LAB 1
Draft an Organization-Wide Security Management Policy for Acceptable Use

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

Overview

In this lab, you are to create an organization-wide acceptable use policy (AUP) that follows a recent compliance law for a mock organization. Here is your scenario:

- Regional FPT 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 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 eliminate use of social media (i.e. Facebook, Twitter,…) and non-business related instant messaging (i.e. Zalo, Facebook Messenger,…)
- The organization wants to monitor and control use of the e-mail system by implementing e-mail security controls
- The organization wants to implement this policy for all the IT assets it owns and to incorporate this policy review into an annual security awareness training

Instructions

Create an Acceptable Use Policy for FPT Credit union/bank according to the following template.

FPT Credit union/bank

Secure Banking Operations Policy

Policy Statement

The goal of the Security Team's publication of an Acceptable Use Policy is not to impose limitations that go against the transparent, trustworthy, and honest culture that FPT Credit Bank has always fostered. FPT Credit Bank is dedicated to shielding its partners, staff, and business from harmful or unlawful acts taken by anybody, whether they do so intentionally or not.

FPT Credit Bank owns the network model systems, which include but are not limited to computer hardware, mobile devices, software, operating systems, databases, and network accounts that enable email, Web surfing, and FTP. During regular business operations, these systems are to be used for business reasons in order to serve the interests of our clients and customers as well as the company. For further information, please see the Human Resources policy.

Working together, all FPT Credit Bank employees and affiliates who handle information and/or information systems must provide effective security. Every computer user has an obligation to be aware of these rules and to behave in accordance with them.

Purpose/Objectives

This policy's objective is to specify how computers and other electronic devices may be used at FPT Credit Bank. These guidelines are in place to safeguard both FPT Credit Bank and the employee. When used inappropriately, FPT Credit Bank opens itself up to ransomware and other virus assaults, network system and service compromise, data breaches, and legal problems.

Scope

This policy covers the use of data, electronic and computing equipment, network resources, and human resources—whether they are owned or leased by FPT Credit Bank, the employee, or a third party—for FPT Credit Bank business security or to interface with internal networks and business systems. It is the duty of all FPT Credit Bank and its subsidiaries' employees, contractors, consultants, temporary workers, and other workers to use reasonable judgment when it comes to the appropriate use of information, electronic devices, and network resources in compliance with local laws and regulations as well as FPT Credit Bank policies and standards.

This policy is applicable to all FPT Credit Bank employees, consultants, contractors, temporary workers, and other staff members, including those connected to other organizations. This insurance covers all equipment that the party owns or leases.

Standards

1. Data Classification Policy: This policy establishes the appropriate classification of data according to its significance and level of sensitivity. It enables users to comprehend the significance of managing data in accordance with its classification level within the framework of an AUP. This policy may be cited by the AUP to highlight the importance of handling various forms of data in an accountable and secure manner.

2. Data Protection Standard: To protect sensitive data, the Data Protection Standard specifies particular safeguards and procedures. To guarantee that users are aware of the security measures and procedures they must adhere to in order to protect sensitive information throughout its use, the AUP may include references to the Data Protection Standard.

3. Social Media Policy: This sets forth guidelines for how staff members or users may interact on social media sites while representing the company. If social media interactions are an integral element of the organization's operations, the AUP may make reference to the Social Media Policy to establish standards for the proper and responsible use of social media within the network of the organization.

4. Minimum Access Policy: This policy outlines the minimal amount of access required for users to carry out their duties. To emphasize the idea of giving users only the access required for their responsibilities and reducing the danger of unauthorized access and potential misuse, the AUP may make explicit references to the Minimum Access Policy.

5. Password Policy: This document lays down the rules for making and keeping passwords. The Password Policy would probably be included in the AUP to emphasize how crucial it is to keep strong passwords as a cornerstone of responsible system use. It might also include information on how users should manage and safeguard their credentials.

Procedures

1. **General Use and Ownership:**
    - FPT Credit Bank proprietary information stored on electronic and computing devices whether owned or leased by FPT Credit Bank, the employee or a third party, remains the sole property of FPT Credit Bank. You must ensure through legal or technical means that proprietary information is protected in accordance with the Data Protection Standard.
    - You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of FPT Credit Bank proprietary information.
    - You may access, use or share FPT Credit Bank proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
- For security and network maintenance purposes, authorized individuals within FPT Credit Bank may monitor equipment, systems, and network traffic at any time, per Infosec's Audit Policy. FPT Credit Bank reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

2. **Security and Proprietary Information:**
   - Every mobile and computer device connecting to the internal network needs to follow the guidelines set forth by the Minimum Access Policy.
   - Passwords at the system and user levels must adhere to the password policy. It is forbidden to purposefully grant access to another person or to do so by failing to secure such access.
   - Every computer device needs to have a password-protected lock screen and an automatic activation option that lasts no more than ten minutes. When you leave the device alone, you have to either lock the screen or log off.
   - Employees using an FPT Credit Bank email address should post to newsgroups or other online forums with a disclaimer saying that the views they express are solely their own and may not represent FPT Credit, unless doing so is part of their job obligations.
   - Workers should be very cautious when opening email attachments from senders they are not familiar with since they can contain viruses.
3. **System and Network Activities:**

   - Violating any person's or business's rights under copyright, trade secret, patent, or other intellectual property laws, as well as comparable regulations. This includes, but is not limited to, installing or disseminating "pirated" software or other products that are not legally authorized for use by FPT Credit Bank.

