hvs consulting

Company Security Policy (CSP)

This template serves only as an example and does not contain the complete content.

Please contact us for comprehensive advice.

Owner	<name>
Approval	<name>
State	Draft | Review | Approved
Version	x.x
Valid from	<date>
Classification	-CLASSIFICATION-

Table of contents

Farblegende Mustervorlage:

Anzupassen an unternehmensspezifische Begrifflichkeiten

Anzupassen anhand der Unternehmensvorgaben (z.B. private Nutzung erlaubt/verboten)

1 General

1.1 Objective

The objective of this policy is to define binding requirements for the use of IT systems and the handling of business information of IS-Fox GmbH (CLIENT) and to reduce the risks of improper use.

1.2 Target group

The rules defined in this policy are binding for all employees of CLIENT.

This also includes external or temporary personnel (e.g., consultants, freelancer, employees of suppliers or service providers, temporary workers or working students) who perform tasks on behalf of CLIENT in the described field of activity.

1.3 Violations

Violations of, or disregard with the rules defined in this policy may be sanctioned. Details are described in the CLIENT Information Security Policy (ISP) (Chapter 1.4).

1.4 Deviations

Option 1 Exception process below:

Deviations from the rules of this guideline must be reported to the Chief Information Security Officer (CISO). The CISO must evaluate the deviation and - depending on the risk - either reject or approve it.

Depending on the risk of the deviation, approval can be granted on a blanket basis or subject to conditions, i.e. the deviation is only permitted if the defined risk-minimizing measures are implemented.

An exception can be approved both permanently and temporarily. The decision to reject or approve (including the duration of the approved exception) must be documented by the CISO and reviewed again after the deadline has expired.

Option 2 Reference to exception process:

Deviations from the rules defined in this policy must be handled in accordance with the ISMS exception handling process.

2 Roles and responsibilities

Roles and responsibilities under this policy are described in the ISP (Chapter 2).

3 General specifications

3.1 Reporting of information security incidents

An information security incident (InfoSec incident) is defined as a threat of the protection goals of confidentiality, availability, and/or integrity.

Every employee must report any InfoSec incidents detected or suspected immediately to the IT service desk:

- By ticket: [illegible]
- Per telephone: [illegible]

Examples of reportable InfoSec incidents can be found in Annex X.

3.2 Security awareness

Raising the awareness of all employees about all significant threats and ris ks is an essential component of a functioning ISMS.

- All employees must regularly (= at least annually) participate in the security awareness measures offered (especially security eLearning).
- The responsible head of department | the HR department | the direct supervisor must ensure that the security awareness measures offered, are taken up by all employees in their own area of responsibility and that the necessary time is available for participation.
- The HR department must regularly evaluate participation, monitor it, and intervene if necessary.

New employees must complete the security eLearning promptly (as part of the onboarding phase).

3.3 Changes in the employment relationship

In the event of personnel changes (internal transfer, termination of employment), the following must be taken into account:

- The responsible head of department must inform the HR department at an early stage (when the personnel change becomes known).
- The HR department must ensure that the offboarding of the employee is initiated and carried out properly / completely.
- As part of the offboarding process, the HR department (together with the head of department) must ensure that…
  - authorizations that are no longer required are removed or adjusted.
  - Accounts that are no longer required are deactivated or deleted.
  - IT equipment that is no longer required (including notebooks, smartphones, data carriers, authentication tokens, access cards and keys, etc.) is returned.
- Further information can be found in the Personnel Security Policy.

3.4 Procurement of IT systems

- All IT systems (hardware, software, applications, smartphones, printers, multifunction devices, ...) must be procured by IT.
- Further information can be found in the policy Secure procurement of IT systems.

This template serves only as an example and does not contain the complete content.

Please contact us for comprehensive advice.

5.10 Passwords

Each employee receives his or her own personalized user account to use the IT systems.

