COIT13236 – Cyber Security Project

**KN University Network Design**

1. **Network Security Plan**

Group 02

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

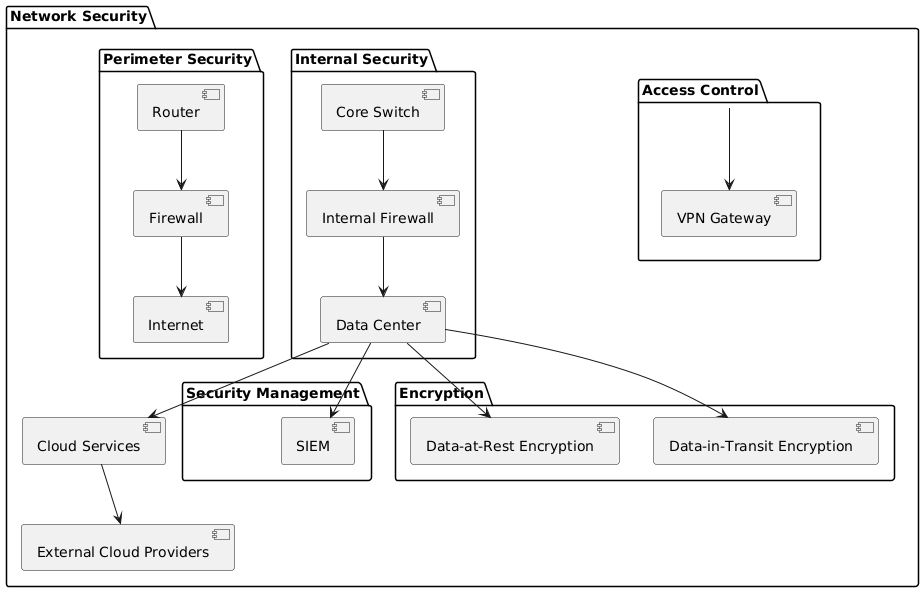
# Network Security Plan

**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:** Guaranteeing the secrecy of delicate information includes a comprehensive methodology that incorporates information classification, access control systems, encryption, secure data storage, access strategies, checking and reviewing, user training, and a robust incident response plan.
* **Integrity:** Ensuring data integrity includes executing measures that shield data from unapproved change and defilement, ensuring its accuracy and consistency all through its lifecycle. This incorporates processes, technologies, and strategies intended to detect and prevent data altering, as well as mechanisms to check data accuracy.
* **Availability:** Ensuring the accessibility of network resources is critical for keeping up with continuous access to data and services for students, workforce, and staff. This includes carrying out measures to prevent downtime, immediately recuperate from interruptions, and keep up with optimal performance.
* **Compliance:** Consistence with legitimate and administrative prerequisites is fundamental for keeping up with the integrity, confidentiality, and accessibility of network resources while guaranteeing the college adheres with material regulations, guidelines, and norms.



**Fig: Network Security Plan**

The KN University network security architecture is shown in the above diagram. The network's first line of defence is perimeter security. The router that links the university's network to the internet is one of its components. By filtering and regulating all data entering and leaving the network, the firewall serves as a security barrier. By limiting access to the network to just safe and approved traffic, this configuration guards against external threats coming from the Internet. The network of the university is shielded from within by internal security. Within the network, data flow is controlled and directed by the Core Switch. An internal firewall protects critical resources by keeping an eye on and managing internal communications. This adds an extra layer of protection. The university stores and maintains its vital data in the Data Centre, which serves as the hub of the network's information systems.

By using a VPN Gateway, Access Control makes sure that only authorised users can connect to the university's network, even from faraway locations. Utilising a SIEM system to track and examine security activity is known as security management. This helps identify and address possible risks. To improve and maintain its digital services, the institution also makes use of cloud services, which establish connections with outside cloud providers. The process of safeguarding sensitive data is called encryption. Data-at-Rest encryption protects stored data by making sure that, even if someone gains access to it, they are unable to read it without the necessary authorisation. Data-in-Transit Encryption safeguards data while it travels over the network, preventing interception or manipulation while it is being sent from one location to another.

The figure demonstrates how the various elements of network security are connected to each other and contribute to the overall security of the KN University network.

**Key Components:**

**Firewalls**

* **Purpose:** Their basic purpose is to make a barrier between a trusted internal network, and untrusted external networks, like the web. Thusly, firewalls help safeguard against unapproved access, cyber threats, and data breaches. Example: Norton 360 Suite
* **Types:**
  + **Perimeter Firewalls:** Their basic role is to make a barrier between a trusted internal network, and untrusted external networks, like the web. Thusly, firewalls help safeguard against unapproved access, cyber threats, and data breaches.
  + **Internal Firewalls:** Internal firewalls, otherwise called segmenting firewalls, are deployed inside an internal network to make various security zones. Internal firewalls can detach basic or delicate areas like finance, HR, or innovative work from the rest of the network.

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

* **Purpose:** Intrusion Detection and Prevention Systems (IDPS) are intended to identify and prevent malicious activities inside a network or framework. They play a significant part in cybersecurity by recognizing expected dangers, cautioning administrators, and making mechanized moves to mitigate risks.
* **Types:**
  + **Network-based IDPS:** Network-Based IDPS (NIDPS) are deployed to monitor and dissect network traffic for indications of malicious movement. They are commonly situated at key points within a network, like gateways, switches, and routers, to give extensive oversight of the data coursing through the network.
  + **Host-based IDPS:** Host Based IDPS (HIDPS) are introduced directly on individual devices or hosts, like servers, workstations, or endpoints. They focus on observing and examining activities well defined for each host to detect and prevent threats.

