

Information Security Standard
Information Security for Externals



Contents

1. Overview.....	3
1.1. Security principles	3
1.2. Organization policy.....	3
2. Introduction.....	3
2.1. Purpose.....	3
2.2. Scope	3
3. General information security management.....	4
3.1. Contractual requirements	4
3.2. Information Security Management System (ISMS)	4
3.3. Compliance with Information Security Standard	4
3.4. ISMS Awareness	5
3.5. Non-compliance	5
3.6. Handling exceptions	5
4. Data classification.....	5
4.1. Labeling	6
4.2. Handling information	7
5. Security control measures.....	8
5.1. Physical access control	8
5.2. Admission control.....	8
5.3. User access control.....	9
5.4. Separation control.....	9
5.5. Data media control.....	9
5.6. Transport control.....	9
5.7. System security.....	10
5.8. Availability control.....	10
5.9. Security Incidents	10
6. Document Control.....	11
7. Version History.....	11

1. Overview

DEKRA's security objective is to ensure that information in all forms – written, verbal, electronic or printed – is protected against accidental or intentional unauthorized modification, disposal or disclosure throughout its entire lifecycle. The security measures for the systems and programs used to process, transfer and store information must achieve adequate level of protection.

1.1. Security principles

- Our business processes and know-how are to be protected
- Our security measures will reduce the risks for the organization
- Our security measures are in alignment with the industry standards
- Each individual is responsible for the security of our information, facilities and systems in their field of expertise.
- We will be implementing a clear separation of responsibilities to avoid conflict of interest
- We will comply with all legal and regulatory requirements
- We will ensure that the security requirements adapt to changing business requirements

1.2. Organization policy

The information security standard may only be enforced in compliance with the co-determination rights of the national employee representatives, as well as the provisions of the applicable employment agreement and local laws (e.g. data protection law).

2. Introduction

2.1. Purpose

The purpose of this information security standard is to ensure business continuity and damage reduction while collaborating with externals (Suppliers, Service Providers, Business Partners, etc.) by eliminating or minimizing security incidents.

The information security standard enables the use of DEKRA information in external organizations in compliance with:

- Confidentiality
- Integrity
- and Availability.

With this information security standard DEKRA Management promotes the importance of the security of information and information systems of DEKRA and information security for the collaboration with external organizations.

2.2. Scope

This DEKRA information security standard is classified as “public” information and is provided to the following target group:

- Suppliers, Business Partners, Service Providers
- Business Customers and end customers
- Contractors, consultants, temporary employees
- And agencies and franchises

Further policies and standards could be applicable depending on the use-case and with consultation from DEKRA SE Information Security (HIT14).

3. General information security management

3.1. Contractual requirements

If an external organization can access sensitive DEKRA data or sensitive DEKRA data is made available to them, a Non-Disclosure Agreement (NDA) must be included in the contract, which applies to all employees of the external organization. This ensures the confidentiality of DEKRA data.

Even after the termination of the service or collaboration, confidentiality must be agreed on the information obtained. This shall also apply to the termination of the employment relationship of a person who was employed at the external organization and was deployed at DEKRA. The DEKRA legal department is to be consulted for this purpose.

If an external organization hires subcontractors for the provision of the service that was agreed with DEKRA, this must be reported to DEKRA before the subcontractor is commissioned. In addition, the external organization commissioned by DEKRA, e.g. suppliers, must ensure that the subcontractors are informed about the terms and conditions of the supplier's contract with DEKRA and that they also commit themselves to these terms and conditions in order to guarantee the security and protection of the information technology systems and the data stored in them at DEKRA. The subcontractors must therefore also be obligated by the supplier or external organization to the DEKRA NDA.

3.2. Information Security Management System (ISMS)

DEKRA expects that the contractually associated external organization processing DEKRA data will have an information security management system based on ISO 27001 or TISAX standards. With these information security standards, a risk-based approach is implemented to carry out a thorough analysis of all information and information processing systems at regular intervals. As a result, the threats and vulnerabilities for transmitted and stored information are recognized and treated with additional security measures in a timely manner to ensure an optimal security level in the organization.

3.3. Compliance with Information Security Standard

This DEKRA Information Security Standard must be observed in every contractually associated external organization.

If an external organization hires a subcontractor for the provision of a software or hardware service, the external organization that has a contractual relationship with DEKRA shall ensure that the subcontractor also undertakes to comply with the DEKRA Information Security Standard.

DEKRA reserves the right, within the framework of the contractual agreements and the agreed general terms and conditions of business, to inspect employees of the external organization as well as external organization itself for compliance with the NDA. In addition, any existing certificates for information security will also be inquired.

3.4. ISMS Awareness

DEKRA Information Security and the IT department can provide target group awareness programs for the external organization. The basic information security requirements are communicated through this Information Security Standard.

3.5. Non-compliance

Failure to comply with DEKRA Information Security Policies and Standards or failure to take appropriate measures to protect the systems, data, information and assets may result in legal action.

3.6. Handling exceptions

Exceptions to or deviations from this Information Security Standard must be documented, justified and approved by the involved DEKRA department. The detailed exception handling process can be requested from DEKRA Information Security.

