Network Design Proposal for the 3rd Floor Computer Lab – King Hall

PROPOSAL FOR IMPLEMENTING WIRED AND WIRELESS SOLUTIONS ON KING HALL'S 3RD FLOOR

Exlexis Archouletta, Jasmine Carvalho, Elsi Castro, Samuel Avila-Varela
Communication Systems 4840-02 | Group 2

Executive Summary

This proposal presents a complete network infrastructure design for Room KH B3018 on the third floor of King Hall at California State University, Los Angeles (CSULA). The goal

is to convert the underutilized space into a modern computer lab supporting 30 student PCs, an instructor workstation, a printer, and wireless access.

The new design includes Gigabit Ethernet, Wi-Fi 6, a 48-port switch, and a firewall/router to ensure high-speed, secure connectivity. All hardware and configurations comply with CSULA's IT standards and support current academic needs such as video conferencing, cloud-based tools, and collaboration platforms.

A feasibility study confirmed the room is suitable for installation, with sufficient space, power, and ventilation. The network is designed to be scalable, with a 10Gbps backbone and modular components to accommodate future growth.

To ensure data protection, a Data Backup and Disaster Recovery Plan has been developed. Backups will run daily and weekly, stored both locally and in the cloud, with regular restoration testing. The disaster recovery plan includes power redundancy, hardware replacement procedures, and recovery objectives to minimize downtime.

The total project cost is estimated at $23,000, providing CSULA with a future-ready, cost-effective lab that enhances student learning and campus technology infrastructure.

Table of Contents

Introduction

The purpose of this project is to design and implement a complete network infrastructure for Room KH B3018, located on the third floor of the B Wing in King Hall at California State University, Los Angeles (CSULA). The proposed computer lab will support 30 student workstations, an instructor PC, a shared printer, and ceiling-mounted Wi-Fi access. The network will meet CSULA IT standards, supporting high-speed internet access and academic tools such as video conferencing, cloud platforms, and collaboration software. The design includes Gigabit Ethernet, Wi-Fi 6, and plans for scalability, security, and disaster recovery.

Project Overview

PROJECT GOALS

The primary goal of this project is to design and implement a modern, reliable, and scalable network infrastructure for Room KH B3018, located on the third floor of King Hall at California State University, Los Angeles (CSULA). This upgraded network will support 30 student workstations, an instructor PC, a shared printer, and wireless connectivity, meeting the needs of both current and future academic applications. Specific goals include:

- Providing high-speed internet access via Gigabit Ethernet and Wi-Fi 6.
- Enabling seamless support for academic tools like video conferencing, cloud-based platforms, and collaborative software.
- Ensuring the network infrastructure is secure, scalable, and able to handle high-bandwidth applications.
- Implementing a disaster recovery plan and data backup system to ensure data integrity and minimize downtime.

SCOPE OF PROJECT

This project encompasses the design and implementation of a complete network infrastructure for Room KH B3018 in King Hall. The scope includes:

- Network Design and Setup: Installing Gigabit Ethernet, Wi-Fi 6 access points, a 48-port switch, and related networking equipment to ensure fast, reliable connectivity.
- Data Backup and Disaster Recovery: Setting up a backup system and disaster recovery plan to ensure data security and business continuity.

- Implementation and Testing: Physical installation of network devices, configuration of equipment, and testing to verify network functionality.
- Support and Maintenance Plan: Providing ongoing support and a plan for regular updates to ensure the network remains operational and secure.

The project **does not include** any renovation or changes to the physical structure of the room beyond the necessary cable management and device installation. It also does not cover user training or upgrades to other areas of King Hall.

Current Infrastructure Overview

King Hall is one of the primary academic buildings at California State University, Los Angeles (CSULA), divided into multiple wings and floors. Room KH B3018, located on the third floor of the B Wing, is currently underutilized and presents an opportunity for conversion into a fully functional computer lab.

