Information security for service providers

Policy

Document control

Name:	ISMS06_HYEU_PL_Information security for service providers		
Version:	1.0		
Issue date:	10-14-2024		
Classification:	☒ Internal	☐ Confidential	☐ Secret
Status:	☐ Draft	☐ In coordination	☒Approved
Responsible:	Information Security Officer (ISO)		
Approved by:	Management		

Change history

Version	Date	Author	Comments
0.5	14.10.2024	B.Marold	Draft
1.0	14.10.2024	Management	Approved

List of abbreviations

Abbreviations	Description

Applicable documents

1 Table of Contents

1 Purpose 4
2 General Requirements 4
2.1 Organizational requirements 4
2.2 Personnel security 4
2.3 Physical and environmental security 5
2.4 Management of organizational assets 5
2.4.1 Classification rules 5
2.4.2 Labeling and handling of information 5
2.4.3 Handling of Data carries 7
2.5 Dealing with information security incidents 7
2.6 Compliance and adherence to legal obligations 8
2.6.1 Early risk detection 8
2.6.2 Intellectual property/license management 8
2.6.3 Data protection 8
2.7 Contractual compliance 8
2.8 Internal rules and regulations 8
2.9 Violations and enforcement 8
2.10 Appointment of Information Security Officer 8
2.11 Liability 8
2.12 Audits 9
3 Additional requirements for contractors with direct access to the internal HEYCO Group network 9
3.1 Definition 9
3.2 Requirements 9
3.2.1 Internal organization 9
3.2.2 Physical and environmental security 9
3.2.3 Protection against malware and mobile program code 9
3.2.4 Backup 9
3.2.5 Access control 10
3.2.6 Access control for networks 11

4 Additional requirements for contractors without direct access to the internal HEYCO Group network 11
4.1 Definition 11
4.2 Requirements 11
4.2.1 Internal organization 11
5 Responsibilities and deviations 11

1 Purpose

Information Security Policy for Service Providers

This document is intended for all service providers of the HEYCO Group. The information security requirements contained herein are binding. The policy is based on specific information security requirements imposed by OEMs on their suppliers. Where possible, references are provided to necessary documents or technical implementations within the framework of the set standards (ISO 27001, TISAX) to fulfill the individual requirements.

2 General Requirements

The following requirements must be complied with by all service providers and their subcontractors of the HEYCO Group.

2.1 Organizational requirements

Only approved devices, systems, and storage media may be used on the company premises.
Data and software may not be used on devices, systems, or storage media that are not provided and approved by the company or the service provider.
Data and software may only be used on approved file services and cloud services.
Information may only be passed on to third parties with written approval.
Compliance with the rules on personal data must be ensured.
The service provider must enforce the confidentiality obligation based on the existing NDA among its employees.
Data encryption on mobile devices must be ensured. Country-specific encryption regulations must be observed.
The transfer of data and its deletion by the service provider at the end of the contract must be carried out by the service provider. Legal retention obligations must be observed in this process.

2.2 Personnel security

The service provider manages user IDs and access rights. If these are no longer required, this must be reported immediately to the HR department and IT.
The service provider manages the identification media. If these are no longer required, they must be handed over to the HR department immediately.
The service provider manages the devices and media provided. If these are no longer required, they must be handed over to the IT department immediately.
In the event of loss of identification media or devices and media provided, the information security and IT departments must be notified immediately.

2.3 Physical and environmental security

Unauthorized viewing and access to IT devices (especially mobile devices) must be prevented. Confidential and secret documents must never be left unattended.

2.4 Management of organizational assets

2.4.1 Classification rules

The service provider must be familiar with the classification based on information security protection objectives and the classification of assets relevant to them.
The service provider must obtain this classification and the information security classification.
Information must be protected according to its confidentiality classification.
The information security department can carry out regular checks of the integrity and availability classification when processing data, if necessary.
The classification must always be verified by the information owner.

2.4.1.1 Confidentiality

Access to information may only be granted to authorized persons.
If the service provider creates new information, it must be labeled accordingly.
The service provider must request the classification for new information from information security.
Until classified, the information is by default "Confidential."
Information that is not explicitly marked has the level "Internal."
If there are doubts about the correct classification, the information security department must be informed.

Levels: Public, Internal, Confidential, Secret

2.4.1.2 Integrity

It must be ensured that information is protected against unauthorized changes.

Levels: Low, Medium, High, Very High

2.4.1.3 Availability

It must be ensured that information is available within a defined period of time.

Levels: Low, Medium, High, Very High

2.4.2 Labeling and handling of information

Information must be protected against unauthorized access. This applies throughout its entire life cycle with the appropriate confidentiality classification.

