Security Management – Case Study 4

Student: Philip Magnus
Student ID: c2410537022
Date: 20.01.2026

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)

Case Study 4 uses the fictional company from Case Studies 1, 2, and 3 as an example: PointPoint GmbH, a SaaS provider headquartered in Vienna with approximately 250 employees.

1. Security Awareness Program

Objectives

- Reduction of phishing and social engineering attacks
- Strengthening the security culture
- Fulfillment of regulatory and compliance requirements

Media and Formats

- Mandatory annual e-learning courses
- Quarterly phishing simulations
- Posters and intranet articles
- Gamification elements (badges, scores)

Topics

- Phishing and social engineering
- Password security
- Mobile and remote working
- Security incident reporting procedures

2. Password Guidelines

Rule	Requirement
Minimum length	12 characters
Complexity	Upper/lower case, number, special character
Reuse	Prohibited
MFA	Mandatory for all critical systems

Rule	Requirement
Password managers	Mandatory use of approved password managers
Change frequency	Every 90 days for critical systems; otherwise, as needed

3. Internet and Email Use Policy

Permitted:

- Business-related usage
- Limited private usage

Prohibited:

- Illegal content
- Uploading sensitive data to private cloud services
- Disclosure of internal company information

Monitoring:

- Logging of security-relevant events
- GDPR-compliant and proportionate monitoring

4. BYOD (Bring Your Own Device) Policy

Requirements

- Mandatory enrollment in Mobile Device Management (MDM)
- Device encryption enabled
- Remote wipe capability

Data Separation

- Logical separation of private and business data
- Rooted or jailbroken devices are not allowed

Liability

- The company protects corporate data
- Private data remains the property of the employee