- Each employee is responsible for all actions performed with the account.
- Passwords may not be passed on - not even to superiors, IT staff, or other colleagues. Passwords may also not be passed on in the event of a deputy (vacation, absence). In such cases, the designated deputy functions must be used.
- Passwords must not be written down. Instead, password safes should be used. These can be provided by IT.
- Passwords must not be stored in automatic login procedures (e.g., macros, scripts, ...) or in the web browser.
- Users with multiple accounts must use a separate password for each account. Reuse of the same password between private and business accounts should also be avoided.
- In case of suspected or detected misuse of the user account, this must be reported as an InfoSec incident (see chapter 3.1).
- When entering the password, care must be taken to ensure that the entry is not observed.

The following is understood as a secure password (concerns user passwords) at CLIENT:

- **Length: 12** characters
- **Complexity: 3** out of **4** (i.e., passwords must contain characters from at least 3 of the following 4 character groups):
  - Capital letters: A B C D E F ...
  - Lowercase letters: a b c d e f ...
  - Numbers: 0 1 2 3 4 5 ...
  - Special characters: * ! & % $ § ... (as long as they are supported by the respective IT system).
- **History**: the last **5** passwords must not be reused.
- **Change interval**: every **180** days (password must be changed).
- Used passwords must contain.
  - no whole words (password, Weißwurst, Rosenheimerherbstfest, ...),
  - no combinations of letters / numbers with regularities (e.g. abc123, test1234, ...) and
  - should not contain "easy to guess parts" or personal information (e.g. date of birth, name of partner, name of children or pet, ...).
- Higher password requirements apply to accounts with elevated or administrative privileges (defined in the Secure IT Operations Policy).
- Mnemonic devices help to remember even secure and complex passwords. E.g.,
  - The password consists of the first letters of a sentence. In addition, certain characters are replaced by numbers or other characters:
  - **T**his **s**ummer **i**t **r**ained **four times** **i**n **w**inter **eight times** ==> Tsir4*iw8*
  - The password consists of one word by replacing letters and numbers and special characters: Weißwurst ==> **W3!55wur5t**

This template serves only as an example and does not contain the complete content.

Please contact us for comprehensive advice.

6 Physical security requirements

6.1 Site, buildings, and zones

The CLIENT subdivides property (parts), building (parts) or premises into the following security zones:

Security zone	Description
Public area	Areas and spaces that do not contain information or facilities that require protection. **Examples**: Parking and outdoor areas, entrance and waiting areas.
Employee area	Areas and spaces that contain non-public information and information-processing facilities with access to non-public information. **Examples**: Open plan offices, standard offices, meeting rooms, corridors within buildings.
Security area	Areas and rooms containing central information-processing facilities (e.g., server room, archive, etc.), providing access to particularly sensitive data, or containing collection facilities of records/items to be destroyed. **Examples**: HR office, archive, management offices, IT workstations, technical rooms, server rooms.
High security area	CLIENT data center. **Example**: Data center.

Security requirements for the public area

Access to public areas is generally provided or permitted for third parties during duty / service hours.

- Outside of service hours, access to CLIENT buildings must be protected against entry by unauthorized persons.
- Only information or information processing equipment intended for public use may be stored, operated, or provided in the public area.

Security requirements for the employee area

Only authorized employees are permitted access to the employee area. All other employees (employees without authorization) have access only to areas directly related to their work environment or area of responsibility.

- The person responsible for key / card management must keep a list of persons authorized for access.
- All non-authorized persons may only be in employee areas when accompanied by an authorized employee.
- If an authorized person leaves an employee area and no other authorized employee is present there, the employee area must be locked, or it must be ensured that no unauthorized persons gain access to this area.
- The presence of unknown persons in the employee area must be questioned in a friendly but consistent manner (reason for their stay, contact person at CLIENT). If there is no valid reason for the stay, the person must be asked to leave the staff area.

This template serves only as an example and does not contain the complete content.

Please contact us for comprehensive advice.

Ready to set up your ISMS?

Let's get started together!

Contact us now for individual advice and support.