The HEYCO Group has specific guidelines for each level of confidentiality regarding labeling, duplication and distribution, storage, deletion, disposal, authentication, and transport. These guidelines also apply to IT systems.

Classification level Public:

- No restrictions
- Compliance with the requirements for positioning the label

Classification level Internal:

- Labeling: none or "Internal" (in the local language) on the first page, compliance with the requirements for positioning the label
- Reproduction and distribution: only authorized employees and third parties within the scope of their activities or area of application
- Storage: protection against unauthorized access
- Deletion: data no longer required
- Disposal: secure disposal, reliable overwriting, physical destruction

Classification level Confidential:

- Labeling: "Confidential" (in the local language) on each page, electronically or printed, observing the specifications for positioning the label
- Duplication and distribution: limited group of authorized employees and third parties within the scope of their activities or area of application, the distributor is responsible for suitable channels (if encryption is used)
- Storage: Access only for a limited group of authorized employees and third parties within the scope of their activities (closed user groups), use of suitable storage locations and media
- Storage: In locked steel cabinets or locked rooms, access only for authorized persons
- Deletion: data no longer required
- Disposal: secure disposal, reliable overwriting, physical destruction
- Authentication: strong, 2 out of 3 -> possession, knowledge, inherence
- Transport: sealed neutral envelopes ("personal" if necessary), delivery only directly to the recipient

Classification level strictly confidential:

- Labeling: "strictly confidential" (in the local language) on each page, electronically or printed, compliance with the specifications for positioning the label, page labeling with "page x of y"
- Reproduction and distribution: extremely limited group (e.g., list of names) of authorized employees and third parties within the scope of the activity or area of application, prior approval by owner, state-of-the-art encryption (if not possible, a comparable solution), additional organizational or technical measures depending on the application (prohibition of forwarding, prohibition of printing, watermarks) Prevention of eavesdropping (encrypted video conferences)

- Storage: Access only for a very limited group (e.g., list of names) of authorized employees and third parties within the scope of their activities or area of application, prior approval by the owner, state-of-the-art encryption (if not possible, a comparable solution), additional organizational or technical measures depending on the application
- Storage: In locked steel cabinets with separate locks
- Deletion: data no longer required
- Disposal: secure disposal, reliable overwriting, physical destruction
- Authentication: strong, 2 out of 3 -> possession, knowledge, property
- Transport: sealed neutral outer envelopes (no additions), a second inner envelope marked "Secret"

2.4.3 Handling of Data carries

- The service provider must protect data carriers containing HEYCO Group information from unauthorized access, loss, destruction, and mix-ups.
- Data carriers containing HEYCO Group information that are no longer needed or are defective must be disposed of securely in the following manner:
- Deletion by reliable overwriting
- Physical destruction in accordance with DIN 66399

2.4.3.1 Exchange of information

Eavesdropping on any audio communication (e.g., conversations, telephone calls, web meetings) containing confidential or secret information must be prevented.
Fax and email directories must be maintained. If there is any uncertainty, the recipient's current address or number must be requested.
A management system has been set up for the transport of end devices and data carriers outside the company premises.
When sending emails, the sender is responsible for the content and distribution. The recipient is then responsible for further processing and distribution.
Chain emails must not be sent.

2.5 Dealing with information security incidents

All information security incidents must be reported immediately to the HEYCO Group's information security department if their data or systems are affected.
Any suspected vulnerabilities and weaknesses in HEYCO Group IT systems must be reported immediately to the information security department. Independent investigation of the suspicion is not permitted.
Immediate notification to the information security department must be made if there is suspicion of loss of confidential or secret information.
At the request of the HEYCO Group, the service provider must provide a security report.

2.6 Compliance and adherence to legal obligations

A compliance management system (resources, control, continuity, protection) must be established for all information, hardware, and software.

2.6.1 Early risk detection

A process has been established for detecting and dealing with risks and threats to data and systems.

2.6.2 Intellectual property/license management

Compliance with intellectual property rights must be ensured.
No unlicensed software may be used.
In the case of licensed software, the legal provisions must be observed. The software may only be used in accordance with the license agreements for the agreed purpose.

2.6.3 Data protection

Compliance with country-specific data protection laws must be ensured. To this end, the service provider must be obligated by its management.

2.7 Contractual compliance

The service provider must establish a process based on the PDCA principle to prove that all contractual requirements have been met.

2.8 Internal rules and regulations

The service provider must have an employee management system in place that contains rules and guidelines for handling information and IT systems.

2.9 Violations and enforcement

Violations of information security must be investigated and punished. The relevant operational, contractual, and legal regulations and agreements apply.

2.10 Appointment of Information Security Officer

The service provider must notify the responsible department at HEYCO Group of its central contact person for information security.

2.11 Liability

Compliance with the requirements of this document must also be ensured for subcontractors of the service provider.

