Huba Control

HUBA CONTROL AG
INFORMATION SECURITY
STATEMENT

1 Statement

Huba places great importance on information security (ISEC). Huba's cybersecurity strategy prioritizes detection, analysis, and response to known, anticipated or unexpected cyber threats, effective management of cyber risks, and resilience against cyber incidents. Huba continuously strives to meet the industry's information security best practices and applies controls to protect our clients and Huba.

2 Identify

2.1 Information Security Policies

Huba maintains a comprehensive set of information security policies to document Huba's approach to compliance with laws, rules, regulations, best practices, and company management directives.

Huba reviews and updates its information security policies on an annual basis. Employees must acknowledge these policies.

2.2 Asset Management

Huba maintains an asset management program to appropriately inventory, classify, and protect applications, data, and hardware.

2.3 Information Security Advisor

Huba has an appointed Information Security Advisor who is responsible for security compliance, and education.

2.4 Staff screening

Huba conducts background screening at the time of hire (depending on position and to the extent permitted or facilitated by applicable laws / countries). In addition, Huba's information security base guideline is part of the work contract.

3 Protect

3.1 Training & Awareness

Huba provides all employees with annual cybersecurity awareness training. The training is mandatory and teaches employees to understand security risks and threats, especially "Social Engineering" and "Phishing". This is to ensure that employees understand that criminals may try to deliberately attack, steal, damage, or misuse Huba systems and information.

Additional, targeted training is delivered periodically and in a timely manner to ensure personnel maintain awareness of evolving cyber threats and countermeasures.

3.2 Identity & Access

Huba has implemented controls to identify, authorize, authenticate, and manage individuals' access to Huba's systems and information assets.

Huba grants access on a need-to-know basis, reviews permissions, and revokes access immediately on termination.

3.3 Application / Software Security

Huba maintains a centralized inventory. Software Updates are regularly applied.

3.4 Network Security

Huba protects its infrastructure through a control framework which includes architecture reviews, vulnerability testing, system hardening, and malware protection.

The vulnerability management program includes frequent scans, identification, and remediation of security vulnerabilities on servers, workstations, network equipment, and applications.

3.5 Device Security

All mobile computers are equipped with hard disk encryption and up-to-date antivirus software.

3.6 Data Protection and Data Privacy

Huba has implemented controls designed to safeguard Huba and client information which covers data classification, secure storage, handling, transmission, and destruction.

3.7 Physical Security

Huba has implemented physical access controls on all company facilities including branch offices, and data centres. Rooms with network equipment are always locked and can only be accessed by designated employees. Furthermore, entrances and server rooms are under camera surveillance.

4 Detect

4.1 Continuous Monitoring

Huba maintains a security scanner to detect and remediate security issues to avoid risk exposure.

4.2 Enforcing Protective Measures

Huba tests and confirms protective security measures to verify the effectiveness and coverage.

5 Respond

5.1 Security Incident Management

Huba's security incident management program enables effective detection and management of security threats and incidents that have a potential impact on the confidentiality, integrity, or availability of Huba's information and technology environment, including notification to clients as required by applicable laws and regulations.

5.2 Response Planning

Huba incorporates coordinated response planning processes during and after any security incident, which include managing communications and analysing the effectiveness of response activities.

5.3 Logging

Application and infrastructure systems logs are stored for troubleshooting, security reviews, and analysis by authorized Huba personnel. Logs are preserved in accordance with regulatory requirements.

6 Recover

Huba has business continuity plans in place to counteract interruptions to information systems and business activities from the effects of major failures or disasters. This involves data being securely backed up and verified regularly.

Würenlos, November 2022

Huba Control AG
signed by Information Security Advisor