Case 1

Security Policies

Group 10

Participants

Athanasios Ntales (atnt3398)
Bilal Riaz (biri9477)
Chanchala Fernando (chfe1432)
Emad Abdulsamad (emab9908)
Lekhaz Adapa (lead3201)
Muhammad Usama Younas (muus4313)

Overarching Cyber Security Policy

Purpose: The goal of this policy is to create the principles and procedures that will govern the management of Eastchange's information systems and assets to prevent unauthorized access, use, disclosure, interruption, modification, or destruction. There is no prior approval required.

Scope: All employees, contractors, vendors, and partners who have access to Eastchange's information system and assets are subjected to this policy.

Statement of needs: Since neither Bitflip AB nor Eastchange AB has ever had a proper cyber security policy, it is essential to constitute some rules that have to be followed in order to ensure the enforcement of the CIA triad regarding data processing.

Policy: The policy focuses on specific key areas of cyber security, such as access control, authentication, encryption, incident management, vulnerability management, physical security, business continuity, and awareness training.

- Data protection impact assessments will be carried out to estimate the likelihood and impact of security failures, as well as the required security measures to be implemented.
- All identified or suspected data breaches or incidents must be reported in line with Eastchange's Data Breach Policy.
- All staff members of the company must complete the mandatory Information Governance training course. Associates(including temporary employees) may be required to complete the course if it is relevant to their work.
- Eastchange will keep an information asset register to keep track of the assets, systems, and applications utilized for processing or storing personal data across the organization.
- Eastchange must employ physical security controls, such as access control, monitoring, and surveillance, to protect the organization's physical assets, such as servers, routers, and switches, according to the policy.
- Additionally, Eastchange is required by policy to establish and maintain a business continuity strategy to guarantee that important company processes can continue in case of a cyber security attack or another disruptive event.
- Furthermore, the policy requires Eastchange to have an incident management procedure for detecting, responding to, and recovering from cyber security issues.
- Algorithms in use must meet the standards defined for use in NIST publication SP-800 or any superseding document, according to the date of implementation.

Technical Cyber Security Policy that relates to the technical aspects of the scenario is mentioned in ISO/IEX 27002

According to our understanding, the following is the most crucial factor for the technological execution of the cyber security policy in the above scenario presented in the case study:

- Cryptographic Control Policy [10.1]

Principles: Information security objectives can be achieved in a number of ways by using cryptographic controls, including:

- Encrypting data to protect sensitive or important information while it is being stored or sent is the process of maintaining confidentiality.
- checking the integrity or authenticity of important or sensitive data that has been saved or transmitted using message authentication codes or digital signature certificates.
- Cryptography provides assurance of the data source so that the data source can be verified. In addition, cryptography provides confirmation that the sent data is received correctly.
- Cryptography provides protection for credential information through the authentication process.

Scope and Targets: Cryptography can provide security for data and communication by applying cryptographic techniques:

- Strong cryptography techniques must be provided to secure data on the storage media.
- High-performance cryptography functions must apply to secure communication and data transmission in different networks such as internet remote access and wifi.
- Include strong and complex cryptographic techniques in access control mechanisms to protect authentication data.
- Use cryptographic techniques to validate the identity of data origin and confirm the data delivery.
- Use required cryptographic techniques to ensure the stored and transmitted data integrity.

Controls: Following controls East change should apply to achieve cryptography policy targets:

- Apply encryption in all employee's computers' storage media.
- Use encryption and Raid matrices in all the servers.
- Provide a secure channel for remote access using IPsec, VPN, and SSH.
- Allow only secure connection for internet access using TLS/SSL protocols.
- Apply public key encryption for internal email messaging.
- Use DNSSEC and digital certificate to validate all received emails.
- All-access authentications must be processed using TLS/SSL security protocols.
- Apply hashing on passwords stored in the user's database.
- Apply public key encryption on users' databases.

- Use digital signatures to validate all selling and buying requests, contracts, and financial transactions.
- Apply MD5 hashing in all stored and transmitted data to confirm the data integrity.