4. Data classification

A classification is used to ensure adequate protection of confidential information. Regardless of the classification, the integrity and correctness of the data classification must also be protected. The assigned classification and the associated measures must be implemented depending on the sensitivity of the information. The most sensitive elements of the information define the classification level. Information recorded in different formats (e.g. printed documents, electronic voice recordings, electronic reports) must have the same classification regardless of its format.

Following data classes are to be implemented:

	Potential damage caused by unauthorized disclosure, alteration or destruction	Access restrictions
Public	None	
Internal	The potential damage is marginal, short-term nature, and limited to a single entity.	Only employees Others with NDA
Confidential	The potential for damage is considerable, or of a medium-term nature, or not limited to a single company.	Only named persons (can include trusted system administrators)
Strictly Confidential	The potential for damage threatens the company's existence, or is of long-term nature, or is not limited to a single company.	Only named persons, restricted use

4.1. Labeling

Proper labeling is a prerequisite for the safe handling of information. Information should therefore be marked according to its confidentiality classification.

In addition to the document owner, both the recipient and the processor of the information must be familiar with the data classes and therefore know and apply the associated requirements for handling the information.

Correct labeling is particularly important when confidential or strictly confidential information is transmitted between companies (e.g. to partner companies and suppliers). When marking information, the form of the information and its classification level must be taken into account.

If information is not marked and the classification is not obvious, it must be considered "internal".

4.2. Handling information

Classification	Labeling	Data at rest*	Data in transit*	Disposal
Public	none/optional (e.g. Note in imprint)	Electronic data: no restrictions Paper data: no restrictions	Electronic data: no restrictions Paper data: no restrictions	Electronic erasure: no restrictions Physical disposal: no restrictions
Internal	Indicate the level of confidentiality in national language or in English / or mark „internal“ on the first page of the document	Electronic data: Access restricted on external servers Paper data: Should be kept in locked storage when not in use	Electronic data: Encrypted on external networks Paper data: External transport only in closed envelopes	Electronic erasure: Secure erasure by overwriting media with at least one pass of writes with a fixed data value, such as all zeros. OR Degaussing device approved by security team for magnetic storage (following NIST SP 800-88 Rev. 1) Physical disposal: Procedure following ISO 21964 (DIN 66399), minimum class 1 level 2
Confidential	Indicate the level of confidentiality in national language or in English / or mark „confidential“ on every page of the document in electronic and printed format	Electronic data: Principally access restricted Paper data: Locked away when not in direct use and oversight, not to be exposed in public places	Electronic data: Always encrypted Paper data: Only in appropriately closed envelopes	Electronic erasure: Secure erasure by overwriting media with at least one pass of writes with a fixed data value, such as all zeros. OR Degaussing device approved by security team for magnetic storage (following NIST SP 800-88 Rev. 1) Physical disposal: Procedure following ISO 21964 (DIN 66399), minimum class 1 level 4
Strictly Confidential	Indicate the level of confidentiality in national language or in English / or mark „strictly confidential“ on every page of the document in electronic and printed format	Electronic data: Principally access restricted, individually encrypted files, messages or databases, storage on physically insecure devices (cloud, mobile data storage, laptop, phone) only if explicitly allowed Paper data: Locked away when not in direct use and oversight, location restricted, not to be used in public places	Electronic data: End-to-end encrypted Paper data: Only special courier service	Electronic erasure: Secure erasure by overwriting media with at least one pass of writes with a fixed data value, such as all zeros. OR Degaussing device approved by security team for magnetic storage (following NIST SP 800-88 Rev. 1) Physical disposal: Procedure following ISO/IEC 21964-1:2018-08 (DIN 66399), minimum class 1 level 5
*Exceptions possible with risk acceptance signed by the business owner				

5. Security control measures

5.1. Physical access control

DEKRA data stored or processed by external organization must be used in such a way that no unauthorized person can view or access this data. Confidential and strictly confidential documents must never be left unattended to prevent access by unauthorized persons.

The same applies to DEKRA IT equipment or systems used by external organizations. The equipment provided must be handled properly and protected against loss or unauthorized modification. Specific security measures are required when using mobile systems.

Third party companies should have adequate building security and a regulated visitor management system.

5.2. Admission control

Unauthorized use of the DEKRA data processing systems or connected external systems shall be prevented as follows:

- Registration in the network/on the PC is only possible with a valid account, the user identification is personalized.
- Use of a user ID or an account of another person is not permitted.
- The transfer of means of identification (e.g. SmartCards or SecurID cards) is not permitted.
- Use of an individual and secure password is guaranteed.
 - Passwords or PINs of a user ID intended for personal use (designated as "personal user ID") must be kept strictly confidential and may not be passed on.
 - The storage or writing down of passwords (e.g. on paper, via mobile devices or in files) is not permitted unless this is specified as a secure method.
 - If there is any suspicion that a password or PIN has been compromised or has become known, it must be changed immediately.
 - All passwords or PINs must be changed the first time they are used and after one year at the latest (the latter applies only to passwords).
 - Temporary passwords (e.g. for new accounts) must be changed at the first login.
 - All passwords or PINs must be changed on first use and after three months at the latest (the latter applies only to passwords).
 - Spying out passwords is not permitted.
 - Passwords are to be classified at least as confidential.
 - Do not use an identical password for private and professional purposes
 - The minimum password length enforced by systems must be observed. It depends on the specifications of the corresponding regulation.
 - Trivial passwords (e.g. "Test123456") or passwords with personal reference (e.g. name, date of birth) are not permitted.
 - If certain systems or applications require more complex passwords (as defined in the password regulation), then these requirements must be met.
 - A screen saver is installed on all clients/PCs, which requires a password to reactivate the system.
- Ensuring that those authorized to use an automated processing system have access only to the data covered by their access authorization.

