented to safeguard our systems and equipment. To ensure that they are aware of potential dangers and how to avoid them, all personnel will receive monthly cybersecurity training. Lastly, we will regularly analyze and audit our systems to find and proactively fix any potential vulnerabilities.

10.2 Phishing

Our solution to phishing is that all staff members must undergo regular cybersecurity training and testing to detect any systemic vulnerabilities in order to identify, prevent, and report these kinds of attacks. The goal of these sessions should be being able to identify phishing emails and to avoid opening any attachments from unidentified sources. Frequent testing can also be done by sending routine phishing emails to employees to find out who could need further assistance or training. Using multi-factor authentication can also assist in stopping attackers from gaining login credentials, while spam filters and anti-malware software can stop additional attempts from damaging crucial equipment.

10.3 Denial-of-Service (DoS) & Distributed Denial-of-Service (DDoS) Attacks

We intend to utilize network monitoring tools like SIEM and analytical tools that can spot odd traffic to protect against DoS and DDoS attacks. As an illustration, the tool SCADA Guardian, which offers real-time cybersecurity and operational analysis for ICS and SCADA systems, is something we are considering using for CEDAR. This tool is especially made to keep an eye on and protect vital infrastructure from various online threats. To be ready for any such attacks, we will also create a disaster recovery and business continuity plan.

10.4 Advanced Persistent Threats (APTs)

We will employ network monitoring technologies to find and eliminate potential dangers in order to stop such attacks. Also, we will develop efficient access controls by examining everyone in our organization's access permissions and limiting access solely to those who need it to carry out their duties. We'll also use methods like domain whitelisting, two-factor authentication, and encryption to further strengthen our security. Domain whitelisting will restrict which domains can be visited from our network.

10.5 Insider Attacks

Insider attacks can be decreased by establishing effective access controls and carefully monitoring user activity. Access restrictions should be built on the principle of least privilege. In our case, involving the electrical grid, we'll implement strict access restrictions by auditing each employee and granting access only as necessary for doing their jobs. In order to guarantee that people only have access to the systems and data they need to perform their jobs, role-based access control (RBAC) will also be utilized. Also, we'll monitor user activity with the use of a Security Information and Event Management (SIEM) system, which will also notify us of any odd behavior.

10.6 Ransomware

There are several solutions you can implement in order to mitigate and prevent these attacks from happening less frequently. One of them is to ensure that you have a working disaster recovery plan. In the case of the event, you can use backups to back up your entire system in order to avoid paying the ransom. You can also ensure your data even though that is an expensive option depending on the size could save you more money in the long run. When it comes to preventing ransomware attacks it is important that all systems are patched and frequently scanned. Another control to implement is to keep software up to date to prevent any vulnerabilities from being exploited in the first place.

10.7 Supply Chain

To prevent these supply chain attacks, we should devote company resources into creating separate divisions to analyze the build processes of software or patches before they are implemented onto our servers. CEDARs vendors and suppliers should also be monitored periodically, and security assessments should be done for any potential security issues such as breaches.

10.8 SCADA Attacks

One of the keyways to prevent these attacks is to understand and limit any possible connections that are not needed on the programmable logic controllers (PLC). Due to PLCs being manufactured for many different companies the likelihood that they have unneeded functions that are a threat to security is very high. Ensuring that these functions are removed or disconnected is especially important for hardening the system as we can’t patch SCADA servers. CEDARs SCADA system should also be isolated from other networks to reduce the risk of access from an unauthorized party.

10.9 Social Engineering

Our company is just as susceptible to this in order to mitigate this risk it is important to make sure all company devices are secured, enable two factor authentication making physical access a part of the equation, apply strict filtering on our company emails, and to regularly train the employees on how to identify phishing. 2.10 Nation-State-Sponsored Aside from having good security, the best way to mitigate these attacks for us is to have good communication with government agencies that are responsible for our nation's protection. Their investigative resources are key for our nation to be aware of what's going on and how we can further protect everyone.

11 IMPLEMENTATION PLAN

The proposed implementation plan for CEDAR's three locations - Lombard, Oakbrook, and Waukegan - begins with the procurement of necessary hardware, including servers, workstations, routers, firewalls, switches, and physical security components, scheduled for two weeks post contract signing. The plan adopts a site-by-site approach, starting with Oakbrook, then Waukegan, and finally Lombard, ensuring uninterrupted services. Prior to the arrival of new equipment, the old hardware will be decommissioned and removed, followed by the installation and testing of new cabling infrastructure. Concurrently, enhanced physical security systems like CCTV, biometric sensors, RFID systems, and alarms will be installed. The plan also includes setting up and configuring the new hardware, conducting a thorough security assessment, and configuring all employee workstations. Notably, Lombard will undergo significant upgrading, including the installation of 150 new workstations and a new credit card payment system. Oakbrook will receive an additional router for added network depth. Finally, all systems will undergo comprehensive testing to ensure optimal operation and efficiency. The execution timeline will align with the contract signing date and equipment delivery schedules, aimed at minimizing operational disruptions and enhancing cybersecurity at all sites.

This timeline will span over approximately 6 months, divided as follows:

1. **Contract Finalization and Equipment ordering:** Estimated Time: 2 weeks - Starting June 1, 2023

2. **Oakbrook Location:**
   - Equipment Removal: 1 week - Starting June 15, 2023
   - Physical Security Implementation: 2 weeks - Starting June 22, 2023
   - Cabling and Equipment Installation: 3 weeks - Starting July 6, 2023
   - Security Assessment and Workstation Configuration: 2 weeks - Starting July 27, 2023
   - Extra Router Implementation and Systems Testing: 2 weeks - Starting August 10, 2023

3. **Waukegan Location:**
   - Equipment Removal: 1 week - Starting August 24, 2023
   - Physical Security Implementation: 2 weeks - Starting August 31, 2023
   - Cabling and Equipment Installation: 3 weeks - Starting September 14, 2023
   - Security Assessment and Workstation Configuration: 2 weeks - Starting October 5, 2023
   - Systems Testing: 1 week - Starting October 19, 2023

4. **Lombard Location:**
   - Equipment Removal: 1 week - Starting October 26, 2023
   - Physical Security Implementation: 2 weeks - Starting November 2, 2023

- Cabling and Equipment Installation: 4 weeks (including the 150 workstations) - Starting November 16, 2023
- Set up Credit Card Payment Systems: 1 week - Starting December 14, 2023
- Security Assessment and Workstation Configuration: 2 weeks - Starting December 21, 2023
- Systems Testing: 1 week - Starting January 4, 2024

5. **Estimated Delivery Date:** January 11, 2024

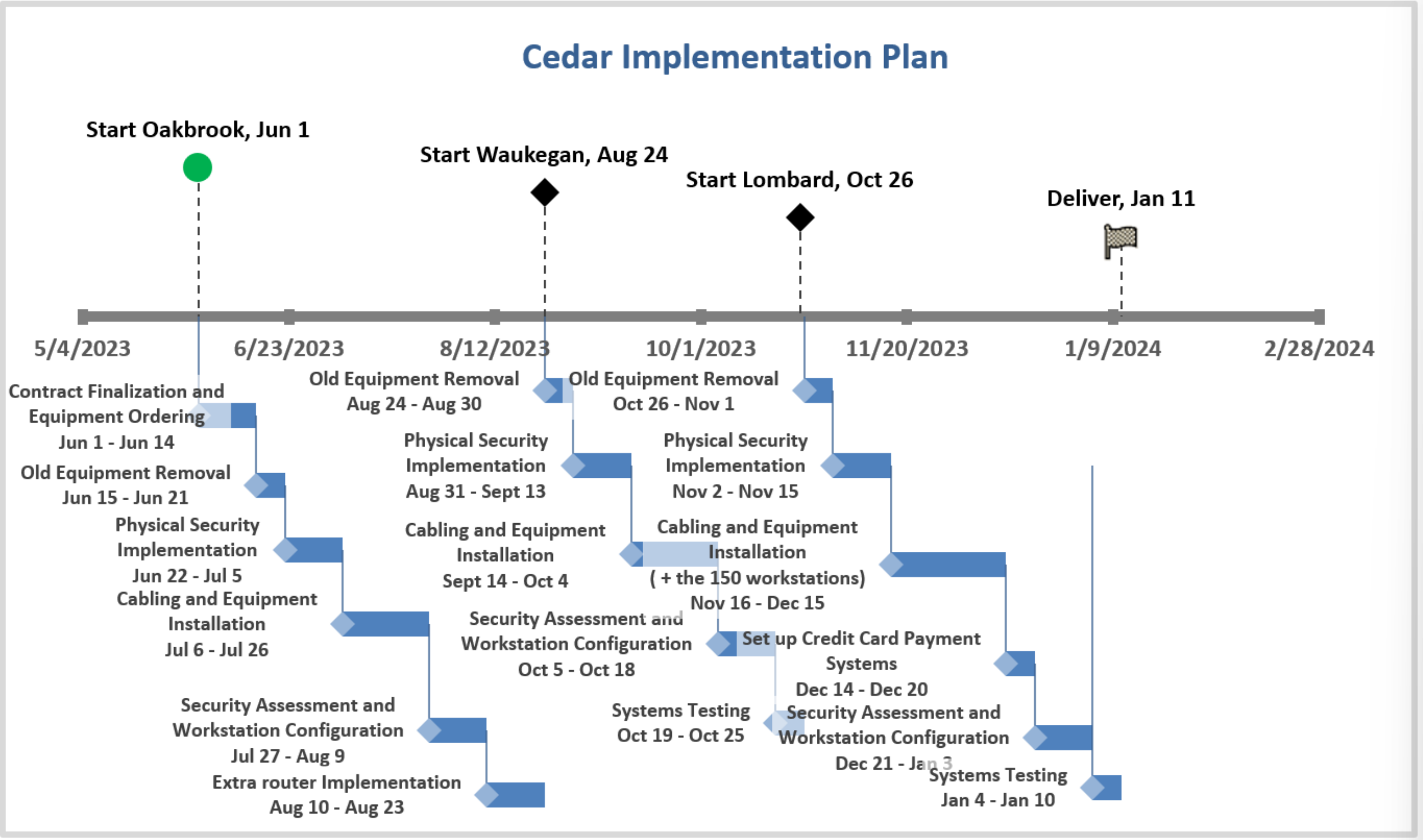


FIGURE 28: CEDAR IMPLEMENTATION PLAN

12 COMPLIANCE REQUIREMENTS

As mentioned prior, CEDAR needs to adhere to NERC CIP. Below are all of the requirements that CEDAR needs to follow and what we have done to remain compliant.