The existing network on the third floor includes standard Ethernet connectivity and campus-wide Wi-Fi; however, it experiences inconsistent coverage and network congestion during peak hours. Our proposed design aims to upgrade the infrastructure with dedicated Gigabit Ethernet connections, a centralized 48-port switch, and a ceiling-mounted Wi-Fi 6 access point. These enhancements will support modern academic needs, including high-bandwidth applications, video conferencing, and cloud-based collaboration tools.

Proposed Network Solution

The network for KH B3018 will use a Star Topology with a central 48-port Gigabit switch connecting 30 student PCs, one instructor PC, a shared printer, and a Wi-Fi 6 access point. All devices will use Cat 6 Ethernet cabling for reliable, high-speed connections.

The lab will connect to the internet via a Fortinet FortiGate 40F firewall and CSULA's campus router. Traffic will be segmented into VLANs for students, instructors, and printers to enhance security and performance.

The design supports future scalability, is compliant with CSULA IT standards, and can handle modern academic workloads such as video conferencing, cloud apps, and remote access.

Feasibility Study

Room KH B3018 was physically inspected to assess its suitability for conversion into a modern computer lab. During the walkthrough, detailed photos were taken of all four walls and the ceiling to evaluate space layout, power accessibility, and cable routing options. The room measures approximately 25 feet by 24 feet, which provides sufficient space to accommodate 30 student workstations, an instructor station, a network printer, and supporting network infrastructure.

Key features that make this room feasible for the proposed project include:

- **Power Accessibility:** Multiple power outlets are distributed throughout the room to support all necessary devices.
- **Ceiling Support:** The ceiling structure allows for the installation of a ceiling-mounted wireless access point and the routing of Cat6 Ethernet cables.
- **A** standard HVAC system provides adequate ventilation for electronic equipment.
- **Open Layout:** The open floor plan enables flexible arrangement of desks and networking equipment without causing clutter or obstruction.

The proposed network setup—including a 48-port Gigabit switch, Cat6 cabling, a router, and a firewall that can be implemented efficiently within the existing space, without requiring significant renovations. Overall, KH B3018 offers a practical and well-suited environment for implementing a secure, efficient, and scalable computer lab.

Information on the Existing Network and Application

The current network infrastructure on the third floor of King Hall, particularly in room KH B3018, is a basic wired Ethernet setup designed for general academic and administrative tasks. Each room includes Ethernet ports, and Wi-Fi is available throughout the floor. However, wireless signal strength and reliability are inconsistent in certain areas, especially near the ends of the building.

Typical applications include office productivity tools such as email, document editing, and file sharing via CSULA's campus servers. Video conferencing platforms like Zoom and Microsoft Teams are frequently used for virtual lectures and meetings. A range of academic applications also support student collaboration, research, and classroom instruction.

While the network is stable during light usage, it experiences performance issues, including lag and occasional crashes, during peak hours, particularly with high-bandwidth activities. These challenges highlight the need for a network upgrade that can deliver consistent, high-performance connectivity to support current and future academic needs.

Information on New Applications

As digital learning continues to evolve, the redesigned network will support a range of new academic and administrative applications aimed at enhancing the student experience and enabling future-ready instruction.

ACADEMIC APPLICATIONS

Immersive STEM Solutions

- Biology/Chemistry: Support for virtual dissection tools and molecular modeling software.
- Network Requirements: Low-latency connectivity to ensure smooth simulations; approximately 50+ Mbps bandwidth per workstation.

DATA SCIENCE TOOLS

- Applications: Cloud-based analytics platforms and enhanced data visualization tools for student research.
- Budget Consideration: Open-source alternatives will be explored to reduce licensing costs.