2.12 Audits

Audits must be carried out to verify compliance with information security at the supplier.
The audit may be carried out by an uninvolved, qualified third party.
The service provider has a duty to cooperate in audits.
The advance notice period for audits is at least 48 hours.
Audits of suppliers without TISAX certification may be carried out at any time.
Audits of suppliers with TISAX certification may only be carried out if an incident is suspected.

3 Additional requirements for contractors with direct access to the internal HEYCO Group network

3.1 Definition

The following requirements apply to service providers when using end devices and/or a connection to IT systems (remote access, VPN access, direct connection, partner connection). The requirements apply both inside and outside the company premises.

3.2 Requirements

3.2.1 Internal organization

HEYCO IT equipment and data may only be used with HEYCO's consent. This consent may be withdrawn at any time.
Hardware and software may not be installed without the approval of the IT department.
The manipulation of IT equipment (e.g., installation, removal, modification of security settings) may only be carried out by the IT department.
The use or modification of programs may not be carried out without the approval of the IT department.
No external data may be processed on IT equipment.
The service provider shall ensure that information, programs, and devices are only used for business purposes and within the scope of the assignment. No private software or data may be used on IT devices.

3.2.2 Physical and environmental security

The service provider shall ensure the proper handling of the HEYCO Group's IT devices and protect them against loss and modification.
The manufacturer's instructions must be observed.
IT devices may only be removed from the company premises with the approval of the information security department.

3.2.3 Protection against malware and mobile program code

IT devices and data carriers belonging to the HEYCO Group may not be used if malware is suspected.
The responsible department must be notified immediately.

3.2.4 Backup

Data storage should be carried out on assigned network drives wherever possible.

Any other backup storage (e.g., local) is the responsibility of the user.
Backup data and media are subject to the same rules as original data.

3.2.5 Access control

3.2.5.1 Business requirements for access control

The use of other people's user IDs or accounts is prohibited.
The disclosure of identification media is prohibited.
There is a duty of confidentiality and a prohibition on passing on personal user IDs (passwords, PINs).
There is a prohibition on storing or writing down passwords, except using verified methods (e.g., KeePass).
Passwords or PINs must be changed immediately if there is any suspicion that they have been compromised.
Temporary passwords must be changed upon initial login.
Passwords must be changed at least once per year.
Spying on passwords is prohibited.
Passwords must be classified as at least "confidential."
If it is necessary to store passwords in writing, the following rules apply:

- Password in sealed envelope in safe
- Appropriate updates are ensured
- Envelope signed for by employee
- List of names of persons authorized to open envelope is available
- Application of the "two-person rule"
- Documentation and report of each opening
- Immediate change of password after opening
- Use of alternative IT systems with corresponding functionality for the described rules is permitted

Users are required to lock the system when leaving a system during operation (multifunction cards must be taken with them).

3.2.5.2 Generation of passwords

The use of identical passwords from private life is prohibited.
The use of identical passwords from third-party systems is prohibited.
There is an obligation to comply with the minimum length of passwords.
Trivial passwords and passwords with personal references are prohibited.
There is an obligation to comply with the relevant requirements if complex passwords are required.

3.2.5.3 PINs for unlocking smartphones and tablets

The requirements are identical to those for passwords.

3.2.5.4 PINs for authentication smart cards

The requirements are identical to those for passwords.

3.2.5.5 Group IDs

- Group IDs are permitted under the following conditions:
- Assignment of the user ID by a responsible person, ensuring logging and archiving

- Written confirmation of receipt by the user, ensuring archiving
- Change of password after receipt of the user ID by the user
- Change of password after return of the user ID by responsible person
- Compliance with archiving periods

3.2.6 Access control for networks

3.2.6.1 Rules for the use of network services

IT devices belonging to the HEYCO Group may only be connected to internal networks or external networks (with the exception of mobile networks).
The connection must be terminated immediately when it is no longer needed.

3.2.6.2 Device identification in networks

Unrestricted connection to internal HEYCO Group networks is only permitted with HEYCO Group devices.

4 Additional requirements for contractors without direct access to the internal HEYCO Group network

4.1 Definition

The following requirements apply to service providers who do not use end devices and do not have a connection to IT systems (remote access, VPN access, direct connection, partner connection).
Data is exchanged with the HEYCO Group.

4.2 Requirements

4.2.1 Internal organization

- [Company] data must be separated from third-party data (rights management).
- Access by third parties must be prevented (encryption).
- The classification for information security must be adopted.
- The implementation of appropriate information security measures must be guaranteed.
- Access to data must be based on the principle of "need to know."

5 Responsibilities and deviations

All service providers must ensure compliance with the requirements in this document. Deviations are only permitted on a temporary basis and after consultation with the information security department at HEYCO Group.