**Virtual Private Network (VPN)**

* **Purpose:** A Virtual Private Network (VPN) is a technology that gives secure remote admittance to a network over the web. VPNs utilize solid encryption conventions to safeguard information on the way, guaranteeing that any captured information is unreadable without the encryption keys.
* **Types:**
  + **Site-to-Site VPN:** A Site-to-Site VPN is a method used to safely connect at least two or more networks, commonly corporate or hierarchical LANs, over the web. The main role of a Site-to-Site VPN is to safely connect geographically scattered campuses, permitting them to share assets and information safely over a public network like the internet.
  + **Client-to-Site VPN:** A Client-to-Site VPN, otherwise called Remote Access VPN, permits individual clients to interface with a private network from remote areas. The main role of a client-to-Site VPN is to give remote clients secure and encrypted access to an organization's internal network. This guarantees that sensitive information and communications stay secured, in any event, when accessed over possibly unreliable public networks like home Wi-Fi or public hotspots.
* **Encryption:** Encryption is a security process that changes data into an encoded design, making it unreadable to unauthorized users. Strong encryption algorithms, for example, AES-256, give a strong safeguard against cyber threats, ensuring the secrecy and security of data sent over possibly insecure networks.

**Access Control**

* **Purpose:** Access control is a safety measure that manages who or what can view or use resources in a computing environment. The basic role of access control is to restrict access to delicate data and critical frameworks in view of user roles and consents.
* **Mechanisms:**
  + **Role-Based Access Control (RBAC):** RBAC is a method for managing access to assets based on the roles of individual clients inside an organization. The main role of RBAC is to simplify and smooth out the management of client permissions by allotting roles instead of individual permissions to every client. This approach guarantees that clients have fitting access based on their work capabilities and obligations.
  + **Multi-Factor Authentication (MFA):** MFA is a security mechanism that expects clients to give at least two or more verification factors to get access to a resource. The basic role of MFA is to diminish the risk of unapproved access by guaranteeing that regardless of whether one validation factor is compromised, other factors are required to get access.

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

* **Purpose:** Security Information and Event Management (SIEM) is a comprehensive approach to deal with cyber security that consolidates Security Information Management (SIM) and Security Event Management (SEM) to provide real-time analysis, monitoring, and reaction to security events inside an organization. The main role of SIEM is to improve a network security pose by giving incorporated perceivability into network activities, distinguishing potential security dangers, and empowering quick reaction to incidents.
* **Features:**
  + **Log Management:** Log management refers to the process of gathering, storing, and analysing log information created by different gadgets, applications, and frameworks inside a network. SIEM frameworks gather log information from many sources, including network gadgets (routers, switches), security machines (firewalls, IDS/IPS), servers, applications, and endpoint gadgets.
  + **Event Correlation:** Event correlation is the method involved with analysing and corresponding log information from various sources to identify patterns and detect potential security dangers. SIEM frameworks use predefined rules, heuristics, and progressed examination to correlate events and create significant security cautions.
  + **Incident Response:** Incident response refers to the actions initiated by a university to distinguish, examine, and respond to security occurrences. SIEM systems play a critical part in working with and automating the incident response process.

**Patch Management**

* **Purpose:** The purpose of patch management is to guarantee that product and frameworks are up to date with the latest patches and updates. This is urgent for keeping up with the security, stability, and performance of systems.
* **Process:**
  + **Inventory Management:** Inventory management includes maintaining a comprehensive list of all products, applications, and frameworks inside an organization.
  + **Patch Deployment:** Patch deployment is the process of applying patches to programming and frameworks to address weaknesses, fix bugs, or improve functionality.
  + **Testing:** Testing includes approving that patches and updates are applied accurately and don't present new issues or conflicts.

**Policies and Procedures**

**Network Security Policy:** The Network Security Policy lays out rules and guidelines for safeguarding an organization's network foundation. Clients ought to just approach the network resources important for their roles.

* **Guidelines:**

**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:** Risk evaluation is an essential part of risk management. Its main role is to identify, assess, and focus on risks to an association's resources, tasks, and goals. By understanding these dangers, associations can develop methodologies to mitigate or manage them effectively, guaranteeing the continuity and strength of their operations.

**Risk Mitigation**

Risk mitigation implies implementing strategies and activities to decrease the probability and effect of identified risks. The objective is to limit likely dangers and weaknesses, consequently safeguarding a network resources, tasks, and goals. Convey firewalls to control and screen network traffic, preventing unapproved access and alleviating outer dangers. Occasionally survey and update security approaches and methods to guarantee they stay important and successful in tending to current dangers. Provide training on general

security practices, including perceiving phishing attempts, safe web use, and legitimate treatment of sensitive data.

**Continuous Monitoring**

Persistent checking includes the continuous perception of a university's IT environment to identify and respond to security dangers and performance issues progressively. Network observing devices track the performance, accessibility, and security of network framework. They give bits of knowledge into network traffic, gadget status, and potential issues that could affect network performance or security.

# References

International Organization for Standardization (ISO) (2024) ISO 31000:2018 Risk Management Guidelines. Available at: https://www.iso.org/iso-31000-risk-management.html (Accessed: 3 August 2024).

SANS Institute (2024) Network Security Policy. Available at: https://www.sans.org/security-resources/policies/network-security-policy (Accessed: 3 August 2024).

Cybersecurity & Infrastructure Security Agency (CISA) (2024) Multi-Factor Authentication. Available at: https://www.cisa.gov/multi-factor-authentication (Accessed: 3 August 2024).

Microsoft (2024) Encrypting Data Using AES-256. Available at: https://docs.microsoft.com/en-us/windows/win32/seccrypto/encrypting-data-using-aes (Accessed: 3 August 2024).