OPTIMIZATION FOR CRITICAL TOOLS

QoS Prioritization for:

- Video conferencing platforms (e.g., Zoom, Microsoft Teams)
- Virtual classroom environments
- Cloud-based software applications

Wi-Fi 6 Deployment to support:

- Mobile learning applications
- VR headsets and immersive lab technologies

CLOUD INTEGRATION

Seamless access to:

- Microsoft 365
- Google Workspace

- Shared academic resources hosted on the cloud

These new applications have been selected not only to improve the quality of education but also to work within budget constraints. By leveraging open-source tools, scalable platforms, and enterprise-grade wireless technology, the network ensures maximum value while supporting modern educational needs.

Technical/Network Requirements/Needs

Room KH B3018 requires a modernized infrastructure to support data-intensive applications and stable, high-speed connectivity. The primary requirement is upgrading to Gigabit Ethernet at the user level and installing Wi-Fi 6 access points to support a growing number of connected devices and ensure reliable wireless performance.

The network backbone should be upgraded to 10 Gbps to handle increased internal data traffic and ensure efficient communication across the third floor.

A comprehensive traffic analysis w ted to identify peak usage times and potential bottlenecks. This data will inform Quality of Service (QoS) policies that prioritize real-time applications like video conferencing and cloud collaboration tools.

To maintain high performance and reliability, the network will incorporate a centralized monitoring system that enables IT staff to detect, diagnose, and resolve issues proactively.

Security measures will include the deployment of firewalls, intrusion detection systems (IDS), and strong encryption protocols to safeguard sensitive academic and personal data.

Integration of a New Application with Network Design

The proposed network design for the third floor is built to support the seamless integration of modern academic and administrative applications. With cloud-based platforms like Microsoft 365 and Google Workspace now central to daily operations, the network is optimized for consistent throughput and low-latency access.

To ensure smooth performance of real-time tools such as high-definition video conferencing and virtual classrooms, Quality of Service (QoS) settings will prioritize bandwidth allocation for latency-sensitive applications—crucial for today's hybrid learning environments.

To support emerging technologies, the network includes high-capacity switches and low-latency wireless access points for fast, reliable data transmission. Anticipating the use of

IoT devices like environmental sensors and IP-based security systems, the design includes VLAN segmentation to manage traffic efficiently and enhance security.

Overall, this network represents a substantial infrastructure upgrade designed to meet both current demands and future growth.

Scalability and Future Expansion Plan

The proposed network is designed with scalability in mind to support the future growth of King Hall's 3rd floor. It uses structured cabling and high-capacity backbone links (10 Gbps or higher), allowing easy expansion without major rewiring. New switches, access points, or devices can be added with minimal disruption.

As student enrollment, research needs, and technology use grow, the network will scale to meet demands. Support for Wi-Fi 6 and future compatibility with Wi-Fi 7 will ensure fast, reliable wireless access for many users at once. This is ideal for streaming, collaboration, and cloud tools.

Centralized management tools will help IT monitor performance, update systems, and manage access remotely. The design also supports IPv6 and meets modern security standards, making it flexible and future-proof.

By planning for expansion now, CSULA avoids costly upgrades later and ensures long-term network reliability and performance.

