South East Asian Institute of Technology, Inc
College of Information and Communication Technology
Crossing Rubber, Tupi, South Cotabato

An Information Assurance and Security Policies Documentation on

TITLE

As partial requirement for the Subject

IT 421

Information Assurance and Security 2

By-

{Last Name, First Name}

TABLE OF CONTENT

Table of Contents

I. Introduction

- **Purpose**- Describe the purpose of this document, such as safeguarding information and assets, protecting against unauthorized access, and ensuring data integrity.
- **Scope**- Define the scope, including the systems, data, and processes the policies cover.
- **Audience**- Identify who should follow these policies (e.g., all system users, administrators, IT personnel).

II. Overview of Security Principles

- **Key Security Objectives**- Outline goals, such as confidentiality, integrity, and availability.
- **Compliance Requirements**- Mention applicable regulations (e.g., GDPR, CCPA) and internal compliance standards.

III. Security Policies

For each policy, include-

- **Purpose-** State the purpose of this security feature to your system
- **Policy Description-** Define the requirement of the policy indicated
- **Roles-** Define the users/person involved to this policy

IV. Policy-Specific Evaluation and Implementation Guidelines

For each policy, include-

- **Implementation Steps-** Clear steps for policy implementation.
- **Evaluation Checklist-** A checklist to confirm compliance.

V. Incident Response Procedures and Adaptability

- **Incident Detection** - Describe how incidents are detected (e.g., alerts, anomaly detection).
- **Incident Response Steps -** Define step-by-step procedures for responding to different types of incidents.
- **Post-Incident Review** - Outline procedures for reviewing incidents to improve policy and response.
- **Adaptability -** Ensure the policy is flexible to accommodate emerging threats and regulatory changes.

Rubrics and Criteria for Scoring

Summary Table for General Evaluation of Security Policies

Criterion	Description
Policy Definition	Clarity, purpose, and stakeholder understanding of the policy guidelines
Implementation Consistency	Consistent application across system components, with enforcement of role-based access or restrictions
Monitoring and Maintenance	Continuous monitoring and regular maintenance to ensure policy remains effective
Incident Response and Adaptability	Defined incident response, adaptability to new threats, and maintenance of logs for post-incident analysis