TABLE 12: NERC CIP COMPLIANCE CHECKLIST

NERC CIP Compliance Checklist			
Requirement	**Description**	**Compliance Status (Y/N)**	**Explanation**
CIP-002 Asset Identification and Classification	Identify critical assets and define High, Medium, Low impact ratings for the power grid systems. Set up a review period.	Y	1. **Critical Assets Identification**: We've catalogued all BES-connected key assets, including those vital to facilities, systems, and power grid's stability and security. This also covers ranking assets as HIGH, MEDIUM, and LOW impact, with explanations. 2. **Review Frequency**: We have a set schedule for asset review, comparing with past records. An authorized person evaluates the findings. Our asset inventory includes a regular review section, ensuring updates are documented, reviewed, and greenlit by a senior manager.
CIP-003 Policy and Governance	Implement access controls. Conduct personnel risk assessments. Implement security awareness training.	Y	1. **Access Controls**: We've set up robust access controls for crucial cyber assets, including secure authentication, least privilege rules, and regular access permission reviews. 2. **Personnel Risk Assessments**: We carry out background checks and risk assessments for staff accessing vital cyber assets, ensuring their reliability

	Establish Incident response plans. Implement physical security measures.		and trustworthiness. 3. **Security Awareness Training**: Regular security awareness trainings are provided to all personnel with access to critical cyber assets, emphasizing their security roles and responsibilities. 4. **Incident Response & Recovery Plans**: Documented incident response and recovery plans are in place, detailing the procedures for identifying incidents. 5. **Physical Security Measures**: As per CIP-006, suitable physical security measures have been developed and implemented to shield critical cyber assets from unauthorized access or tampering.
CIP-004 Personnel and Training	Personnel Risk Assessments. Security awareness / Cyber security training. Access management.	Y	1. **Personnel Risk Assessments**: We conduct pre-access background checks and risk assessments for personnel with potential electronic or physical access to crucial cyber assets, updated every seven years. 2. **Security Awareness**: We have a security awareness program that educates critical cyber asset handlers about security risks and their responsibilities, reinforced with reminders, updates, and alerts every 15 months. 3. **Access Management**: We manage and rescind electronic and physical access to critical cyber assets through

			an access management program that reviews and validates access rights every 15 months. 4. **Cybersecurity Training**: We offer role-specific cybersecurity training, tailored to job functions, for personnel with authorized access to critical cyber assets. Topics include policies, access controls, incident response, and asset use, refreshed every 15 months.
CIP-005 Electronic/Security Perimeter (ESP)	Remote Access is managed. Access Control Rules. IDS/IPS system in place.	Y	We meet the requirement for malicious traffic inspection through security measures like Intrusion Detection or Intrusion Prevention Systems (IDS/IPS) or alternative deep packet inspection methods to ensure effective monitoring of ESPs.
CIP-006 Physical Security of BES Cyber Systems	Identify Physical security assets. Develop a physical security plan. Implement physical access controls. Use monitoring and surveillance technologies. Secure access points. Establish visitor control procedures.	Y	1. **Asset Identification**: We maintain a documented inventory of key cyber assets and define Physical Security Perimeters (PSPs) encompassing these assets to deter unauthorized access. 2. **Physical Security Plan**: We have a comprehensive plan addressing all physical security aspects, including access controls, monitoring, and incident response. 3. **Physical Access Controls**: We use physical barriers like locks and gates to restrict PSP access to authorized personnel only, keeping a record of access permissions. 4. **Monitoring Technologies**: We

			employ surveillance tech such as security cameras, intrusion detection systems, to detect and deter unauthorized access. 5. **Secure Access Points**: All access points, like doors, windows, and vents, are secured to prevent unauthorized entry. 6. **Visitor Control Procedures**: We manage visitor access within the PSP, including logging visits, escorting visitors, and ensuring compliance with security policies.
CIP-007 System Security Controls	Develop security policy. Implement access controls. Establish security patch management. Implement system security management. Monitor and log security events Perform vulnerability assessments.	Y	1. **Security Policy**: We've established a comprehensive security policy covering system security aspects like access controls, vulnerability management, incident response, and security awareness training. 2. **Malware Prevention**: Antivirus and malware prevention measures are in place on critical cyber assets, maintained with regular updates and scans to identify and mitigate threats. 3. **System Security Management**: We monitor and manage vital cyber assets, including network devices, firewalls, and intrusion detection/prevention systems, ensuring the secure operation of the bulk electric system. 4. **Security Event Monitoring**: We have monitoring and logging systems to collect and analyze security events, detect patterns or trends, and aid

			incident response. 5. **Vulnerability Assessments**: We conduct regular vulnerability assessments to spot potential weak points in crucial cyber assets and implement necessary mitigations.
CIP-008 Cyber Security Incident Response	Develop an incident response plan.	Y	We meet the requirement by having a comprehensive incident response plan in place, detailing procedures for detecting, reporting, and responding to cybersecurity incidents.
CIP-009 Recovery Plans	Develop a recovery plan	Y	We meet the required of a comprehensive and documented recovery plan that outlines the procedures for restoring critical cyber assets affected by a cybersecurity incident to their normal operation as quickly and securely as possible.
CIP-010 Change and Vulnerability Management	Develop a configuration change management process. Patch management.	Y	1. **Patch management**: We have a vulnerability plan in place. 2. **Change Management**: Establish a documented process for managing changes to critical assets, including baseline configurations.
CIP-011 Protection of BES Cyber System Information	Develop an information protection program. Identify and classify sensitive information.	Y	**Access controls**: We have established access controls for sensitive information.

CIP-012 Control Center Communications	Ensure the security of sensitive data during transmission and to prevent unauthorized access, modification, or disclosure	Y	**Data Protection Plan**: Documented plan that addresses the identification, classification, and protection of real-time assessment and real-time monitoring data transmitted between control centers.
CIP-013 Supply Chain Security	Address risks associated with the supply chain for products and services that could impact the reliable operation of critical cyber assets.	Y	**Supply chain Risk Management Plan**: Documented plan that addresses the identification, assessment, and mitigation of supply chain risks related to critical assets.
CIP-014 Physical Security of Key Substations	Ensure that organizations identify and protect transmission stations, substations, and control centers from potential physical threats that could impact the reliable operation of the bulk electric	Y	1. **Recognition of Essential Facilities**: We have established a method for identifying and ranking critical facilities. 2. **Risk Assessment**: We routinely perform risk assessments of these essential facilities to determine potential physical threats, vulnerabilities, and possible outcomes. 3. **Physical Security**: We have developed a detailed and documented plan for physical security, addressing the safeguarding of key facilities from

	system.		identified threats, with measures including access management, surveillance systems, and intrusion detection. 4. **Physical Security Protocols**: We have designed and implemented suitable physical security protocols for essential facilities, which may include barriers, security cameras, access control, and alarm systems. 5. **Train Personnel**: Regular training will be provided for personnel tested in maintaining the physical security of critical facilities.

13 POLICIES AND PROCEDURES

As part of upgrading CEDAR’s core infrastructure, it is vital that the right policies and procedures are implemented to ensure smooth operations across all three locations. We have carefully designed a handful of relevant procedures that CEDAR should implement to ensure proper operations and also so that they meet compliance standards. Below you will find our team's policy writeups for CEDAR.

These are the policies we have created for CEDAR:

- Disaster Recovery Policy
- Incident Response Policy
- PGCC Security Policy
- Security Awareness Training Policy
- Guest Policy
- Acceptable Use Agreement Policy
- Change and Vulnerability Management Policy
- Data Protection Policy
- Supply Chain Risk Management Policy

13.1 Disaster Recovery Policy

13.1.1 Introduction

The Disaster Recovery Plan is designed to ensure the continuation of vital processes in the event that a disaster occurs. This plan involves restoring the Supervisory Control and Data Acquisition system (SCADA), payment systems, and customer data following any unplanned downtime.

13.1.2 Disaster Recovery Statement

CEDAR aims to establish and maintain appropriate levels of protection for its critical IT assets and data. The goal is to minimize loss, restore normal business operations as quickly as possible, and meet both business obligations and industry regulatory requirements.