Network Designs and Topologies

PHYSICAL DIAGRAM

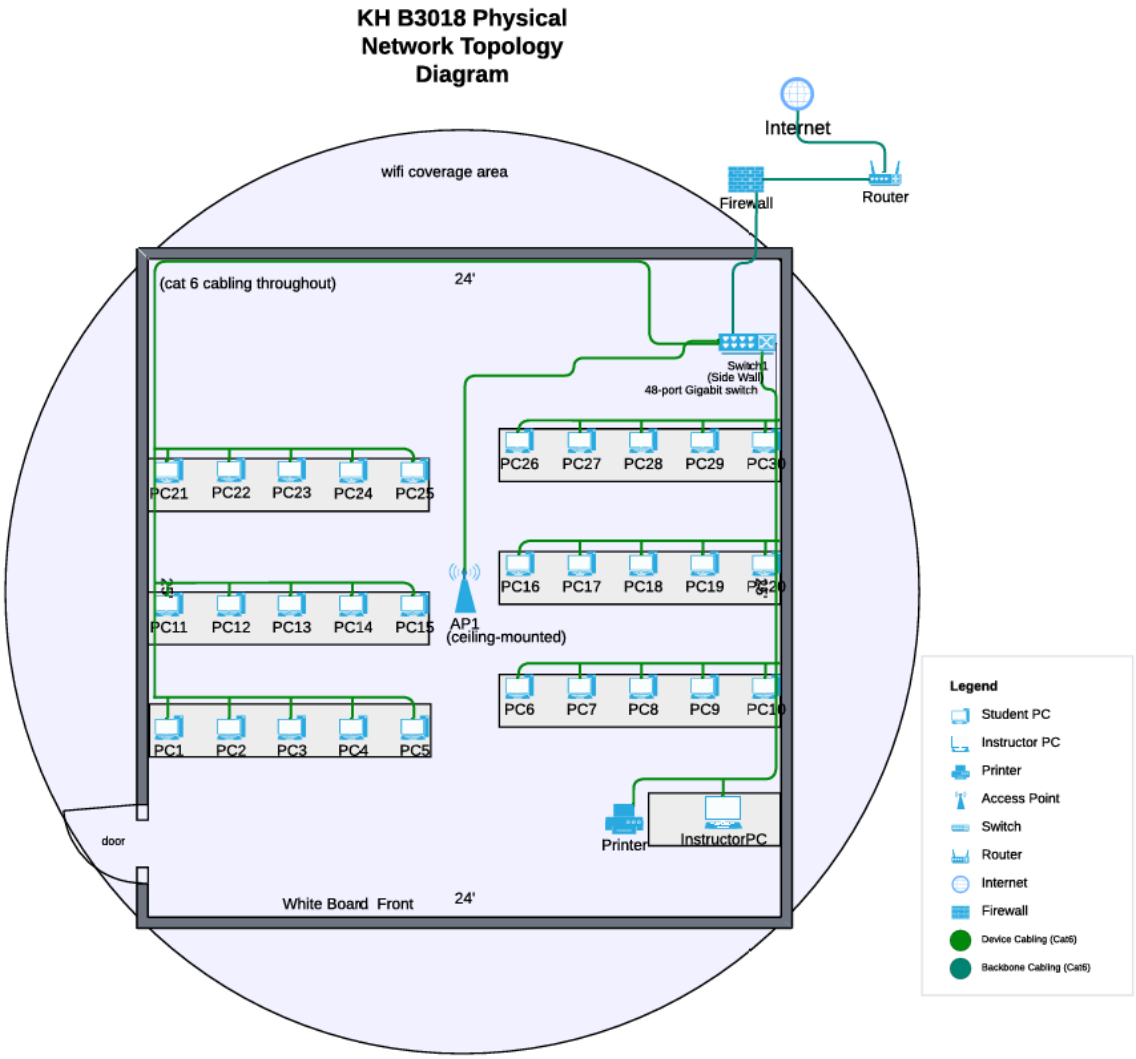

Figure 1 – KH B3018 Physical Network Topology

This diagram illustrates the real-world layout of the KH B3018 computer lab, designed using star topology. It includes 30 student PCs, an instructor station, a ceiling-mounted Wi-Fi access point, a shared printer, a 48-port Gigabit switch, and firewall/router equipment. All wired devices are connected using Cat 6 Ethernet cabling routed along the room's perimeter.

