COIT13236 – Cyber Security Project

**KN University Network Design**

**Technical Artefacts**

1. **Client’s Details**

Group 02

|  |  |  |
| --- | --- | --- |
| **Name** | **Role** | **Student ID** |
| Krishan Himesh Abeyrathne | System Administrator | 12217274 |
| Narayan Parajuli | System Security Analyst |  |

# Client’s Overview

KN University offers a quality educational experience at the Melbourne, Sydney, Brisbane, and Adelaide campuses. To this end, the network infrastructure is another instrumental ingredient in the process. This document describes the university's network environment's key physical and logical characteristics for academic and administrative purposes.

# Business Goals

1. High-Speed Internet Access

It is important to provide internet connection on all the campuses to enhance academic and administrative tasks.

1. Secure and Reliable Wi-Fi Coverage

Ensure that all the buildings within the campuses, including common areas, are connected to safe and efficient Wi-Fi.

1. Scalability for Future Growth

Implement a plan for scalability in a network infrastructure to account for future growth in enrolment, as well as new faculty and technologies.

1. Centralized Network Management

Ensure the organization has an effective centralized network management system to minimize the challenges of monitoring, troubleshooting, and configuring the available networks adequately.

1. High Performance for Academic and Administrative Applications

Ensure high network performance by supporting all the e-learning platforms, research databases, and administrative systems.

# Technical Requirements

1. **Wired and Wireless Connectivity**

* Wired Network: Provide wired network connectivity by implementing new Cat6 and Fiber Optic cables to prevent failures in conducting crucial academic and administrative operations.
* Wireless Network: Set up a fully functional wireless network that can provide sufficient coverage to lecture halls, libraries, laboratories, offices, and other general spaces. Check if the wireless network complies with the current standards (e.g., WiFi 6).

1. **Security Measures**

* Firewalls: Use superior firewalls to prevent external threats from accessing the network.
* VPNs: Establish Virtual Private Networks (VPNs) that would give people at the university secure access to the network.
* IDS/IPS: Deploy Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to detect and prevent malicious activities.
* Access Control: Strict access control is required to ensure that only permitted persons can touch restricted data or documents.

1. **IoT Device Integration**

* IoT Deployment: IoT devices are used for security and monitoring of the environment and campus buildings.
* Network Segmentation: You should implement network segmentation to separate IoT devices from the standard corporate network for better security and network performance.

1. **Cloud Service Integration**

* Cloud Resources: Incorporate cloud services for storage, backup and/or computational purposes. Optimize the transition between internal / on-premises and cloud infrastructure.
* Security in the Cloud: Ensure that cloud-stored and cloud-processed data are protected from unauthorized access using encryption and security vulnerability assessments.

1. **Scalability and Manageability**

* Scalable Infrastructure: Ensure that the design of the network is easily scalable to accommodate new buildings, users, and devices, among others, without requiring reconstruction of the entire network.
* Centralized Management: Integrate a network management system that will enable real-time monitoring, configuration, and resolution of problems. Ensure that the tools used for the frequent and recurrent tasks and information updates are automated.

1. **Performance and Optimization**

* Performance Metrics: Set performance standards and always check the status of the network to enhance its performance.
* Load Balancing: Utilize load balancing methodologies to avoid traffic concentration in a particular point in the network, making the network slow, often with congestion points.

1. **Compliance and Regulatory Requirements**

* Data Protection: Compliance with the Data Protection Act and policies, including GDPR and other countries’ data protection regulations.
* IT Policies: Comply with the IT policies and/or frameworks established by KN University to design and implement network solutions.

1. **User Experience**

* Easy Access: Make sure that all the network systems are easily negotiable, especially for students, faculty members, administrators, and even visitors.
* Support and Training: Education/Training of the network users on network usage to ensure that they can manage to use the resources available in the network.