LAB 4
Assessment Worksheet
Policy Statement Definitions

Course:	**POLICY DEVELOPMENT IN INFORMATION ASSURANCE (IAP301)**
Semester:	**SP24**
Class:	**IA1702**
Name:	**Trần Minh Triết**
(roll numbers):	**SE172241**

Overview

Create a policy statement that defines how these policies mitigate the risk, threat, or vulnerability as indicated in the gap analysis matrix below for each of the gaps identified and recommended policy definitions.

Risk, Threat, or Vulnerability	IT Security Policy Definition
Unauthorized access from public Internet	Access Control Policy, Internet Ingress/Egress Traffic & Web Content Filter Policy
User destroys data in application and deletes all files	Data Classification Standard & Encryption Policy, Asset Protection Policy
Hacker penetrates your IT infrastructure and gains access to your internal network	Access Control Policy, Intrusion Detection & Prevention System (IDS/IPS) Policy, Security Awareness Training Policy
Intra-office employee romance gone bad	Asset Protection Policy, Human Resources Policy
Fire destroys primary data center	Business Continuity & Disaster Recovery Policy, Data Backup Policy
Communication circuit outages	WAN Service Availability Policy
Workstation OS has a known software vulnerability	Patch Management Policy, Asset Protection Policy
Unauthorized access to organization owned workstations	Access Control Policy, Asset Protection Policy
Loss of production data	Data Classification Standard & Encryption Policy, Production Data Back-up Policy
Denial of service attack on organization e-mail server	Internet Ingress/Egress Availability (DoS/DDoS) Policy, Security Awareness Training Policy

Remote communications from home office	Remote Access VPN Policy
LAN server OS has a known software vulnerability	Patch Management Policy, Asset Protection Policy
User downloads an unknown e-mail attachment	Internet Ingress/Egress Traffic & Web Content Filter Policy, Security Awareness Training Policy
Workstation browser has software vulnerability	Patch Management Policy, Asset Protection Policy
Service provider has a major network outage	WAN Service Availability Policy
Weak ingress/egress traffic filtering degrades performance	Internet Ingress/Egress Traffic & Web Content Filter Policy
User inserts CDs and USB hard drives with personal photos, music, and videos on organization owned computers	Asset Protection Policy
VPN tunneling between remote computer and ingress/egress router	Access Control Policy, Security Awareness Training Policy
WLAN access points are needed for LAN connectivity within a warehouse	Wireless LAN Access Control & Authentication Policy
Need to prevent rogue users from unauthorized WLAN access	Wireless LAN Access Control & Authentication Policy, Security Awareness Training Policy

For each identified gap, insert a recommendation for an IT security policy to help mitigate the risk, threat or vulnerability:
Define a policy statement (2 or 3 sentences max) for each of the following policy definitions that are needed to remediate the identified gap analysis for the IT security policy framework:

1. Access Control Policy Definition

The guidelines and processes for approving and denying access to resources controlled by the organization are outlined in this policy. It assists in reducing the possibility of illegal access to systems and sensitive data.

2. Business Continuity – Business Impact Analysis (BIA) Policy Definition

The procedure for locating, evaluating, and reducing risks to the organization's capacity to carry out its business is outlined in this policy. It lessens the possibility that a cyberattack, natural disaster, or other occurrence may disrupt company.

3. Business Continuity & Disaster Recovery Policy Definition

The steps for getting back up after a business disruption are outlined in this policy. It contains instructions for backing up systems, apps, and data. It assists in reducing the chance of downtime and data loss.

4. Data Classification Standard & Encryption Policy Definition

The guidelines for sensitivity-based data classification are outlined in this policy. It also outlines the steps involved in encrypting private information. It lessens the possibility of data leaks.

5. Internet Ingress/Egress Traffic & Web Content Filter Policy Definition

The guidelines for filtering data entering and departing the company network are outlined in this policy. It also outlines the steps involved in preventing access to particular websites and types of material. It assists in reducing the possibility of malware infestations and other security risks.

6. Production Data Back-up Policy Definition

The methods for backing up production data are outlined in this policy. In the event of a disaster, it helps to ensure that data is not lost.

7. Remote Access VPN Policy Definition

This policy lays out the guidelines and processes for giving and rescinding VPN access to the company's network. It assists in reducing the possibility of distant users gaining unwanted access to the network.

8. WAN Service Availability Policy Definition

The processes for guaranteeing the organization's WAN services are outlined in this policy. It contains instructions for keeping an eye on the WAN and handling outages. It lessens the possibility of interruptions in service.

9. Internet Ingress/Egress Availability (DoS/DDoS) Policy Definition

The methods for reducing the danger of distributed denial-of-service (DDoS) and denial-of-service (DoS) attacks are outlined in this policy. It contains instructions for both blocking and filtering attack traffic.

10. Wireless LAN Access Control & Authentication Policy Definition

This policy defines the rules for granting and revoking access to the organization's wireless LAN. It helps to mitigate the risk of unauthorized access to the wireless network.

11. Internet & E-Mail Acceptable Use Policy Definition

This policy defines the rules for using the internet and e-mail. It includes restrictions on the types of content that can be accessed or sent. It helps to mitigate the risk of malware infections and other security threats.

12. Asset Protection Policy Definition

This policy defines the rules for protecting the organization's assets, including hardware, software, and data. It includes steps for securing assets and preventing theft or loss.