   - It is strictly forbidden to install any copyrighted software for which FPT Credit Bank or the end user does not have an active license, as well as to digitize and distribute photographs from magazines, books, or other copyrighted sources.

   - It is also forbidden to access data, a server, or an account for any reason other than carrying out FPT Credit Bank business, even if you have permission to do so.

   - It is prohibited to export software, technical data, encryption software, or technology in contravention of national or international export control regulations. Any substance that is in doubt should not be exported without first consulting the relevant management.

   - The introduction of harmful software, such as trojan horses, worms, ransomware, and viruses, into the server or network.

- Giving out your passphrase or account password to third parties or permitting unauthorized users to use your account. When working from home, family members and other household members are included in this.

- Causing network communication failures or security vulnerabilities. Unless these tasks are within the scope of routine duties, security breaches include, but are not limited to, accessing data that the employee is not supposed to receive or entering into a server or account that the employee is not specifically permitted to access. In this section, "disruption" refers to a variety of activities, such as brute-forcing accounts, packet spoofing, ping floods, network sniffing, denial of service, and maliciously generated routing information.

- Port scanning and security scanning are strictly forbidden unless the Infosec Team is notified beforehand.

- Carrying out network monitoring in any way that could intercept data not meant for the employee's host, unless the employee is required to do this for work.

- Getting beyond any host, network, or account's security or user authentication.

- Installing honeynets, honeypots, or other comparable technology on the network of FPT Credit Bank.

- Installing honeynets, honeypots, or other comparable technology on the network of FPT Credit Bank.

- Interfering with or preventing any user from using the system other than the host of the employee (denial of service attacks, for instance).

- Sending any form of message or using any program, script, or command with the intention of interfering with or disabling a user's terminal session locally.

4. **Email and Communication Activities**
   - Unsolicited email correspondence, such as "junk mail" or other promotional materials sent to recipients who haven't asked for them (email spam).
   - Any kind of harassment, including texting, calling, emailing, or paging, regardless of the message's size, content, or frequency.
   - The forgery or unauthorized use of email header data.
   - Email addresses other than the poster's account being requested, either with the intention of harassing the recipient or gathering responses.
   - Developing or disseminating "Ponzi," "chain letter," or other "pyramid" scams.
   - Use of unsolicited email coming from other Internet/intranet/extranet service providers' networks within FPT Credit Bank on behalf of or in promotion of any service offered by FPT Credit Bank or linked through its network.
   - Sending out identical or almost identical non-business-related messages to a lot of Usenet newsgroups (newsgroup spam).

Guidelines

1/ Resistance to Change:

Problem: If new policies affect how employees access and manage information, they may be resistant to changes in their everyday routines.

Method: Explain the rationale for the policy adjustments in detail, stressing the significance of security and compliance for the banking industry. Organize training sessions to answer any questions staff members may have and assist them in understanding the new policies.

2/ Technological Compatibility:

Problem: New security standards and procedures may be difficult to integrate with legacy systems or antiquated technologies.

Method: Make an investment in modernizing or swapping out outdated systems to make sure they adhere to security regulations. Implement strategies that close the gap between current and legacy technology, and phase out outmoded systems little by bit.

3/ User Awareness and Training:

Problem: Staff members don't know enough about the value of security measures and their part in keeping them in place.

Method: Hold frequent training sessions to inform staff members about security best practices, possible hazards, and the particular regulations mentioned in the policies. Employ real-world instances that are pertinent to the banking industry to highlight how important compliance is.

4/ Maintaining Productivity and Security:

Problem: It might be difficult to strike a compromise between putting strict security measures in place and continuing to run financial operations effectively.

Method: Make sure you identify crucial locations that need more security by doing a thorough risk assessment. Automate regular security activities, implement multi-layered security solutions, and make sure that productivity is not unnecessarily hampered by security measures.

5/ Regulatory Compliance:

Problem: There are many regulations that apply to the banking industry, and it can be difficult to ensure that you are in compliance with them all.

Method: Assemble a specialized compliance group to monitor and adjust policies in response to regulatory modifications. Engage legal professionals to interpret and modify rules in response to changing regulatory environments, and conduct routine process audits to guarantee continued compliance.

6/ Data Privacy Issues:

Problem: It's difficult to strike a compromise between safeguarding private client information and keeping it available for legal banking needs.

Method: To protect consumer data, put in place strong encryption techniques, access limitations, and frequent security assessments. Employee education regarding the value of privacy in the banking industry should be done, and policies should clearly describe data protection methods.

***Note**: Your policy document should not be more than 3 pages long.*