- Access rights and roles are assigned according to the "need to know" principle, whereby the respective authorizations are tailored to the role (least privilege).
- The access/administration rights for PCs and/or servers are precisely documented.
- Authorizations that are no longer required are promptly removed as part of a user identification management system.
- Access to the PCs/server environment from outside is only possible via an encrypted communication (VPN tunnel).

5.3. User access control

The business requirements for access to DEKRA information systems must be defined and documented before they are approved. The access requirements are based on the business requirements.

The information owner and the system owner authorize access to data and IT services in accordance with the business requirements and security specifications. DEKRA's information systems are only used for authorized business purposes, unless otherwise agreed. All relevant security incidents are documented, including a record of successful and unsuccessful login attempts.

The physical and logical access to confidential and internal information and data processing systems are regulated. To ensure an appropriate level of access, various security measures are specified by the responsible information security officer.

5.4. Separation control

If external organizations also work with other customers, separation in multi-tenant architecture according to customer requirements, is logically and physically ensured.

A system separation for test and production must be implemented, based on a risk assessment.

5.5. Data media control

Data carriers (such as CDs, DVDs, USB sticks and hard disks) must be protected against loss, destruction and confusion as well as against unauthorized access.

Data carriers that are no longer required must be disposed in a safe manner as described in chapter 4.2. Transportation of data carriers with personal data to a certified shredding company may only be carried out in closed containers and in closed vehicles so that no material can be lost.

5.6. Transport control

The confidentiality and integrity of data must be ensured when information is transmitted.

Data traffic that transports personal data, e.g. e-mail, web access, is encrypted. Data transfers are encrypted, e.g. S-FTP, VPN. Unauthorized disclosure or transmission of data is not permitted.

Fax numbers and e-mail addresses are to be taken from current directories or requested from the recipient to avoid faulty transmissions. The sender is responsible for the content and distribution of an e-mail. The recipient is responsible for further processing and distribution. The creation and sending of chain e-mails is not permitted.

In all conversations (including telephone calls, video and web conferences) that involve or contain confidential or strictly confidential information, it must be ensured that this information cannot be overheard or recorded without authorization.

5.7. System security

Information should be protected from accidental or intentional modification or destruction.

Measures such as logging must be implemented, which subsequently checks and determines whether and by whom information has been entered, changed or removed from data processing systems.

A transfer of information must take place exclusively in accordance with the respective contractual agreements. This transfer must also be logged. The network/PCs are protected by a firewall system against unauthorized access from outside, and by a zone concept for perimeter security. It must be ensured that the information is up to date.

It must be ensured that stored information cannot be damaged by malfunctions of the systems. Status of systems are continuously and automatically monitored to detect malfunctions at an early stage. Regular maintenance must also be defined to review the integrity of e.g. databases. Only authorized and skilled personnel are allowed to make changes to systems during the change process and to correct malfunctions.

The security requirements for an information system apply throughout the entire life cycle, and the responsibility for compliance lies with the responsible business management. The introduction of new technologies must not jeopardize DEKRA's security level.

5.8. Availability control

Information and services should always be available when needed through proper archiving, the use of an anti-virus protection concept, an uninterruptible power supply and an appropriate backup and recovery concept.

Information system managers regularly develop, maintain and test plans to maintain the operation of critical information systems in accordance with regulatory, contractual or other business requirements.

5.9. Security Incidents

Any actual or suspected security or data privacy incident must be reported to the following recipients as soon as possible:

Information.security@dekra.com

konzerndatenschutz@dekra.com

All employees of the external organization and sub-contractors must be informed of the procedure for reporting security incidents.

The responsible Information Security Officer regularly reviews the reported security incidents, the feedback and the measures taken.

6. Document Control

Document Owner	HIT14/Prerna Walhekar
Translated by	Prerna Walhekar
Edited on	2021-01-22
Reviewed by	Thomas Hottewitzsch
Reviewed on	2021-01-22
Approved by	Thomas Hottewitzsch
Approved on	2021-01-22
Version	1.1

7. Version History

Date	Version	Name of editor	Revision
2020-10-26	0.1	Prerna Walhekar	First translated version
2020-10-27	1.0	Prerna Walhekar	Final Version
2021-01-22	1.1	Prerna Walhekar	DEKRA Scope correction

DEKRA SE

Abteilung HIT 14
Handwerkstraße 15
70565 Stuttgart
Telefon +49.711.7861-0
Information.security@dekra.com