13. Audit & Monitoring Policy Definition

The processes for auditing and keeping an eye on the company's IT systems are outlined in this policy. It outlines procedures for gathering and examining data in order to find security holes. It lessens the possibility of security lapses.

14. Computer Security Incident Response Team (CSIRT) Policy Definition

The processes for handling computer security issues are outlined in this policy. It contains procedures for locating, containing, and fixing problems. It assists in lessening the effects of security lapses.

15. Security Awareness Training Policy Definition

The processes for educating staff members on security awareness are outlined in this policy. It contributes to increasing knowledge about security threats and countermeasures.

Craft an IT Security Policy Definition

Overview

In this lab, you are to create an organization-wide policy defining from the list provided in Lab #10 – Part A. Here is your scenario:

- Regional ABC Credit union/bank with multiple branches and locations throughout the region
- Online banking and use of the Internet is a strength of your bank given limited human resources
- The customer service department is the most critical business function/operation for the organization
- The organization wants to be in compliance with GLBA and IT security best practices regarding employees
- The organization wants to monitor and control use of the Internet by implementing content filtering
- The organization wants to eliminate personal use of organization owned IT assets and systems
- The organization wants to monitor and control use of the e-mail system by implementing e-mail security controls
- The organization wants to fill the gaps identified in the IT security policy framework definition
- Select one of the identified policy definitions from the gap analysis and define an entire IT security policy definition for this needed policy definition

Instructions

Using Microsoft Word, create an IT security policy definition of your choice to mitigate the risks, threats, and vulnerabilities identified in the gap analysis. Use the following policy template:

ABC Credit Union

Policy Statement

The Information Security Policy of ABC Credit Union aims to safeguard the confidentiality, integrity, and availability of the organization's information assets by establishing guidelines and procedures for the secure handling of sensitive information, data access controls, and incident response protocols. This policy applies to all employees, contractors, and third-party vendors who have access to ABC Credit Union's information systems and data.

Purpose/Objectives

The purpose of this policy is to establish a comprehensive framework for managing information security risks within ABC Credit Union. The objectives of this policy include:

- Ensuring the confidentiality of sensitive information such as customer data and financial records.
- Protecting the integrity of information assets to prevent unauthorized modification or tampering.
- Maintaining the availability of critical systems and services to support business operations.
- Complying with relevant regulatory requirements and industry best practices in information security.

This policy definition fills the identified gap in the overall IT security policy framework by providing specific guidelines and procedures for addressing information security risks within ABC Credit Union. It mitigates risks, threats, and vulnerabilities by establishing clear responsibilities, controls, and response mechanisms to protect against unauthorized access, data breaches, and other security incidents.policy definition fills the identified gap in the overall IT security policy framework definition and how it mitigates the risks, threats, and vulnerabilities identified.}

Scope

This policy applies to all systems, networks, and data assets owned or operated by ABC Credit Union, including:

- Workstations and laptops used by employees for business purposes.
- Servers hosting critical applications and databases.
- Network infrastructure components such as routers, switches, and firewalls.
- Mobile devices issued by the organization or used to access company resources.
- Cloud-based services and third-party applications used to store or process sensitive information.

The Seven Domains of a typical IT infrastructure impacted by this policy include:

- User Domain: Employees and authorized users accessing information systems.
- Workstation Domain: Desktops, laptops, and mobile devices used for business operations.
- LAN Domain: Local area network infrastructure connecting devices within the organization.
- WAN Domain: Wide area network infrastructure connecting multiple locations or remote offices.
- Security Domain: Security measures and controls implemented to protect information assets.
- Internet Domain: Internet connectivity and access controls for external network communications.
- Remote Access Domain: Secure remote access solutions for employees working from off-site locations.

Standards

This policy references industry-standard frameworks such as ISO 27001 and NIST SP 800-53 for establishing information security controls. Additionally, it aligns with internal standards and guidelines defined by ABC Credit Union's Information Security Management System (ISMS). Specific hardware, software, and configuration standards include:

- Encryption standards for protecting data in transit and at rest.
- Password complexity requirements for user accounts and privileged access.
- Network segmentation and access control lists (ACLs) to restrict unauthorized access.
- Patch management procedures for ensuring timely updates and vulnerability remediation.

Incident response procedures for detecting, reporting, and mitigating security incidents.

Procedures

Implementation of this policy organization-wide will involve the following steps:

1. Conducting a comprehensive risk assessment to identify potential threats and vulnerabilities.
2. Developing security controls and safeguards based on the risk assessment findings.
3. Communicating the policy to all employees and providing training on information security best practices.
4. Implementing technical controls such as firewalls, intrusion detection systems, and encryption mechanisms.
5. Monitoring and auditing compliance with the policy through regular security assessments and reviews.
6. Establishing incident response procedures to address security breaches and incidents promptly.

Guidelines

Potential roadblocks or implementation issues that may arise include resistance from employees to adopt new security measures, lack of resources for implementing technical controls, and difficulty in integrating security solutions with existing systems. To overcome these challenges, ABC Credit Union will:

- Provide ongoing training and awareness programs to educate employees about the importance of information security.
- Allocate sufficient resources and budget for implementing necessary security controls and technologies.
- Collaborate with IT vendors and industry partners to leverage expertise and resources for addressing specific security requirements.
- Continuously monitor and evaluate the effectiveness of security measures, making adjustments as needed to improve overall protection.