Information Security Standard
Information Security for Externals

DEKRA

On the safe side.

Contents

1. Introduction

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. General conditions

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. Motivation

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, trainees, 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, trainees, temporary employees and
- Agencies and franchises

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

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. The NDA must be signed before the access is granted. 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 must also apply to the termination of the employment relationship of a person who was employed at the external organization and was deployed at DEKRA. In case of access to our systems, a procedure for the communication of termination for employees who belong to external organization must be defined. 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 or third party NDA with all DEKRA requirements included.

3.2. Information Security Management System (ISMS)

DEKRA expects that the contractually associated external organization processing DEKRA data must be certified for information security (ISO27001, TISAX or ISO27017, etc.). In case there is no certification, they must have an information security management system based on ISO 27001 or TISAX standards if they are going to access DEKRA information or systems. 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 processed 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 must 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. External organization staff must be trained in security on a regular basis.

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

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

4. Information 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 external organization must provide their information classification policy to map it with DEKRA information classification policy. The assigned classification and the associated measures must be followed depending on the sensitivity of the information. Information recorded in different formats (e.g. printed documents, electronic voice recordings, electronic reports) must have the same classification regardless of its format.

Following information classes are implemented at DEKRA:

	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
Classified	The potential for damage threatens the existence or vital interest of the government. Severe damage.	Only employees authorized by the Government

4.1. Labeling

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

Correct labeling is particularly important when confidential or strictly confidential information is transmitted between companies (e.g. to partner companies and suppliers) no matter if the information is digital or paper.

If information provided by the external organization is not marked or labeled, DEKRA will label this information "internal".

4.2. Handling information

DEKRA handles information based on the classification as follows:

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	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

	„confidential“ on every page of the document in electronic and printed format			approved by security team for magnetic storage (following NIST SP 800-88 Rev. 1) Physical disposal: Procedure following ISO 21964 (DIN 66399), minimum class 2 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 3 level 5
Classified	Indicate the level of confidentiality in national language or in English / or mark “Classified“ on every page of the document in electronic and printed format	Access restricted, individually encrypted files, messages or databases, storage on physically insecure devices (cloud, mobile data storage, laptop, phone) is forbidden.	End-to-end encrypted, include only the minimum amount of information necessary and the transmission must be recorded, when and by whom	Procedure following ISO/IEC 21964-1:2018-08 (DIN 66399), minimum protection class 3 and security level 6 and stir bags of shredded material to mix up contents
	*Exceptions possible with risk acceptance signed by the business owner and Managing Director and approved by Information Security			

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, strictly confidential and Classified 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.

All external organizations who access DEKRA building will be properly identified with an identification card.

Entry or walking around in DEKRA building, specifically (without the company of authorized personnel) in restricted access areas for externals is not permitted, unless they are accompanied by authorized DEKRA personnel and have signed the NDA.

In case of external access door to the general warehouse, it is intended for the entry/exit of goods, and its use by customers or other external persons is not allowed. The external personnel of the transport companies will only access the warehouse office position for administrative procedures.

Third party companies must have adequate building security and a regulated visitor management system at their locations.

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).
- In case of access to confidential, strictly confidential or classified information, multi factor authentication must be used in the external accounts

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 DEKRA 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, strictly confidential or classified 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. Vulnerability scan must be carried out. 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 must 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 incident must be reported to the following recipient as soon as possible:

Information.security@dekra.com

Incidents, involving personal data must be reported to the following responsible DEKRA legal entity recipient as soon as possible:

- datenschutz.akademie@dekra.com
- datenschutz.arbeit@dekra.com
- datenschutz.assuranceservices@dekra.com
- datenschutz.automobil@dekra.com
- datenschutz.certification@dekra.com
- datenschutz.claimsservices@dekra.com
- konzerndatenschutz@dekra.com
- datenschutz.incos@dekra.com
- datenschutz.media@dekra.com
- datenschutz.qualification@dekra.com
- datenschutz.testingandcertification@dekra.com
- datenschutz.visatec@dekra.com
- datenschutz.gkk@dekra.com

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

The responsible local DEKRA Information Security Officer and Data Protection Officer reviews the reported security incidents regularly, and provides the feedback and involves the responsible parties at the earliest.

6. Document Control

Document Owner	Global Information Security
Created by	Prerna Walhekar
Reviewed by	Mabel Gonzalez
Reviewed on	2023-01-26
Approved by	Dražen Morog
Approved on	2023-01-26
Version	1.3

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
2021-11-24	1.2	Mabel Gonzalez and Prerna Walhekar	New requirements for termination in chapter 3.1, physical security requirements in chapter 5.1 and minor changes Minor changes to chapter 3.2 concerning certification and chapter 5.9 concerning the email addresses
2023-01-26	1.3	Mabel Gonzalez	New information class is included in chapter 4 Mandatory security awareness is included for external organization staff in chapter 3.4. Adaptation of the policy to the new classification category and minor changes Change in the labeling of this document from Internal to Public Document Reference Chapter is deleted because there were internal references

DEKRA SE

Global Information Security HGIIT340
Handwerkstraße 15
70565 Stuttgart
Telefon +49.711.7861-0
Information.security@dekra.com