LOGICAL DIAGRAM

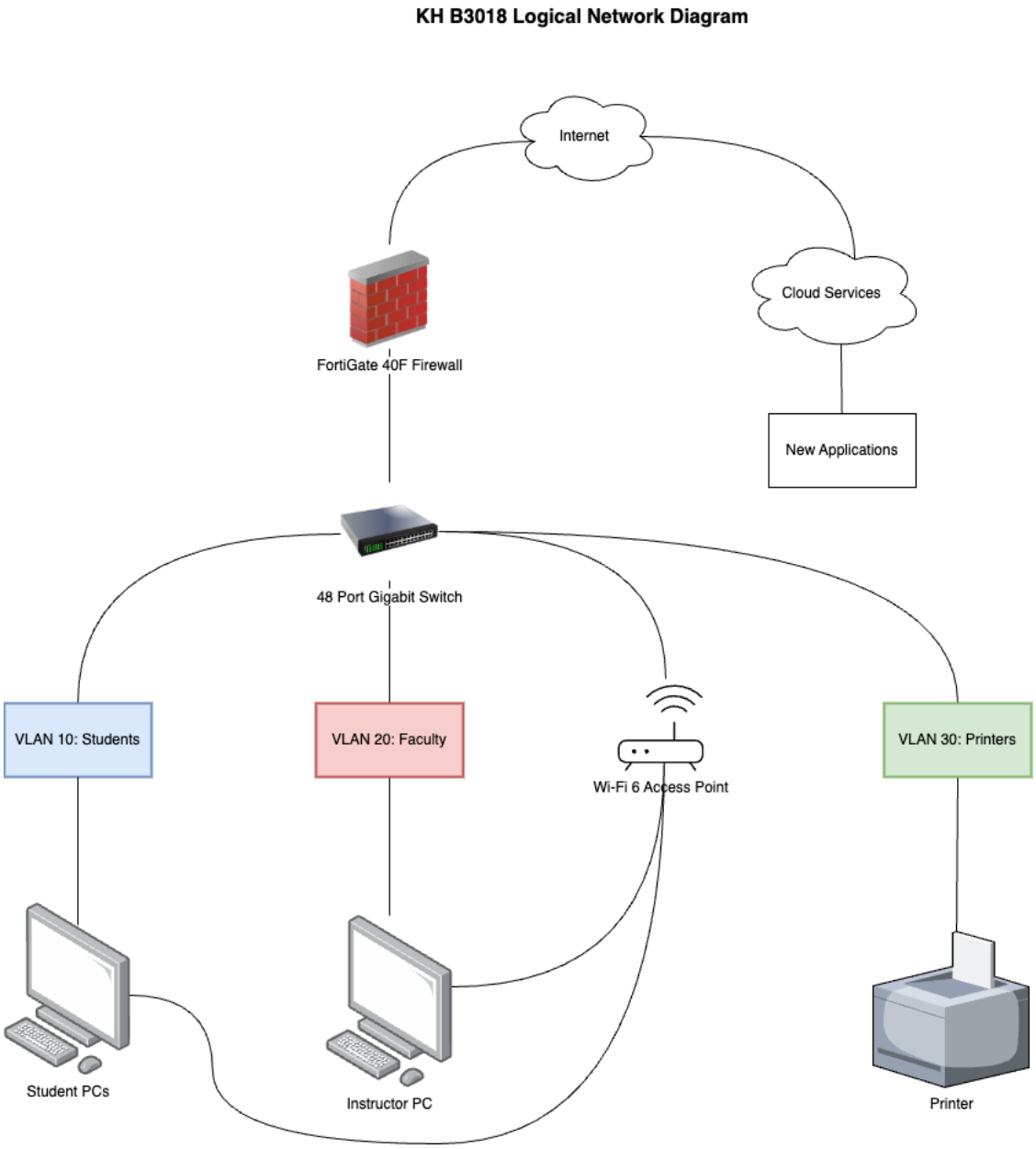

Figure 2 – KH B3018 Logical Network Diagram

This diagram illustrates the logical network design, featuring Internet and Cloud Services connected to a firewall which routes traffic through a 48-Port Gigabit switch. The switch will then distribute connections to VLANs and a Wi-Fi 6 access point, providing wireless access for students, an instructor station, and a shared printer.

Collaboration on Implementation Plan

To ensure successful deployment of the KH B3018 network upgrade, the implementation plan will follow phased steps:

Phase 1: Preparation (Weeks 1–2)

Design Finalization

- Confirm final network design, including VLAN configuration (students, faculty, printers).
- Approve access point placement as shown in Figure 1.

