**Orilla, Ma. Althea B.**

**BSIT 3106 IM**

1. **Network Security**

* **Definition:** Network security refers to the technologies, policies, people, and procedures that defend any communication infrastructure from cyberattacks, unauthorized access, and data loss.
* **Examples:**
* Multi-Factor Authentication (MFA).
* Encryption
* Virtual Private Networks (VPNs) that secure remote access to a network.

1. **Endpoint Security**

* **Definition:** Endpoint security is the process of protecting devices like workstations, servers, and other devices (that can accept a security client) from malicious threats and cyberattacks.
* **Examples:**
* Antivirus software installed on a laptop.
* Application Control
* Mobile Device Management (MDM) solutions that secure mobile devices.

1. **Information Security**

* **Definition:** Information security, often referred to as InfoSec, refers to the processes and tools designed and deployed to protect sensitive business information from modification, disruption, destruction, and inspection.
* **Examples:**
* Data Encryption
* Access Control
* Security Awareness Training

1. **Application Security**

* **Definition:** Application security, or app sec*,* is the practice of using security software, hardware, techniques, best practices, and procedures to protect computer applications from external security threats.
* **Examples:**
* Web Application Firewalls (WAF)
* Secure coding practices that prevent common vulnerabilities.
* Regular security patches and updates to fix software vulnerabilities.