13.1.3 Disaster Recovery Strategy

CEDAR will maintain a secondary backup site at the Waukegan location. This site will provide full functionality in the event of a disaster at the primary Oak Brook location.

13.1.4 Roles and Responsibilities

A designated Disaster Recovery Team will be responsible for initiating the recovery process, coordinating recovery efforts, and ensuring effective communication throughout the recovery process. This team should consist of IT personnel, network administrators, security officers, and personnel from each of CEDAR's main functional areas.

- **DR Coordinator**: Responsible for coordinating DR operations and communications.
- **IT Team Lead:** Responsible for managing the technical recovery operations.
- **Network Administrator:** Ensures the restoration of network services and connections.
- **Security Officer:** Responsible for ensuring security protocols are followed during recovery.

13.1.5 Response/Plan Activation

Scenario: Cyber Attack or Technical Disaster Affecting Primary Site

In the event of a disaster, the following steps will be taken:

- **Identify and report the incident:** Upon detection of a cyber-attack or technical disaster, the first responding party will immediately inform the DR coordinator. The DR coordinator, after assessing the severity of the disaster, will then activate the disaster recovery plan and notify the rest of the DR team.

- **Activate the Disaster Recovery Plan:** The Disaster Recovery Team will be responsible for activating the plan.
- **Notify stakeholders:** All relevant stakeholders (employees, customers, partners, regulators, etc.) should be notified about the situation and informed about what steps are being taken.

13.1.6 Recovery

Depending on the type and extent of the disaster, the Disaster Recovery Team will initiate the appropriate recovery processes:

- **Failover to Waukegan location:** If the primary site (Oak Brook) is compromised, systems should failover to the Waukegan location. This process will be initiated by the Network Administrator.
- **Data Recovery:** In the event of a disruption or outage, the power grid should be able to recover and restore its operations to a state where no significant data or power generation is lost beyond a few minutes or seconds.
- **Systems Restoration:** Systems should be restored in order of criticality, with the SCADA system being given highest priority. In this order: SCADA system, payment systems, customer data systems.

13.1.7 Post-Recovery Actions

Once the systems are restored:

- Conduct a post-mortem analysis to understand the cause of the disaster and to learn from the event.
- The DR team should then work together to implement changes in systems, procedures, or infrastructure based on findings from the post-mortem analysis.
- Update the DR plan as necessary based on lessons learned.

13.1.8 Testing and Maintenance

The disaster recovery plan should be tested at least biannually to ensure its effectiveness. This can include tabletop exercises, simulations, or full-scale drills. All tests will be documented, and lessons learned should be incorporated into the plan.

13.1.9 Training

All staff will be trained on the disaster recovery plan. This training will include their roles and responsibilities, how to report an incident, and what steps will be taken in the event of a disaster.

13.2 Incident Response Policy

13.2.1 Introduction

This document aims to establish a clear operational framework for handling network security incidents and to present specific procedures for conducting investigations. The target audience for this document includes the Incident Response Team, analysts from Managed Security Service Providers, and any external Incident Responders participating in the resolution of security incidents. Within this document, each "playbook" section outlines the foundational investigative actions to be executed for each alert, according to the relevant use case.

13.2.2 Incident Response Model with Tiers

The Incident Response team's operational scope is defined by Cedar's tiered Incident Response model. This model outlines and allocates essential tasks to be carried out at every stage of a network security incident, irrespective of the incident type. Please note that if a tier is not applicable, Tier 2 will be responsible for any of the following.

Tier 1

Tier 1 incident response is the responsibility of CEDAR's Managed Security Service Provider (MSSP) if applicable.

- Evaluate alerts for false positives (Is there a compromise?)
    - **Logical**
        - The alert logic is flawed, and the detected event does not align with the intended threat.
    - **Parametric**
        - The alert logic is accurate, but the numeric threshold for detecting a threat pattern requires adjustment.
    - **Contextual**
        - The alert logic and threshold are valid, but the events that triggered the rule are part of a known legit operation that matches a threat pattern.

Tier 2

Cedar's Incident Response team handles Tier 2 incident response.

- Validate Tier 1 investigations.
- Determine if an alert is a true positive (Is there a compromise?)
    - Signature
        - The events represent Indicators of Compromise (IOCs) matching known threats.
    - Policy
        - The events represent a violation of a Cedar’s security policy.
    - Behavioral
        - The events are anomalous based on an established behavioral baseline.
- Identify Indicators of Compromise (What is the nature of the compromise?)
    - Network
        - IP addresses, Domains, Protocols, Ports, Packet captures
    - Host
        - Logs, Files, Registry keys/values, Processes, Configurations
    - User
        - Accounts, Groups, Permissions
- Perform Network posturing actions to support Tier 3
    - Increase Network Visibility
    - Decrease Network Noise
    - Capture Forensic Evidence
    - Deny Threat actors’ access.
    - Degrade Threat actors’ capabilities.

Tier 3

Cedar will obtain outside professional services for Tier 3 Incident Response (If applicable)

- Validate Tier 2 investigations.
- Determine the point and method of intrusion (How did the compromise occur?)
- Assess the scope of the network compromise (Who/What is compromised?)
- Understand the intruder's intent (Who/What is the ultimate goal?)
- Perform network eradication.
- Validate remediation steps.

13.2.3 Investigations

13.2.3.1 LATERAL MOVEMENT PLAYBOOK

Threat Scenario

Lateral Movement detection rules assume that an intruder has successfully entered the network, established persistence, analyzed the internal network, compromised credentials, and is now attempting to move laterally across the network.

Investigation Goals

Detect Credential Compromise**:** The aim is to determine whether authentication events were performed by an authorized user/application or an intruder posing as a user/application. Simply asking the user to recognize the authentication is rarely sufficient, as most network authentications are not interactive.

Rule Guidelines

Type 1

Lateral Movement Type 1 rules detect threats engaging in high-volume, rapid lateral movement using automated tools. These threshold-based rules evaluate timeframes in 10-minute increments, which means an intruder must generate significant activity to be detected. Users outside IT operations teams responsible for patching should rarely trigger a Type 1 rule.

Type 2

Generally, users should operate within a single trust zone and trust category. Vertical movement between trust zones should only occur through choke points, like jump servers and Administrator VDIs, using designated accounts. Lateral movement between categories should be authorized based on Active Directory groups. Type 2 rules aim to detect intruders inadvertently violating Cedar's expected trust model.

Type 3

The Lateral Movement Type 3 rules are designed to add context to Type 1 and 2 alerts in the form of risk modifiers. The risk modifiers are not alerts, but instead represent a measurement of how different a user’s current behavior is compared to the user’s historic baseline.

In the case of Lateral Movement, users increase their risk scores by logging into destinations they do not usually visit using logon methods they do not usually use.

Investigation Steps

- Identify the Source
    - Identifying the source involves determining the origin of the malicious activity, such as the IP address, domain, or specific device involved. This step enables the Incident Response team to track the attacker's entry point and assess the potential damage caused by the incident.
- Identify the Destination
    - identifying the destination, the Incident Response team can assess the potential impact on business operations, as well as the attacker's motives and goals. This information will also be helpful when prioritizing remediation efforts and deciding on the appropriate course of action to protect critical assets and minimize potential losses.
- Identify the User
    - Identifying the user account, group, or role associated with the suspicious activity. Identifying the user helps determine if the incident is a result of compromised credentials or insider threat and assists in tracing the attacker's movements within the network, as well as evaluating the user's access rights and privileges.
- Make a Determination
    - After gathering information on the source, destination, and user, the Incident Response team must analyze the collected data to make a determination. This involves deciding whether the incident is a false positive or a true positive and classifying the nature of the security event. The team should assess the potential impact of the incident on the organization's operations, data, and reputation, and formulate an appropriate response plan.

13.3 PGCC Security Policy

This defines standards for the configuration, maintenance, and review of the Power Grid Control Center System. Vulnerable and unsecured servers continue to be a security risk and a main target for malicious threat actors.

13.3.1 Purpose

The purpose of this policy is to establish the confidentiality, integrity, maintenance, and periodic review of the power grid control center system. This establishes guidelines for security of the platforms and to minimize unauthorized access to the PGCC.

13.3.2 Scope

This policy applies to the servers that make up the Power Grid Control Center in both the Oakbrook and Waukegan locations. This would be the Solaris and Windows servers that directly communicate with the power grid components and host the application used by the grid operator.

13.3.2.1 GENERAL GUIDELINES

- All configurations done on these servers should be in accordance with its operations as the power grid control center system.
- All configurations should be done in accordance with NECR CIP compliance.
- Any change to the configuration set in the system must be authorized by the appropriate personnel.
- Configuration changes for servers must follow appropriate change management procedures.
- Services and applications other than what are necessary for these servers to carry out their operations as the power grid control system must be disabled for efficiency.
- The standard principle of least privilege access would be required to use the servers or perform a function.
- Do not use root when a non-privileged account will do.
- Security patches must be periodically updated to recent versions made possible to ensure proper functionality of the server.
- Server should be physically located in an access-controlled environment.
- Overall security and authorized access to the systems must be emphasized.

13.3.2.2 ACCESS CONTROL

As a critical infrastructure, these servers would have no remote access, and it would have very restricted access in person.

- There would be no unauthorized access to these servers.
- The servers would be physically secured away and secured. Authorized personnel would require identification and authentication to gain access to the physical space and then the server.