Purchasing and Logistics

- Procure all required hardware (switch, firewall, Cat6 cables), based on the Budget Table.
- Schedule licensed technicians for installation and setup.

PHASE 2: INSTALLATION (WEEKS 3–4)

Physical Deployment

- Mount the Wi-Fi 6 access point on the ceiling.
- Install the 48-port Gigabit switch.
- Run Cat6 cabling along the room's perimeter for clean and efficient cable management.

Configuration

- Set up VLANs and Quality of Service (QoS), prioritizing Zoom, VR, and real-time applications.
- Configure and test the firewall to restrict non-academic traffic.

PHASE 3: TESTING (WEEKS 5–6)

Performance Validation

- Perform stress testing with 30+ student devices to assess bandwidth and stability.
- Verify low-latency performance for VR and other high-demand applications.

User Training

- Develop reference guides for faculty and staff (e.g., accessing VLANs, connecting to the printer).
- Train IT personnel in managing new network tools and hardware.

PHASE 4: GO LIVE AND MONITORING (WEEK 7 AND BEYOND)

Lab Launch

- Open the lab for limited classroom use (1–2 classes) as a soft rollout.
- Monitor bandwidth usage and system performance closely.

Ongoing Improvement

- Conduct monthly reviews to evaluate performance.
- Adjust as needed to ensure optimal operation and support future needs.

Implementation Costs, Contracts, and Support Plan

LEGAL CONTRACTUAL TERMS AND CONDITIONS

All hardware and software acquisitions for this project will follow California State University, Los Angeles (CSULA) procurement guidelines to ensure compliance with IT security policies, accessibility standards, and sustainability goals.

All networking equipment—including switches, routers, access points, and cabling—must be sourced from certified vendors offering standard warranties (minimum one year). Installation will be carried out by licensed contractors or CSULA IT personnel, following all safety codes, cable management standards, and fire regulations.

Software licensing for network management, security, and endpoint protection must adhere to CSU system-wide license agreements. Any third-party service providers will be required to sign contracts that include service level agreements (SLAs), liability terms for hardware failure or misconfiguration, and limitations on access to CSULA internal systems.

No network hardware will be installed without prior approval from CSULA's IT department.

BUDGET AND EXPENSES

Item	Quantity	Unit Price	Total	Description / Model
Student Desktop PCs	30	$600	$18,000	Dell OptiPlex 7010 SFF (i5, 16GB RAM, 256GB SSD)

Instructor PC	1	$800	$800	Dell OptiPlex 7010 (higher config for dual display)
Network Printer	1	$300	$300	HP LaserJet Pro M404dn – network-capable
48-Port Gigabit Switch	1	$500	$500	Cisco CBS250-48T-4G
Ceiling-Mounted Wi-Fi 6 Access Point	1	$250	$250	Ubiquiti UniFi 6 Lite
Firewall / Router Combo	1	$600	$600	Fortinet FortiGate 40F
Cat6 Ethernet Cables	35	$10	$350	Monoprice / Ultra Clarity Cat6, 10ft
Installation Labor	-	-	$1,200	Cabling, mounting, testing, configuration
Software Licenses	-	-	$1,000	Windows 11 EDU Volume License, endpoint security
Total Estimated Cost	-	-	$23,000	

COST-BENEFIT ANALYSIS

The estimated project cost of $23,000 enables CSULA to establish a secure, high-performance, and scalable computer lab in Room KH B3018. This investment supports academic computing, cloud-based applications, and video conferencing for hundreds of students each semester.

Compared to renting off-site lab space or relying on temporary technology setups, this solution offers long-term cost savings and greater reliability. The chosen hardware and structured cabling are expected to remain effective for 5–7 years with minimal upgrade needs. The modular network design also allows for easy expansion as future academic and technological requirements grow.

