COIT13236 – Cyber Security Project

**KN University Network Design**

**Technical Artefacts**

**2. Client Requirements**

**Group 02**

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

# Client’s Overview

KN University is a prestigious university in Australia with Melbourne, Sydney, Brisbane, and Adelaide campuses. The university offers undergraduate programs across four faculties. The schools include those in engineering, technology, law, and business. Every campus has teaching and administrative facilities that enhance education provision.

# Client Requirements

## Business Goals

* High-Speed Internet Access: Ensure all campuses connect to high-speed internet to enable academic and administrative work.
* Secure and Reliable Wi-Fi Coverage: Ensure connectivity and wireless networking are available in all the buildings across campus and common areas.
* Scalability for Future Growth: Make certain the implemented networks can grow or expand after some time to cover other new students, faculties or any new technologies.
* Centralized Network Management: These solutions include Organising an integrated network management system to supervise, diagnose, and alter if necessary.
* High Performance for Academic and Administrative Applications: Ensure optimum network performance for the learning management systems, databases, and administrative applications.

## Technical Requirements

### Wired and Wireless Connectivity

* **Wired Network:** Install a powerful wired network through the use of Cat6 cables and Fibre Optic cables, which will enable the institution to have a strong network for core functions such as learning and administration.
* **Wireless Network:** Establish sufficient wireless connectivity in all the buildings, such as classrooms, lecture halls, libraries, laboratories, workplaces, and other social settings. Check that the wireless network complies with the current standards (e.g., Wi-Fi 6).

### Security Measures

* **Firewalls:** Use state-of-the-art firewalls to shield the network from the outside world.
* **VPNs:** specified Virtual Private Networks (VPNs) to allow authorized users to connect remotely to the university’s network securely.
* **IDS/IPS:** Use IDS and IPS to track and terminate unlawful activities on the firm’s computer system.
* **Access Control:** Realize strict levels of access control to touch base with the authorized personnel to access the confidential information.

### IoT Device Integration

* **IoT Deployment:** Connect and apply IoT devices to protect the campus, monitor the environment, and manage the buildings.
* **Network Segmentation:** This involves partitioning of IoT devices from the organizational network to improve security while at the same time improving the performance of the network.

### Cloud Service Integration

* **Cloud Resources:** Integrate with cloud services for storing and backing up information and utilising computing resources. Foster correct combination of on-premises and cloud infrastructures.
* **Security in the Cloud:** Ensure effective security procedures are adopted for both stored and data processed in the cloud, including encryption and constant vulnerability assessments.

### Scalability and Manageability

* **Scalable Infrastructure:** Ensure that the network can be easily expandable with new buildings, users and/or devices, meaning that expansion will not require a complete overhaul of the whole design.
* **Centralized Management:** Use a centralized network management tool for monitoring and configuring the network and troubleshooting as and when necessary. Using automation tools for tasks and updates, leverage the regular work processes.

### Performance and Optimization

* **Performance Metrics:** After creating a simple network, define specific activity standards and keep track of the system’s performance constantly.
* **Load Balancing:** Helps balance the network traffic so that different areas of the networks do not get overloaded with traffic, which may slow down the network.

### Compliance and Regulatory Requirements

* **Data Protection:** Compliance with data protection laws like the GDPR or the local data protection laws.
* **IT Policies:** IT policies can also be applied to maintain the policies of KN University’s IT department and follow the most effective network design and implementation standards.

### User Experience

* **Easy Access:** Make the network easy to use and accessible to students, faculty, administration and all other individuals who will be using that network.
* **Support and Training:** Create awareness for the various network users so they can exploit the available resources.

Through such aspects of business and technical concern, the network design will help KN University to provide a network infrastructure that will favour its objectives of securing an effective, secure, and efficient network that will support and improve the academic/administrative end user’s experience.