13.3.3 Monitoring

All events and incidents on critical systems like this must be logged for analysis and facilitates auditing of the systems. All security event logs will be kept for a stipulated period, and other forms of backups would be retained in accordance with the time period stipulated in the backup policy. Every security-related event must be reported to IT for log review. Security-related events includes but is not limited to:

- Unauthorized access to critical assets.
- Discrepancies in logs obtained from the environment.

In the event of an incident, logs are collected, and the incident is properly documented in accordance with what is indicated in the incidence response policy.

13.3.4 Compliance

The servers are specifically used as part of a Power Grid Management System Application whose sole purpose is to distribute electrical energy to clients, so it has to be compliant with any energy redistribution compliance act.

- Periodic audits would be implemented and performed by assigned personnel at Cool Electrical Distribution and Redistribution (CEDAR)
- An external audit as required by NERC CIP would be performed by the authorized personnel as indicated.
- Audits would be done during non-peak times to avoid failures or disruptions.
- Any exception to this policy must be approved by the IT team in advance.

13.3.5 Enforcement

Employees found to violate this policy would be subject to disciplinary actions like suspension or termination of employment, depending on the severity of incident, perpetrators could be subject to fines and/or legal consequences.

13.4 Security Awareness Training Policy

13.4.1 Overview

Security is an important part of any modern-day organization, and since about 95% of security breaches are caused by human error it is important to train personnel to try and reduce the probability of error. As an organization that works with sensitive information, resources, and assets; It is important that employees, and every other user of the company network, device, and other resources are educated on the necessary measures to maintain a highly secured environment.

13.4.2 Purpose

The purpose of this policy is to establish the minimum requirements (processes and procedures) for the Security Awareness and Training Program. This includes designing a robust program that is properly developed, implemented, and updated. Employees have an obligation to demonstrate an understanding of security awareness in their respective positions that would equip them to better protect the organizations data, information, and assets.

13.4.3 Scope

This policy applies to all Employees that work at Cool Electrical Distribution and Redistribution and use its resources and/or assets.

13.4.4 Responsibility

The IT unit has the primary responsibility for planning, developing, and updating the security awareness training program. The education aspect may be performed by the IT team or any personnel they deem fit to provide the training. With that said, all employees and users have a responsibility to implement the concepts taught within the security awareness program.

13.4.5 Exceptions

Exceptions to this policy are likely to occur. Exception requests must be made in writing and must contain:

- The reason for the request,
- Risk to the organization if policy is not duly followed,
- Specific mitigations that will not be implemented,
- Technical and other difficulties, and
- Review date.

Request for exception must be submitted to the IT team for approval for careful review.

13.4.6 Policy

13.4.6.1 DEVELOP

1. A program for performing security awareness training must be established.

2. This process must be documented and approved.

13.4.6.2 EDUCATE

1. Users must receive security awareness training, at a minimum, on an annual basis. The IT team is responsible for this training.

2. All new users must receive cybersecurity awareness training before being granted access to enterprise assets.

3. Users who require access to the critical assets and the grid must be trained on how to securely access and operate the systems.

4. Users must be trained on how to recognize social engineering attacks.

5. Periodic simulated attacks must be carried out as part of security awareness training to assess and identify areas for improvement and best mitigation practices.

6. Users must be trained on best practices for authentication in the enterprise. Users must be trained on best practices for handling enterprise data.

    a. Training must be included on the following subjects as it pertains to the enterprise’s data management:

        i. Identifying sensitive data

        ii. Storing sensitive data

        iii. Transferring sensitive data

        iv. Archiving sensitive data

        v. Destroying sensitive data

        vi. Any legal and / or regulatory obligations of the above.

    b. Clear screen and clean desk best practices must be included in the training.

7. Users must be trained on the causes of unintentional data exposure in the enterprise.

8. Users must be trained on ethical technology practices.

9. Users must be trained on best password practices, the need for periodic password changes.

10. Users must be trained on understanding NERC CIP and other operation related compliance.

11. Users must be trained on how to recognize and report security incidents.

12. Users must be trained on how to identify and report if their enterprise assets are missing security updates.

13. Users must be trained on the dangers of connecting to and transmitting enterprise data over insecure networks.

13.4.6.3 ENFORCEMENT

Employees found to be in violation of this policy would be subject to disciplinary actions and necessary sanctions. Sanctions include but is not limited to one or more of the following:

- Access restriction or access termination
- Suspension or termination of employment
- Criminal penalties which may include fees and/or fines.

13.4.6.4 UPDATE

The content of the security awareness training program must be reviewed and updated annually, or when significant changes to the enterprise occur.

13.5 Guest Policy

13.5.1 Overview

The Guest Policy is an important policy to ensure that when people other than employees visit the organization, they do not pose a threat to people, property, and resources of the organization. It is basically a list of protocols and procedures that must be followed to manage guests' access while on premises. It can vary based on what your organization agrees to as the generally acceptable behavior.

13.5.2 Scope

This policy applies to any guest at any of CEDAR's three office locations.

13.5.3 Policy

Listed below are some main requirements to be considered for our guest policy.

- Unauthorized guests are not allowed to visit, no appointment no entry.
- Appointments are only valid for one individual, there are exceptions to this rule (group tours/visits), but they must be pre-authorized.
- Guests are only allowed during general working hours.
- When guests come in at the main gate, they must self-identify with any form of identification and surrender to security screening.
- Guests are only allowed to park in guest parking.
- Guests must sign in at the gate and the front desk.
- Unless previously stated, visitors cannot go further than the waiting area & office space.
- Guests would be provided with a key card that gives access ONLY to the bathroom and general office space/cubicle, and it is to be always displayed as a form of identification else guests might be asked to leave.
- A guest should not be left alone and must always have a guide while on the premises.
- Guests must return their key card at the end of their visit.
- Guests upon departure must pass through a security screening and exit inspection.
- NO SOLICITING, NO DISRUPTION, or Acts of violence.
- Employees must give at least 12 hours' notice of personal guest visitation.
- Deliveries are to be dropped off at the gate while employees go and receive their orders.
- The previously listed rules apply to guests who have multiple visits for 5 days or less.
- If a guest must visit for 5+ days, they get a temporary id which is to be returned after, but they are still subject to the entry and exit screening.

13.5.4 Punitive Measures

This defines penalties for guests and guests' guides when the stated guest policy is not adhered to.

- Violation of any of the previously stated requirements by a guest is grounds for guest removal from premises or prosecution in severe cases.
- Violation of any of the previously stated requirements by an employee is grounds for disciplinary action (like queries and suspensions) up to prosecution and termination in severe cases.

13.6 Acceptable Use Agreement

The Acceptable Use Policy, also known as AUP, is a set of rules that gives an outline of the appropriate use or access to devices, networks (corporate or the internet), forms, and documentation between two or more parties. Organizations must construct an acceptable use policy to be well suited to their business requirements and operations for it to best serve the organization.

13.6.1 Overview

CEDAR as an organization provides access to its internet services and other related resources to employees and guests. It is necessary to extensively highlight the appropriate use of technology and other technological components to have ground rules and have some form of control over functions carried out within the organization. This policy would also mean respecting the integrity of the office buildings, the rights of other users, and other license and contractual obligations and agreements.

13.6.2 Scope

This policy applies to any employee (customer service personnel, grid operator, and dispatch riders) at the Oakbrook, Waukegan, or Lombard locations. It also applies to the use of the physical facilities.

13.6.3 Generally Acceptable use

The list below outlines practices and behaviors that are generally expected to be adhered to while using resources at CEDAR.

- Equipment, systems, and networks may be monitored at any time for security and auditing purposes.
- Encryption of confidential documents, client data, and company resources is highly suggested.
- CEDAR as an organization has proprietary rights on every record and data created and stored on workstations or the organization’s network.
- Enforcement of multi-factor authentication as a form of identification before permission is granted to an organization's resources.
- When on CEDAR’s network privacy is provided but not guaranteed.
- Users of the organization's network and resources must be respectful to others, their privacy, and their rights.
- Employees are responsible for the respectful use of their assigned workstations, and all other company resources. In the case of loss or compromise, they must immediately report to the appropriate team.
- Installation of any productivity software on the company assigned workstation should be done by the IT team or must be approved by the IT team (the former is strongly advised).

- Employees are responsible for the protection of passwords, assigned key cards, and any other access related information. Maintaining a strong password as advised in the Password Policy and following the instructions for protecting assigned key cards and all other access tools as specified in the Access Control Policy.
- Access to certain parts of the facility is restricted for employees that have no business accessing those areas.
- Access to resources (company and client data) is on a strict need-to-know basis.
- Occasional employee training on acceptable use would be conducted to keep employees fully aware of the acceptable use policy and any other updates or changes that are periodically made to it.

13.6.4 Unacceptable Use

The list below outlines behaviors that are generally prohibited when using resources at CEDAR.

- Using an unassigned workstation (to access emails, files, programs, etc.), endeavoring to gain access to workstations that one is restricted from accessing and trying to bypass the security measures and restrictions.
- Using another employee's access card to gain access to restricted areas in the facility and trying to bypass the security measures and restrictions.
- Accessing untrusted sites and links or emails that come from unverifiable sources.
- Involving the organization in any and every act of soliciting, transactions forgery, or fraudulent activity.
- Sending personal non-work-related emails with personal email accounts.
- Using ones assigned workstation to surf the internet for personal use.
- Holding up resources like printers or fax machines for personal use during peak periods.
- Tampering or mishandling information or data.
- Impersonation of any kind under the guise of committing a crime or being involved in any illegal activity.
- Violation of company rules and regulations, divulgence of company’s intellectual property with the intent to cause harm.
- Creation and distribution of material that is offensive, disruptive, or in violation of human rights. Any material created on the organization's system or network with the intent to be malicious towards colleagues or clients is absolutely prohibited.
- Violation of clients' confidentiality and security by exposing their records or data.