MAINTENACE AND SUPPORT PLAN

Ongoing maintenance will be handled by CSULA's IT department, supported by designated lab assistants. Regular physical inspections of the switch, firewall/router, and access point will be conducted to ensure reliable operation and minimize downtime.

Software updates, firmware patches, and endpoint security will be deployed using campus-wide remote management tools. Any hardware failures will be resolved through manufacturer warranties or existing CSULA service agreements.

Basic lab supplies, such as printer toner and paper, will be restocked by support staff as needed. Help desk services will be available during scheduled lab hours to assist students and instructors with any technical issues.

Security and Compliance Plan

To ensure a secure and policy-compliant network in KH B3018, the following measures will be implemented:

- **Firewall & Access Control**: A Fortinet FortiGate 40F firewall will manage external traffic using access control lists and MAC filtering. VLAN segmentation will separate student, instructor, and printer traffic to enhance internal security.

- **Endpoint Protection**: All lab computers will run campus-approved antivirus software and receive regular OS and security updates managed by CSULA IT.
- **User Authentication**: Access to lab systems and shared resources will require campus Single Sign-On (SSO) credentials. Admin privileges will be limited to authorized personnel only.

- **Physical Security**: Networking equipment will be secured in locked cabinets. Physical access to the room will be restricted outside scheduled lab hours.

- **Compliance Standards**: The network design adheres to CSU IT policies, complies with FERPA requirements, and follows best practices based on NIST 800-53 for academic environments.
- **Monitoring & Incident Response**: System and access logs will be monitored, with CSULA IT managing any security incidents in accordance with established campus protocols.

Data Backup Policy

DATA BACKUP PLAN

To maintain secure and uninterrupted access to lab data, the following data backup strategies will be utilized through an automated system:

Data Backup Schedule:

To protect against data loss, the system will follow a structured backup schedule:

- Incremental backups will be performed daily to capture recent changes and updates
- Weekly full backups will be scheduled every Sunday night.

Backup Storage Locations:

- All backups will be stored on a local Network-Attached Storage (NAS) device placed in a secure, access-controlled server cabinet on the 3rd floor of King Hall.
- A secondary backup copy will be uploaded to a cloud-based storage solution aligned with campus IT infrastructure to ensure redundancy.

Data Coverage:

The following data categories will be included in all backup operations:

- Network logs and administrative settings.
- Configuration settings and system files for lab workstations and networking devices.
- User files for both students and faculty, located in personal profiles or shared directories.

Data Retention:

To balance data accessibility and storage efficiency, the following retention policy will be applied:

- Daily backups will be preserved for 7 days.
- Weekly backups will be retained for 3 months.
- Monthly backup snapshots will be archived for 6 months.

Automation and Oversight:

- The IT team will conduct monthly restoration tests to confirm the recoverability and integrity of backed-up data.

- Backup processes will be managed using automated backup software equipped with monitoring and notification features.

Disaster Recovery Plan

RECOVERY PLAN

In the event of a disruptive incident, such as a system malfunction, natural disaster, theft, or cybersecurity breach, a structured recovery plan will be followed to minimize downtime and data loss.

Recovery Objectives:

- Recovery Time Objective (RTO): Resume essential network operations within 4 to 6 hours.
- Recovery Point Objective (RPO): Critical systems will maintain a target RPO of 4–6 hours, ensuring minimal data loss in the event of a failure with other systems target RPO is 12 hours.

Recovery Process

- In the event of hardware failure, pre-authorized vendors will rapidly supply replacement devices.
- Data will be restored from the latest available backup, prioritized based on usage.
- IT personnel will reinstall and configure software, re-establish network connections, and verify user access.

Redundancy and Continuity Measures:

- Network architecture diagrams and configuration files will be securely backed up offsite and stored in the cloud to enable rapid reconfiguration if needed.

Testing and Documentation:

- Biannual disaster recovery drills will be conducted to evaluate response readiness and validate backup functionality.
- Results of tests, recovery logs, and any procedural updates will be documented to meet compliance and institutional standards.