20BDS0146

VENNELA G

CSE3502- Information Security Management

Lab Slot L37+L38

Lab assignment 2

EX. 2 Designing Security Policy

Instruction 1

Assume that you are the CEO of XXX organization with 2000 employees with different priority and access rights. Considering these factors, design a security policy template to secure your organization from unwanted security threats.

- **Internet Security Policy**
- **Access Control Security Policy**
- **Antivirus Security Policy**

• Internet Security Policy

1. Overview

Resources are misused when staff members access the Internet in a way that is not consistent with business requirements. Due to the amount of time spent utilising or "surfing" the Internet, these activities may have a negative impact on productivity. In addition, other forms of misuse could result in reputational damage for the business and perhaps legal action. Until it is verified by another trustworthy source, all information gleaned from the Internet should be taken with a grain of salt. Most of the content on the Internet is out-of-date or false because there is no quality control procedure in place. Users will only be given access to the Internet as needed to carry out their employment and professional tasks and only to assist company activities.

2. Purpose

The purpose of this policy is to define the appropriate security of the Internet by <Company Name>employees and affiliates.

3. Scope

All Internet users (those employed by the company, including full- and part-time permanent employees, contract workers, temporary agency workers, business partners, and vendors) who access the Internet through computing or networking resources are subject to the Internet security Policy.

4. Policy

The following guidelines must be followed to the letter by all internet users:

- Users are not permitted to access or utilise the internet for their own commercial or professional advantage.
- Users are required to access and utilise the internet only for legitimate medical or professional purposes.
- Users must not visit pornographic or otherwise objectionable websites (including, but not limited to, sexist, racist, discriminatory, hate, or other sites that would offend a reasonable person in the same or similar circumstances).
- The user should get permission from the security officer if they have any doubts about whether access to a particular site is appropriate.

5. Policy Compliance

The infosec team will use a variety of techniques, including but not limited to business tool reports, internal and external audits, and reporting to the policy owner, to ensure that this policy is being followed. The Infosec Team must beforehand approve any exception to the policy. If this policy is broken, there may be disciplinary action taken against the employee, up to and including termination.

• Access Control Security Policy

1. Overview

The purpose of this policy is to establish our organization's responsibilities regarding corporate acquisitions and mergers. This policy also defines the minimum-security requirements involved in the Information Security acquisition assessment.

2. Purpose

The purpose of this policy is to define the appropriate accessibility of the <Company Name>employees and affiliates.

3. Scope

This policy applies to all companies acquired by and pertains to all systems, networks, laboratories, test equipment, hardware, software and firmware, owned and/or operated by the acquired company.

4. Policy

- Users are not permitted to access the internet using another user's ID, password, or other form of identity.
- Internet users seeking to connect to the computer network of this workplace before being allowed access to a firewall's internal network, users must authenticate themselves there.
- Without the Security Officer's prior consent, users may not set up modem, internet, or other external network connections that would allow unauthorised users to access this practice's system or information.
- Users are not permitted to create new internet connections or use existing ones to launch new communication channels without the Security Officer's prior consent.

5. Policy Compliance

The Information Security Team (InfoSec Team) will assess whether this policy is being followed by using a variety of techniques, including but not limited to reports from business tools, engagement with the policy owner, internal reviews, and external audits. The Infosec team must beforehand approve any exception to the policy. Any worker, volunteer, or contractor found to have disobeyed this rule discipline, including termination, as a last resort.

• Antivirus Security Policy

1. Overview

The purpose of this policy is to establish our organization’s responsibilities regarding corporate acquisitions and mergers. This policy also defines the minimum-security requirements involved in the anti-virus security policy.

2. Purpose

The purpose of an antivirus security policy is to protect an organization's computer systems and networks from viruses, malware, and other security threats that can compromise the confidentiality, integrity, and availability of data.

3. Scope

Every device that connects to the organization's network, including servers, workstations, laptops, and mobile devices, must meet the specifications for installing and configuring antivirus software. The protocol for upgrading antivirus software, including the frequency and mode of updates, should be outlined in the policy.

The policy should specify the steps to be followed when a virus is discovered as well as the procedures for finding and eliminating viruses.

4. Policy

- Use the supported anti-virus software that is accessible on the corporate download site. It should always be running. Download the most recent version, execute it, and apply any applicable antivirus software updates because nearly every day, new viruses are found.
- Discard spam, chain emails, and other unwanted communications without forwarded messages, in accordance with anti-virus security Policy and avoid downloading anything from shady or unsure sources and never open any files or macros that are attached to emails from unidentified, dubious, or dubious sources. Immediately remove these attachments, then "double delete" them by removing them from your Trash.
- Unless there is a strong business necessity, avoid direct disc sharing with read/write access.
- Run the anti-virus utility to verify a clean computer, turn off the software, and then run the lab test if the anti-virus software and the test conflict and activate the antivirus programme after the lab test.
- Avoid using any programmes that could spread a virus when the anti-virus software is deactivated, such as email or file-sharing.

5. Policy Compliance

An all-encompassing strategy that includes employee training, frequent updates, monitoring and reporting, enforcement, and ongoing audits and reviews is needed to ensure compliance with an antiviral security policy. These steps can help an organisation considerably lower the risk of virus infections while safeguarding important systems and data from destruction or illegal access.

Instruction 2

Design a security policy [any policy] for VTOP users (Administrators | Faculties | Students) at Vellore Institute of Technology, Vellore, by defining its network flow as well as the data flow.

1. Overview

A security policy for VTOP users should include measures to protect the confidentiality, integrity, and availability of the institution's network and data.

2. Purpose

The purpose of a comprehensive security policy for VTOP should aim to protect the website, network, and data from potential security threats, while also ensuring compliance with relevant regulations and standards.

3. Scope

This policy applies to all systems, networks, laboratories, test equipment, hardware, software and firmware, owned and/or operated by Vellore Institute of Technology.

4. Policy

Network Flow: The institution's website's network flow should be specified in the security policy, along with the systems and devices that are permitted to connect to the network and any traffic limitations. To stop illegal access and lessen potential risks, this may involve the deployment of firewalls, intrusion prevention systems, and other network security controls.

Data Flow: The security policy should specify the types of data that are stored, transmitted, and received as well as how they are secured for the institution's website. To guard against unauthorised access, data breaches, and other security concerns, this may involve the use of encryption, access controls, and other data security measures.

Password Guidelines: A robust password policy that specifies the guidelines for generating and maintaining passwords for all users should be part of the security policy. This might involve specifications for the length, expiration, and frequency of password updates.

User Access Control: To prevent unauthorised access to the institution's website, the security policy should specify the user access control procedures. The usage of multi-

factor authentication for privileged access, access control policies based on job positions and responsibilities, and regular user access reviews are a few examples.

Incident Response: Security incident and data breach response protocols, such as incident detection and reporting, containment and analysis, recovery and remediation, should be outlined in the security policy.

Regular Audits: Regular security audits and evaluations of the institution's website, network, and data flow should be part of the security policy in order to spot any potential vulnerabilities and make sure the policy is being followed.

5. Policy Compliance

The company should set up measures to keep an eye on network activity and spot any security risks. Security problems or illegal network activity should be reported right away to the proper personnel. In accordance with user roles and responsibilities, the policy should include access control mechanisms such blocking access to network resources. Only authorised workers should be able to access vital network resources. To find potential network flow vulnerabilities and mitigate them, the company should conduct regular vulnerability scanning and testing.