13.6.5 Punitive Measures

Violation of this policy will result in sanctions like temporary or permanent access revocation. Violation of some parts of this policy is a criminal offense, and the violators would be duly charged and prosecuted to the fullest extent of the law.

- Any employee in violation of this policy would be subject to disciplinary actions (query, suspension, or employment termination), fines, and/or legal actions.
- Any other individual in violation of this policy would be subject to fines and/or legal action.

13.7 Change and Vulnerability Management Policy

13.7.1 Introduction

The purpose of this policy is to define procedures for managing changes to critical cyber assets and assessing vulnerabilities to maintain the reliability and security of Cedar Electric Power Grid systems, in compliance with CIP-010 standards.

13.7.2 Scope

This policy applies to all employees, contractors, and third-party personnel involved in managing and maintaining Cedar's critical cyber assets.

13.7.3 Configuration Change Management Process

Cedar will follow a documented process for managing changes to critical cyber assets. This includes:

- baseline configurations, modifications, and approvals.
- All changes should be reviewed, approved, and documented to always maintain a transparent record of the system configuration.

13.7.4 Baseline Configurations

Cedar will follow baseline configurations for all critical cyber assets, including:

- hardware, and software will be created and maintained. This provides a reference point for system changes and aids in the identification of any unauthorized modification.

13.7.5 Configuration Change Controls

Cedar will establish controls to ensure all changes to critical cyber assets are authorized, tested, and documented. The process will identify and mitigate potential security risks associated with changes to ensure system stability and security.

13.7.6 Monitoring and Tracking Configuration Changes

A process to monitor and track configuration changes will be implemented to detect unauthorized changes and verify compliance with the configuration change management procedure.

13.7.7 Vulnerability Assessments

Cedar will regularly conduct vulnerability assessments of critical cyber assets to identify and mitigate potential weaknesses. These assessments will evaluate baseline configurations, identify vulnerabilities, and prioritize remediation efforts based on risk.

13.7.8 Patch Management

A process for tracking, evaluating, and applying security patches and updates to critical cyber assets will be established and followed diligently. All security patches and updates will be applied in a timely manner to maintain system security.

13.7.9 Documentation and Logs

All configuration change management processes, baseline configurations, changes, vulnerability assessments, and patch management activities will be accurately recorded and maintained as per NERC CIP standards. This documentation will be retained as required and made available for review during audits.

13.7.10 Regular Assessments and Audits

Cedar will conduct periodic reviews and assessments to ensure continued compliance with the CIP-010 standards, identify potential areas for improvement, and implement necessary updates or enhancements.

13.7.11 Policy Review

This policy will be reviewed annually or as required by changes in the CIP-010 standards to ensure its continued effectiveness and compliance.

13.8 Data Protection Plan

CEDAR needs to collect, store, and use certain information. As an energy distribution company, the type of information that CEDAR would handle includes data transmitted between the control centers, information about customers that they offer their services to, information on employees, contractors, any outsourced labor and any other individual that the organization has a business relationship with. The core principles of data protection help to ensure the security and accuracy of data in CEDAR'S possession.

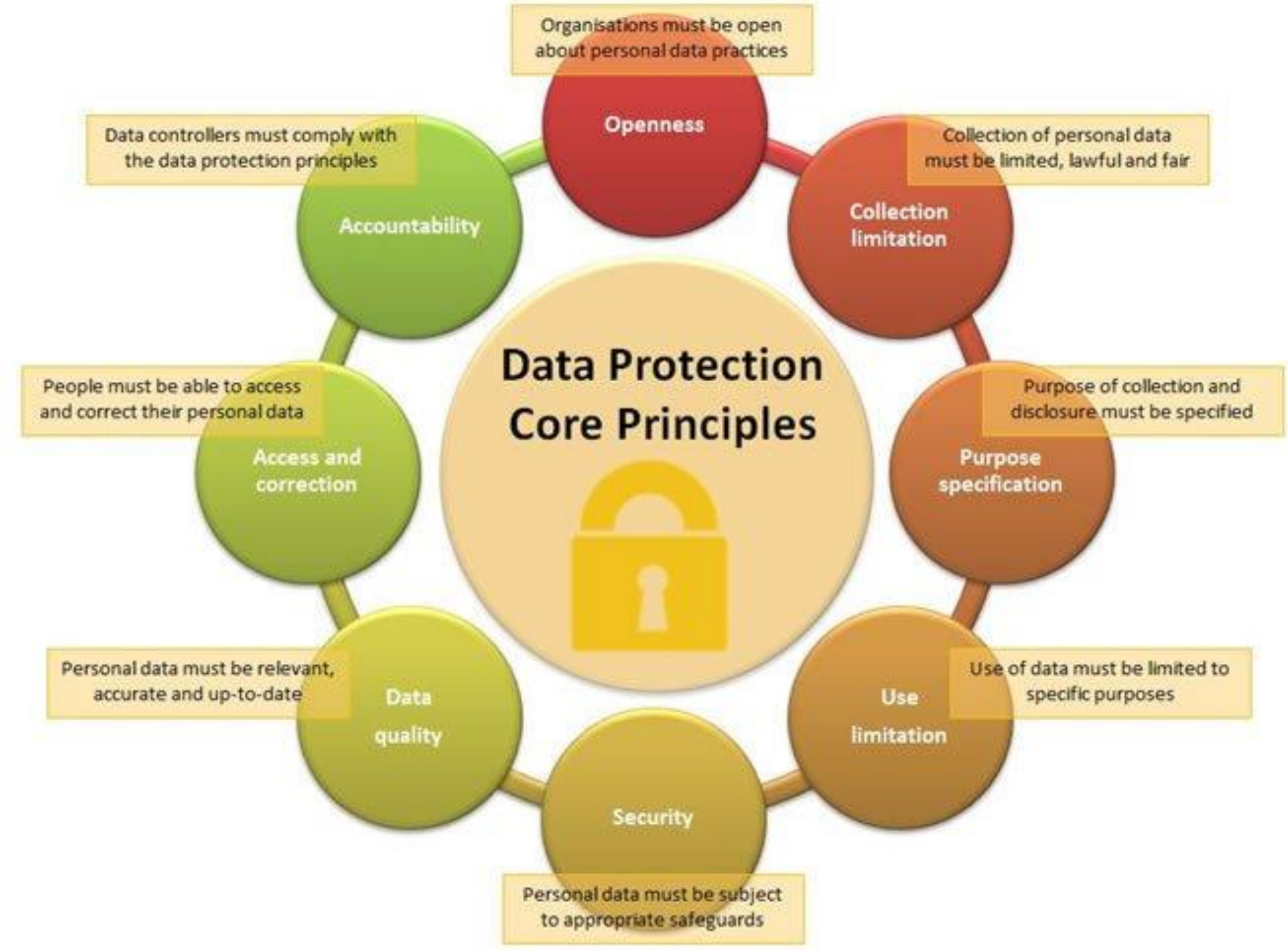

Organisations must be open about personal data practices
Openness
Collection of personal data must be limited, lawful and fair
Collection limitation
Purpose of collection and disclosure must be specified
Purpose specification
Use of data must be limited to specific purposes
Use limitation
Security
Personal data must be subject to appropriate safeguards
Personal data must be relevant, accurate and up-to-date
Data quality
People must be able to access and correct their personal data
Access and correction
Data controllers must comply with the data protection principles
Accountability
Data Protection Core Principles

FIGURE 29: DATA PROTECTION CORE PRINCIPLES

13.8.1 Objective

This policy is a documented plan that defines identification, collection, sorting, handling, and protection of data. This data protection plan exits to ensure that CEDAR:

- Protects the information collected from clients, employees, and others.
- Protects itself from the risks of a security breach.
- Achieves transparency about data collection, storage, and processing.
- Is compliant with data protection laws (especially in the state in which it operates)
- Ensures that all locations can share an up-to-date centralized database of information.

13.8.2 Scope

This policy applies to data collected from the control centers where CEDAR operates, data collected in all locations where CEDAR operates, as well as personal data of employees and clients of CEDAR.

13.8.3 Responsibilities

Every employee who works for CEDAR would be responsible for ensuring that data is collected, stored, and processed appropriately. Every team must ensure that they follow proper procedure outlined within this plan when either processing or handling data.

13.8.3.1 GENERAL GUIDELINES

- The standard principle of least privilege access would be required to access and handle data.
- CEDAR would provide its employees with periodic training on how to properly process and handle data.
- Data collection, handling, and processing must be in compliance with operation or industry-specific regulations.
- Employees would also be taught safety precautions to ensure better data security.
- The purpose of data collected, and its processing style must be explicitly indicated.
- Data transmitted across control centers should have a centralized secure storage system that is made readily available and accessible to all CEDAR’s locations.
- Data transmitted across control centers and personal data collected should be periodically backed up in case of a disaster.
- Data collated should be regularly reviewed and updated if found to be out of date, or false.
- Data collected from individuals must have a stipulated time of storage and must be deleted afterwards.
- Decisions about data should require approval of at least one appointed personnel (preferably a data protection officer).
- Employees should direct questions to and request help from appointed personnel (preferably a data protection officer) about any uncertainty.

