COIT13236 – Cyber Security Project

**KN University Network Design**

**Technical Artefacts**

1. **Network Security Plan**

Group 02

|  |  |  |
| --- | --- | --- |
| **Name** | **Role** | **Student ID** |
| Krishan Himesh Abeyrathne | System Administrator | 12217274 |
| Narayan Parajuli | System Security Analyst | 12144248 |

# Network Security Plan

**Network Security Plan:**

* A Network Security Plan ensures the university's network is protected against threats, maintains data integrity, and provides secure access to resources. Below is a condensed plan that covers key elements of network security.

**. Objectives**

* **Confidentiality:** Protect sensitive data.
* **Integrity:** Ensure data is accurate and unaltered.
* **Availability:** Ensure network resources are accessible.
* **Compliance:** Meet legal and regulatory requirements.

**Key Components:**

**Firewalls**

* **Purpose:** Control traffic between internal and external networks.
* **Types:**
  + **Perimeter Firewalls:** Filter external traffic.
  + **Internal Firewalls:** Segment internal network traffic.

**Intrusion Detection and Prevention Systems (IDPS)**

* **Purpose:** Detect and prevent malicious activities.
* **Types:**
  + **Network-based IDPS:** Monitors network traffic.
  + **Host-based IDPS:** Monitors individual devices.

**Virtual Private Network (VPN)**

* **Purpose:** Secure remote access.
* **Types:**
  + **Site-to-Site VPN:** Connects campus networks securely.
  + **Client-to-Site VPN:** Provides access for remote users.
* **Encryption:** Use strong encryption (e.g., AES-256).

**Access Control**

* **Purpose:** Restrict access based on user roles.
* **Mechanisms:**
  + **Role-Based Access Control (RBAC)**
  + **Multi-Factor Authentication (MFA)**

**Network Segmentation**

* **Purpose:** Isolate different network segments.
* **Techniques:**
  + **VLANs:** Separate traffic types.
  + **Subnetting:** Divide IP address ranges.

**Encryption**

* **Purpose:** Protect data at rest and in transit.
* **Types:**
  + **Data-at-Rest Encryption:** For stored data.
  + **Data-in-Transit Encryption:** For data being transmitted.

**Security Information and Event Management (SIEM)**

* **Purpose:** Monitor and respond to security events.
* **Features:**
  + **Log Management**
  + **Event Correlation**
  + **Incident Response**

**Patch Management**

* **Purpose:** Keep systems updated.
* **Process:**
  + **Inventory Management**
  + **Patch Deployment**
  + **Testing**

**Policies and Procedures**

**Network Security Policy**

* **Guidelines:** Access control, acceptable use, incident response.

**Incident Response Plan**

* **Steps:** Detection, analysis, containment, eradication, recovery, and lessons learned.

**Data Protection Policy**

* **Components:** Data classification, handling procedures.

**User Training**

* **Topics:** Phishing, password management, and safe internet use.

**Risk Management**

**Risk Assessment**

* **Purpose:** Identify and evaluate risks.

**Risk Mitigation**

* **Strategies:** Apply controls, update policies, enhance training.

**Continuous Monitoring**

* **Tools:** Network monitoring, SIEM systems, and IDPS.