HOCHSCHULE
CAMPUS WIEN
UNIVERSITY OF
APPLIED SCIENCES

Case Study 4

Author:

Philip Magnus

Student identification number:

c2410537022

Date:

January 20, 2026

Contents

1 Overview

1.1 Case Study Tasks

1. Design an awareness program (media, approach, topics, ...) for your (virtual) company (6 p)
2. Design guidelines for user passwords in your organization. (4 p)
3. Design an Internet and eMail use policy for your organization. (4 p)
4. Design a BYOD (Bring you own device) policy for your organization. (4 p)

1.2 Summary

This case study focuses on human-related security aspects and compliance measures within the organization. It addresses four main objectives. First, it designs a comprehensive security awareness program for the company. Second, it defines clear and enforceable password guidelines for users. Third, it establishes an Internet and email use policy to reduce legal and security risks. Finally, it defines a Bring Your Own Device (BYOD) policy that balances flexibility for employees with the protection of corporate data.

Case Study 4 uses the fictional company from Case Studies 1, 2, and 3 as an example. The organization is PointPoint GmbH, a Software-as-a-Service (SaaS) provider headquartered in Vienna with approximately 250 employees.

2 Security Awareness Program

2.1 Design an awareness program (media, approach, topics, . . .) for your (virtual) company

Human behavior represents one of the most significant risk factors in information security. Even well-designed technical controls can be undermined by phishing attacks, social engineering, or careless handling of sensitive information. For this reason, PointPoint GmbH implements a structured and continuous security awareness program that targets all employees, regardless of their role or technical background.

2.1.1 Objectives

The primary objective of the security awareness program is to reduce the likelihood and impact of phishing and social engineering attacks by increasing employees' ability to recognize and report suspicious activities. In addition, the program aims to strengthen the overall security culture of the organization by making information security a shared responsibility rather than a purely technical issue. Finally, the awareness program supports compliance with regulatory and contractual requirements, such as ISO 27001 and GDPR, which explicitly require employee training and awareness measures.

Summary:

- Reduction of Phisihing and Social Engineering Attacks
- Strengthening the Security Culture
- Fulfillment of Regulatory and Compliance Requirements

2.1.2 Media and Formats

To ensure effectiveness and broad participation, the awareness program uses a combination of different media and formats. All employees are required to complete a mandatory annual e-learning course that covers fundamental security topics and is documented for compliance purposes. In addition, quarterly phishing simulations are conducted to test employees' awareness in realistic scenarios and to identify areas for improvement.

Supporting materials such as posters and articles published on the company intranet are used to provide continuous reminders of key security messages. To increase motivation and engagement, gamification elements such as badges, scores, or small rewards are integrated into the program. These elements encourage participation and help reduce resistance to mandatory training activities.

Summary:

- Mandatory annual e-learning Courses
- Quarterly Phishing Simulations

- Posters and Intranet Articles
- Gamification Elements (i.e. Basges, Scores)

2.1.3 Topics

The content of the awareness program focuses on threats that are particularly relevant to Point-Point GmbH. This includes phishing and social engineering techniques, secure password usage, and the safe handling of information while working remotely or on mobile devices. In addition, employees are trained on how to report security incidents and suspicious events, emphasizing that early reporting is encouraged and will not result in negative consequences for the employee.

Summary:

- Phishing and Social Engineering
- Password Security
- Mobile and Remote Working
- Security Incident Reporting Procedures

3 Password Guidelines

3.1 Design guidelines for user passwords in your organization.

Passwords remain a critical authentication mechanism in many systems and therefore require clear and enforceable rules. PointPoint GmbH defines organization-wide password guidelines to reduce the risk of unauthorized access caused by weak or reused credentials.

All user passwords must have a minimum length of twelve characters and include a combination of upper-case letters, lower-case letters, numbers, and special characters. Password reuse across systems is strictly prohibited in order to limit the impact of credential compromise. For all critical systems, such as cloud platforms, administrative interfaces, and remote access services, multi-factor authentication (MFA) is mandatory.

Employees are required to use an approved password manager to securely store and generate passwords. This reduces the need to memorize complex passwords and discourages insecure practices such as writing passwords down or reusing them. For critical systems, passwords must be changed at least every 90 days. For less critical systems, passwords are changed as needed, for example after suspected compromise or policy updates.

The password guidelines are defined in Table 3.1.

Rule	**Requirement**
Minimum Length	12 Characters
Complexity	Upper/Lower Case, Numbers, Special Characters
Reuse	Prohibited
Password Managers	Mandatory Use of Approved Password Managers
Change Frequency	Every 90 Days for Critical Systems; Otherwise, as Needed

Table 3.1: Role Based Access Control – PointPoint GmbH

4 Internet and Email Use Policy

4.1 Design an Internet and eMail use policy for your organization.

The widespread use of the Internet and email is essential for daily business operations at Point-Point GmbH, but it also introduces legal, reputational, and security risks. To address these risks, the company defines a clear Internet and email use policy.

Business-related use of Internet and email services is explicitly permitted and expected. Limited private use is also allowed, provided it does not interfere with work duties or violate company policies. This pragmatic approach acknowledges modern working habits while maintaining control over risks.

Certain activities are strictly prohibited. These include accessing or distributing illegal content, uploading sensitive company data to private cloud services, and disclosing internal or confidential information to unauthorized third parties. Such actions may result in disciplinary measures, as they pose significant security and compliance risks.

To enforce the policy and detect security incidents, security-relevant events related to Internet and email usage are logged. Monitoring is performed in a GDPR-compliant and proportionate manner, ensuring that employee privacy is respected while still allowing the organization to detect misuse or attacks such as malware distribution or phishing campaigns.

4.1.1 Permitted

- Business Related Usage
- Limited Private Usage

4.1.2 Prohibited

- Illegal Content
- Uploading Sensitive Data to Private Cloud Services
- Disclosure of Internal Company Information

4.1.3 Monitoring

- Logging of Security Relevant Events
- GDPR Compliant and Proportionate Monitoring

5 BYOD (Bring Your Own Device) Policy

To support flexible working models, including remote work, PointPoint GmbH allows employees to use their personal devices for business purposes under a defined BYOD policy. This policy ensures that corporate data remains protected even when accessed from privately owned devices.

5.1 Design a BYOD (Bring you own device) policy for your organization.

5.1.1 Requirements

All personal devices used for business purposes must be enrolled in the company's Mobile Device Management (MDM) system. This allows the IT department to enforce basic security controls, such as mandatory device encryption and secure configuration settings. In addition, devices must support remote wipe functionality so that company data can be removed if a device is lost, stolen, or compromised.

Summary:

- Mandatory Enrollment in Mobile Device Management (MDM)
- Device Encryption Enabled
- Remote Wipe Capability

5.1.2 Data Separation

To protect both corporate and private data, a logical separation between business and personal data is enforced on BYOD devices. This ensures that company data can be managed and removed independently without affecting the employee's private information. Devices that are rooted or jailbroken are not permitted, as such modifications bypass built-in security mechanisms and significantly increase risk.

Summary:

- Logical Separation of Private and Business Data
- Rooted or Jailbroken Devices are not Allowed

5.1.3 Liability

Under the BYOD policy, PointPoint GmbH is responsible for protecting corporate data stored or processed on personal devices. At the same time, the privacy and ownership of the employee's personal data are respected. The company does not access private data and only applies controls to the business-related environment on the device.

Summary:

- The Company Protects Corporate Data
- Private Data Remains the Property of the Employee