- Data collection, handling, and processing must be in compliance with the Data Protection Act and other data handling laws in the state or country of operation (Illinois PIPA, BIPA).

13.8.3.2 DATA CLASSIFICATION

Data can be classified in several ways, but data processed and handled by CEDAR would be classified by sensitivity levels. Classification by sensitivity levels helps with understanding the value of such data to the organization and what happens if it is changed, lost, or destroyed. This classification also helps with compliance with relevant industry-specific regulations and procedures. Classification by sensitivity level includes:

- **LOW**: These are information that is generally intended for public knowledge. An example is information on the organization's website like services offered by CEDAR, price points, etc.
- **MEDIUM**: These are information that is sensitive and strictly intended for internal use only. An individual who does not work with CEDAR should have access to this knowledge. Examples are business-related information, reports, or email correspondence with no confidential data.
- **HIGH**: These are highly confidential information that if compromised would be damaging to operations and the reputation of CEDAR. An example would be the data transmitted between CEDAR's control centers and the Personal Identifiable Information that is collected on customers.

13.8.3.3 DATA SECURITY MEASURES

In the design of a functional environment for CEDAR, having security measures in place was a priority. Some of the security measures that are implemented to protect data that CEDAR handles from wrongful use, alteration, or unauthorized access include:

- Access Control
- Physical Security
- Network Security
- Security Awareness Training
- Incidence Response and Monitoring

13.8.3.4 ENFORCEMENT

Employees found to violate this policy would be subject to disciplinary actions like suspension or termination of employment, depending on the severity of incident, perpetrators could be subject to fines and/or legal consequences.

13.9 Supply Chain Risk Management Policy

13.9.1 Purpose

The purpose of this policy is to help identify and monitor risks within CEDAR's supply chain. This ensures that CEDAR meets compliance with any relevant bodies as well as maintains in stable operation. The policy's goal is to prevent disruptions and ensure a safe and strong supply chain.

13.9.2 Scope

This policy covers all risks to CEDAR's supply chain, including:

- Compliance risks
- Operational risks

13.9.3 Responsibilities

The following individuals are responsible for implementing this policy:

The Supply Chain Manager: The Supply Chain Manager is responsible for implementing and overseeing the entire supply chain risk management process. This includes conducting risk assessments, managing risk treatment plans, and monitoring the effectiveness of implemented controls. They are also responsible for ensuring compliance with CIP-013 and coordinating with the Chief Risk Officer.

The Chief Risk Officer: The Chief Risk Officer is responsible for the oversight of the overall risk management strategy in CEDAR, including supply chain risks. This includes approving risk assessments and risk treatment plans, ensuring the organization remains compliant with CIP-013 and other relevant regulations, and providing strategic advice on managing risk at the organizational level.

Employees Involved in the Supply Chain: All employees involved in CEDAR's supply chain are responsible for understanding and adhering to the Supply Chain Risk Management Policy. This includes identifying potential risks in their area of work, reporting risks through the appropriate channels, implementing risk treatment controls as directed, and participating in relevant training sessions.

13.9.4 Policy

CEDAR will manage supply chain risks through a risk management process that includes the following steps:

- Identify risks
  - CEDAR will identify all its potential risks in terms of its supply chain by conducting a thorough risk assessment.
- Assess risks
  - CEDAR will then assess the likelihood and impact of each identified risk. The risk assessment will use a scoring system to rank risks based on their likelihood and impact.
- Treat risks
  - CEDAR will treat risks by implementing appropriate controls. The type of controls that CEDAR implements will depend on the results of the risk assessment.
- Monitor risks
  - CEDAR will regularly monitor risks to ensure that the implemented controls are effective. If a risk changes, CEDAR will update its risk assessment and treatment plan.

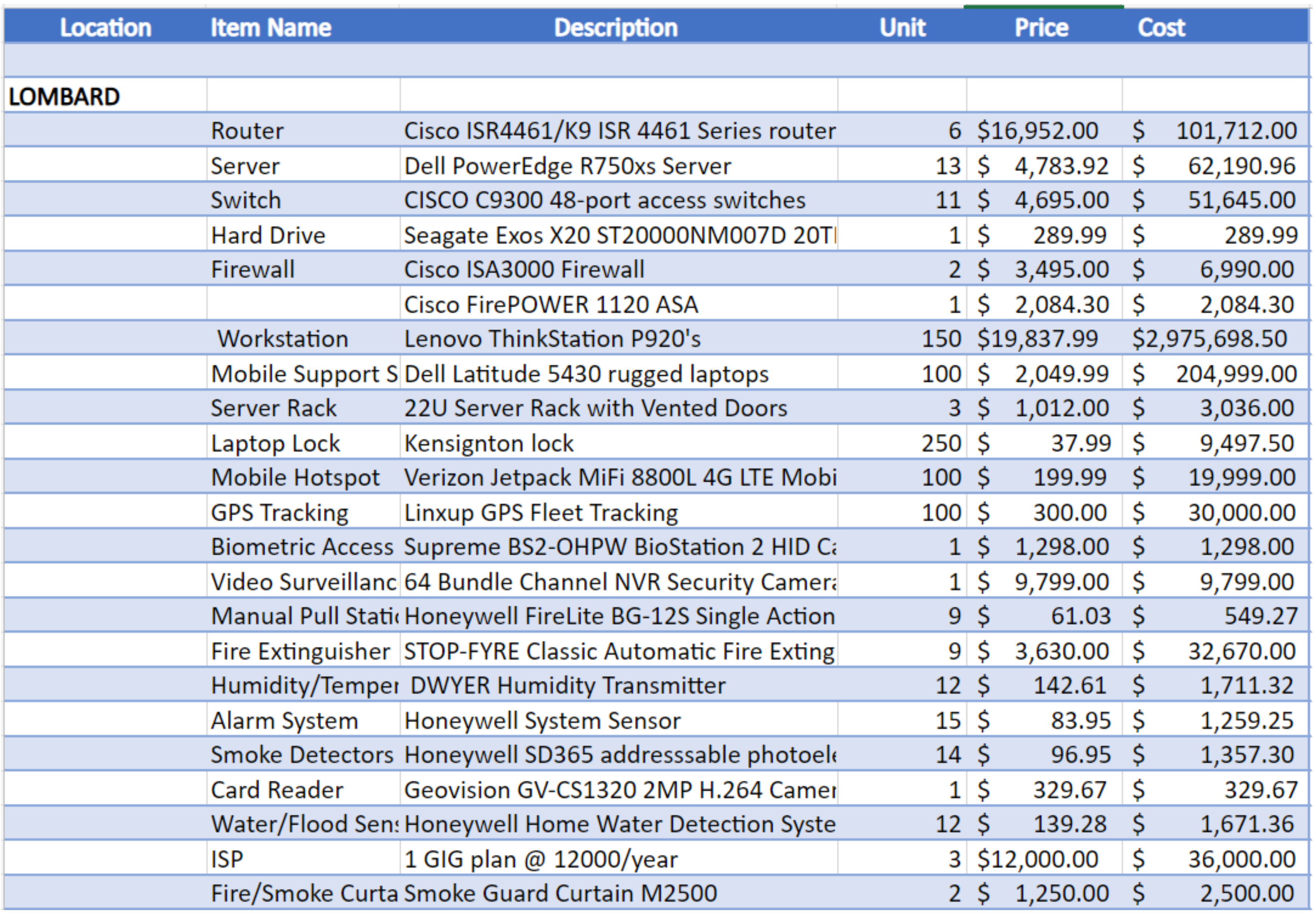
13.9.5 Training

CEDAR will train its employees on identifying and responding to supply chain risks. This will ensure that risks are mitigated to the best of their ability.

Effective Date: This policy is effective immediately.

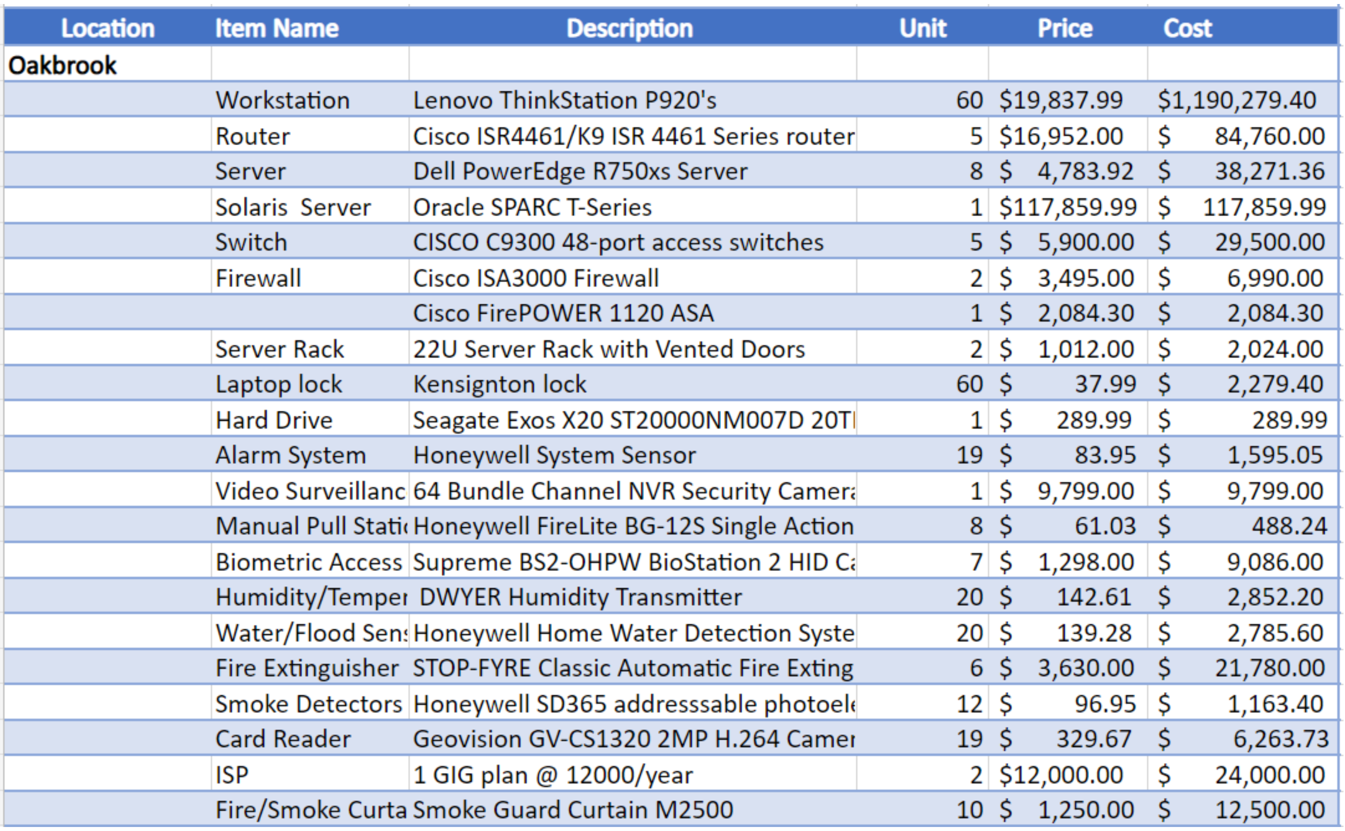
14 COST TOTALS

Below you will find our cost breakdown per location as well as the grand total cost. As mentioned prior, our grand total is $5,975,691.36



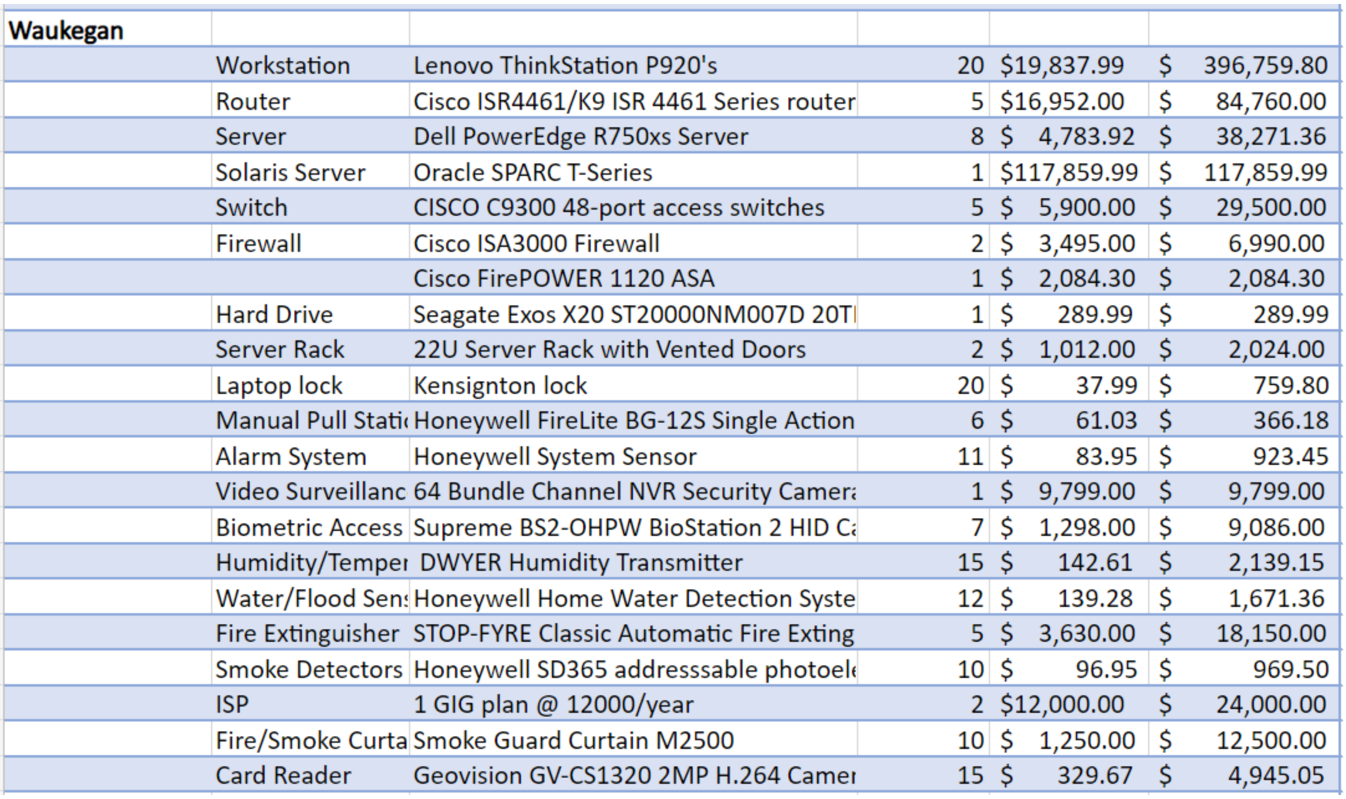
Location	Item Name	Description	Unit	Price	Cost
LOMBARD					
	Router	Cisco ISR4461/K9 ISR 4461 Series router	6	$16,952.00	$ 101,712.00
	Server	Dell PowerEdge R750xs Server	13	$ 4,783.92	$ 62,190.96
	Switch	CISCO C9300 48-port access switches	11	$ 4,695.00	$ 51,645.00
	Hard Drive	Seagate Exos X20 ST20000NM007D 20TI	1	$ 289.99	$ 289.99
	Firewall	Cisco ISA3000 Firewall	2	$ 3,495.00	$ 6,990.00
		Cisco FirePOWER 1120 ASA	1	$ 2,084.30	$ 2,084.30
	Workstation	Lenovo ThinkStation P920's	150	$19,837.99	$2,975,698.50
	Mobile Support S	Dell Latitude 5430 rugged laptops	100	$ 2,049.99	$ 204,999.00
	Server Rack	22U Server Rack with Vented Doors	3	$ 1,012.00	$ 3,036.00
	Laptop Lock	Kensignton lock	250	$ 37.99	$ 9,497.50
	Mobile Hotspot	Verizon Jetpack MiFi 8800L 4G LTE Mobi	100	$ 199.99	$ 19,999.00
	GPS Tracking	Linxup GPS Fleet Tracking	100	$ 300.00	$ 30,000.00
	Biometric Access	Supreme BS2-OHPW BioStation 2 HID Ca	1	$ 1,298.00	$ 1,298.00
	Video Surveillanc	64 Bundle Channel NVR Security Camera	1	$ 9,799.00	$ 9,799.00
	Manual Pull Statio	Honeywell FireLite BG-12S Single Action	9	$ 61.03	$ 549.27
	Fire Extinguisher	STOP-FYRE Classic Automatic Fire Exting	9	$ 3,630.00	$ 32,670.00
	Humidity/Temper	DWYER Humidity Transmitter	12	$ 142.61	$ 1,711.32
	Alarm System	Honeywell System Sensor	15	$ 83.95	$ 1,259.25
	Smoke Detectors	Honeywell SD365 addresssable photoele	14	$ 96.95	$ 1,357.30
	Card Reader	Geovision GV-CS1320 2MP H.264 Camer	1	$ 329.67	$ 329.67
	Water/Flood Sens	Honeywell Home Water Detection Syste	12	$ 139.28	$ 1,671.36
	ISP	1 GIG plan @ 12000/year	3	$12,000.00	$ 36,000.00
	Fire/Smoke Curta	Smoke Guard Curtain M2500	2	$ 1,250.00	$ 2,500.00

FIGURE 30: LOMBARD COST TOTALS



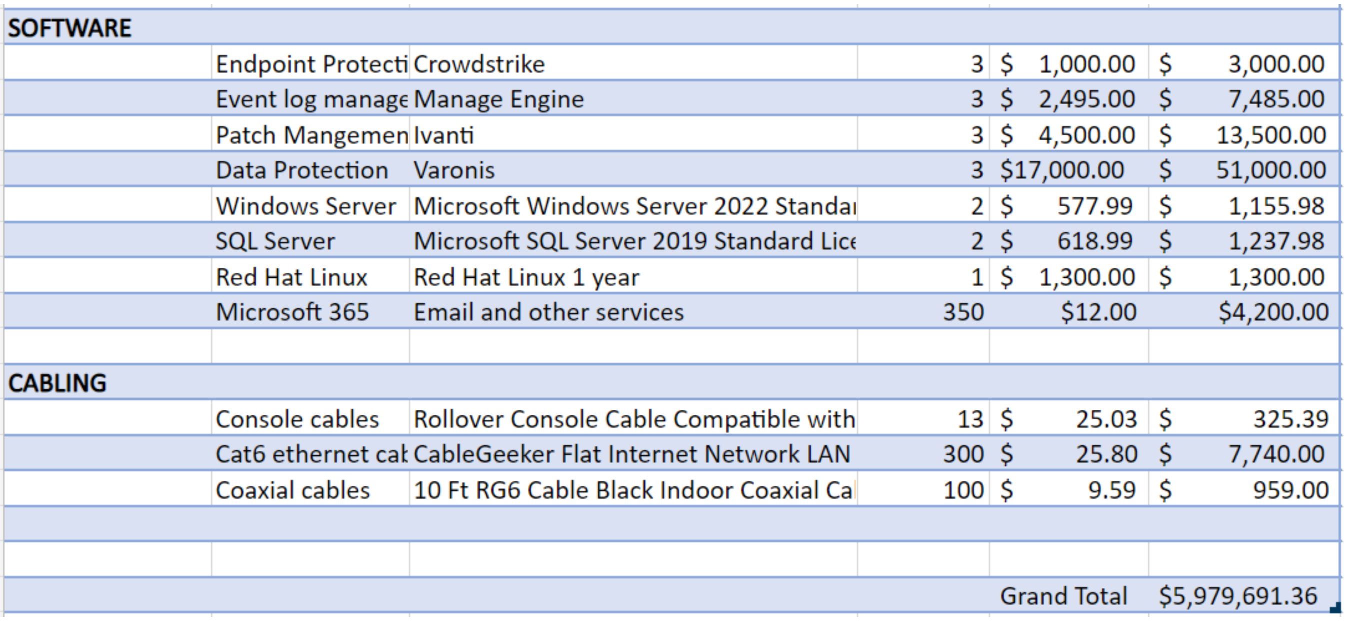
Location	Item Name	Description	Unit	Price	Cost
Oakbrook					
	Workstation	Lenovo ThinkStation P920's	60	$19,837.99	$1,190,279.40
	Router	Cisco ISR4461/K9 ISR 4461 Series router	5	$16,952.00	$ 84,760.00
	Server	Dell PowerEdge R750xs Server	8	$ 4,783.92	$ 38,271.36
	Solaris Server	Oracle SPARC T-Series	1	$117,859.99	$ 117,859.99
	Switch	CISCO C9300 48-port access switches	5	$ 5,900.00	$ 29,500.00
	Firewall	Cisco ISA3000 Firewall	2	$ 3,495.00	$ 6,990.00
		Cisco FirePOWER 1120 ASA	1	$ 2,084.30	$ 2,084.30
	Server Rack	22U Server Rack with Vented Doors	2	$ 1,012.00	$ 2,024.00
	Laptop lock	Kensignton lock	60	$ 37.99	$ 2,279.40
	Hard Drive	Seagate Exos X20 ST20000NM007D 20T	1	$ 289.99	$ 289.99
	Alarm System	Honeywell System Sensor	19	$ 83.95	$ 1,595.05
	Video Surveillanc	64 Bundle Channel NVR Security Camera	1	$ 9,799.00	$ 9,799.00
	Manual Pull Stati	Honeywell FireLite BG-12S Single Action	8	$ 61.03	$ 488.24
	Biometric Access	Supreme BS2-OHPW BioStation 2 HID Ca	7	$ 1,298.00	$ 9,086.00
	Humidity/Temper	DWYER Humidity Transmitter	20	$ 142.61	$ 2,852.20
	Water/Flood Sens	Honeywell Home Water Detection Syste	20	$ 139.28	$ 2,785.60
	Fire Extinguisher	STOP-FYRE Classic Automatic Fire Exting	6	$ 3,630.00	$ 21,780.00
	Smoke Detectors	Honeywell SD365 addresssable photoel	12	$ 96.95	$ 1,163.40
	Card Reader	Geovision GV-CS1320 2MP H.264 Camer	19	$ 329.67	$ 6,263.73
	ISP	1 GIG plan @ 12000/year	2	$12,000.00	$ 24,000.00
	Fire/Smoke Curta	Smoke Guard Curtain M2500	10	$ 1,250.00	$ 12,500.00

FIGURE 31: OAKBROOK COST TOTALS



Waukegan					
	Workstation	Lenovo ThinkStation P920's	20	$19,837.99	$ 396,759.80
	Router	Cisco ISR4461/K9 ISR 4461 Series router	5	$16,952.00	$ 84,760.00
	Server	Dell PowerEdge R750xs Server	8	$ 4,783.92	$ 38,271.36
	Solaris Server	Oracle SPARC T-Series	1	$117,859.99	$ 117,859.99
	Switch	CISCO C9300 48-port access switches	5	$ 5,900.00	$ 29,500.00
	Firewall	Cisco ISA3000 Firewall	2	$ 3,495.00	$ 6,990.00
		Cisco FirePOWER 1120 ASA	1	$ 2,084.30	$ 2,084.30
	Hard Drive	Seagate Exos X20 ST20000NM007D 20TI	1	$ 289.99	$ 289.99
	Server Rack	22U Server Rack with Vented Doors	2	$ 1,012.00	$ 2,024.00
	Laptop lock	Kensington lock	20	$ 37.99	$ 759.80
	Manual Pull Stati	Honeywell FireLite BG-12S Single Action	6	$ 61.03	$ 366.18
	Alarm System	Honeywell System Sensor	11	$ 83.95	$ 923.45
	Video Surveillanc	64 Bundle Channel NVR Security Camera	1	$ 9,799.00	$ 9,799.00
	Biometric Access	Supreme BS2-OHPW BioStation 2 HID Ca	7	$ 1,298.00	$ 9,086.00
	Humidity/Temper	DWYER Humidity Transmitter	15	$ 142.61	$ 2,139.15
	Water/Flood Sens	Honeywell Home Water Detection Syste	12	$ 139.28	$ 1,671.36
	Fire Extinguisher	STOP-FYRE Classic Automatic Fire Exting	5	$ 3,630.00	$ 18,150.00
	Smoke Detectors	Honeywell SD365 addresssable photoel	10	$ 96.95	$ 969.50
	ISP	1 GIG plan @ 12000/year	2	$12,000.00	$ 24,000.00
	Fire/Smoke Curta	Smoke Guard Curtain M2500	10	$ 1,250.00	$ 12,500.00
	Card Reader	Geovision GV-CS1320 2MP H.264 Camer	15	$ 329.67	$ 4,945.05

FIGURE 32: WAUKEGAN COST TOTALS



SOFTWARE					
	Endpoint Protecti	Crowdstrike	3	$ 1,000.00	$ 3,000.00
	Event log manage	Manage Engine	3	$ 2,495.00	$ 7,485.00
	Patch Mangemen	Ivanti	3	$ 4,500.00	$ 13,500.00
	Data Protection	Varonis	3	$17,000.00	$ 51,000.00
	Windows Server	Microsoft Windows Server 2022 Standar	2	$ 577.99	$ 1,155.98
	SQL Server	Microsoft SQL Server 2019 Standard Lice	2	$ 618.99	$ 1,237.98
	Red Hat Linux	Red Hat Linux 1 year	1	$ 1,300.00	$ 1,300.00
	Microsoft 365	Email and other services	350	$12.00	$4,200.00
CABLING					
	Console cables	Rollover Console Cable Compatible with	13	$ 25.03	$ 325.39
	Cat6 ethernet cal	CableGeeker Flat Internet Network LAN	300	$ 25.80	$ 7,740.00
	Coaxial cables	10 Ft RG6 Cable Black Indoor Coaxial Ca	100	$ 9.59	$ 959.00
				Grand Total	$5,979,691.36

FIGURE 33: SOFTWARE, CABLING, AND TOTAL COST

15 HARDWARE FIGURES

FIGURE 34: LENOVO THINKSTATION T920 - TOWER

FIGURE 35: DELL LATITUDE 5430 RUGGED LAPTOP

FIGURE 36: ORACLE SPARC T-SERIES T801 - RACK-MOUNTABLE SERVER

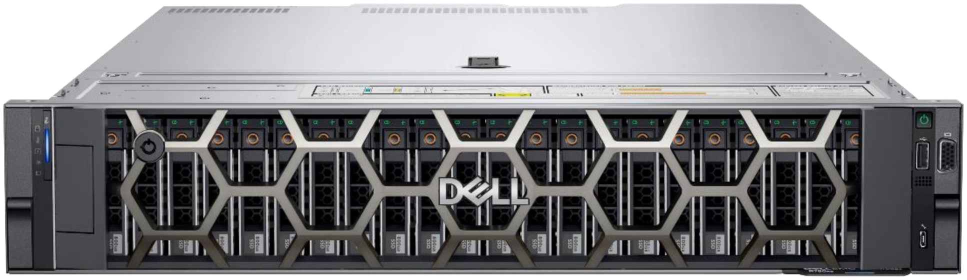


FIGURE 37: DELL POWEREDGE R750XS RACK SERVER

FIGURE 38: CISCO ISR4461/K9 ISR 4461 ROUTER

FIGURE 39: CISCO FIREPOWER 1120 ASA - FIREWALL

FIGURE 40: CISCO ISA3000 FIREWALL

FIGURE 41: CISCO CATALYST 9300 48 PORT SWITCH

FIGURE 42: KENSINGTON LOCKS

FIGURE 43: MOBILE HOTSPOT