# Directive

# Information Security for External Parties

## Content



| **Overview** | |
|---|---|
| Description | Information security requirements for external parties (e.g. suppliers and IT service providers). |
| Area of application | Global |
| Main process | Manage security |
| Related to process or org. framework | - |
| Information class | Internal |
| Translated document | false |

| **Control data** | |
|---|---|
| Author | Beckmann Leon SI-IS |
| Creation date | 14.01.2023 |
| Verifier | Ebert Sebastian GG-Q2 |
| Verification date | 16.01.2024 |
| Approver | Kreuzer Norbert SI32 |
| Approval date | 16.01.2024 |
| Master title | [Master Title] |
| Master creator | [Master Creator] |
| Master preinspector | [Master Preinspector] |
| Master releaser | [Master Releaser] |
| Version | 1.0 |

# 1 Purpose

To ensure the security of DRÄXLMAIER information, this directive defines requirements for external parties (suppliers and other business partners).

# 2 Area of application

This directive applies to all external parties that have business relations with DRÄXLMAIER. It is formally agreed as part of the service contract.

# 3 Definition of terms, abbreviations & roles

| Term | Definition |
|---|---|
| DRÄXLMAIER | The DRÄXLMAIER group (https://www.draexlmaier.com) incl. all subsidiaries and in particular the DRÄXLMAIER company that is contracting party in the business partnership with the external party. |
| DRÄXLMAIER Information | Non-public Information (digital, verbal, physical) shared through DRÄLXMAIER with the external party as part of the business partnership. Not covered under this term is information that is publicly available. |
| DRÄXLMAIER IT services | Includes digital services and portals that are rendered by or on behalf of DRÄXLMAIER and where the external party received access credentials. This includes among others the supplier portal of the DRÄXLMAIER Group, access to the DRÄXLMAIER network and access to DRÄXLMAIER collaboration services. |
| DRÄXLMAIER network | Closed IT network that connects all DRÄXLMAIER sites and IT devices for secured data communication. |
| Abbreviations | All relevant abbreviations you can find in the D-World abbreviations list.<br><br>D-World -> Worldwide -> Service -> Abbreviations |

| Role | Definition |
|---|---|
| External party | Any company that is in business relation with a subsidiary of the DRÄXLMAIER group or one of its affiliates (see http://www.draexlmaier.com for details). This includes among other suppliers, customers, research facilities, authorities. |
| DRÄXLMAIER contact | Ordering person and/or buyer at DRÄXLMAIER |

# 4 Content of the directive

## 4.1 Security of DRÄXLMAIER Information

The external party must implement policies, procedures, and organizational responsibility to ensure the security of DRÄXLMAIER information. The organization, policies and procedures shall be based on state-of-the-art industry security standards, e.g., TISAX (Trusted Information Security Assessment Exchange), ISO 27001 or NIST cybersecurity framework.

The external party agrees to protect DRÄXLMAIER information and its own information, which affects the business with DRÄXLMAIER in any way, against unauthorized access, manipulation, deletion, destruction, theft, or loss. This includes that the external party ensures to segregate DRÄXLMAIER data from data of other customers and to take appropriate protective measures against access to the DRÄXLMAIER information by other customers, and that the external party ensures to implement state of the art solutions for a complete data recovery at any time.

If not indicated otherwise, the external party shall assume default classification for DRÄXLMAIER information as “confidential”.

## 4.2 Instruction of personnel

All personnel of the external party are regularly trained by the external party according to information security standards mentioned above. In addition, all personnel of the external party with access to DRÄXLMAIER IT

services or DRÄXLMAIER data must be instructed according to the regulations set out by this agreement. The instruction must be documented in writing and at least annually renewed. The external party commits on behalf of its personnel that the instructions are followed.

## 4.3 Handling of DRÄXLMAIER IT services

Information provided as part of accessing DRÄXLMAIER IT services is protected under the confidentiality agreement concluded between DRÄXLMAIER and the external party and meant to be processed with secured DRÄXLMAIER IT services only. Active participation of the external party is requested for the following:

- For accessing DRÄXLMAIER IT services, access credentials (e.g., username and password, security token) have been issued to personnel of the external party. Changes in responsibilities or personnel at the external party side must be reported in writing to the contact at DRÄXLMAIER without undue delay for adjusting access permissions to ensure need-to-know principle.

- The external party ensures that access credentials are handled securely according to state-of-the-art industry security standards (e.g., TISAX) and that its employees are provided with appropriate processes, tools, and training. Especially the sharing of individually assigned access credentials (e.g., passwords, security tokens) is not allowed.

- It is forbidden to extract information from DRÄXLMAIER IT services (e.g., by screenshots, photography, video recordings, downloads, manual or automated e-mail forwarding etc.) unless the external party is specifically instructed in writing to do so. Exceptions to this regulation need to be requested from information-security@draexlmaier.com.

- All IT services are provided solely for the purpose of fulfilling contractual obligations towards DRÄXLMAIER. Usage for any other purpose is not allowed.

- Transfer of data to or from DRÄXLMAIER IT services shall not take place unless specifically instructed to do so. For general e-mail communication it is advised to enable a secured connection between e-mail servers by enabling transport encryption as mandatory. For details, the external party shall reach out to the contact person at DRÄXLMAIER.

## 4.4 Requirements for Remote Access

All devices used to access DRÄXLMAIER IT services, including those owned by the external party, must be maintained with due care to ensure they do not pose a security risk. This includes at a minimum that the devices have effective anti-malware protection, a defined security configuration, that security updates are applied regularly, and device integrity is monitored. For accessing the DRAEXLMAIER network, the DRÄXLMAIER standard VPN solution will be accepted by the external party.

## 4.5 Unwanted functionalities in software

The external party must ensure that, in the context of the business relation, used or supplied software (e.g., goods or firmware) is free from undesired functionality (i.e., functionality which was not ordered and accepted by DRÄXLMAIER) and malware (e.g., viruses, trojans, worms). This includes functionality which affects the confidentiality, integrity, and availability of the contractually agreed services and goods (including software and hardware), especially functionality for unwanted data leakage, unwanted manipulation of data and control flow.

## 4.6 Onsite visits

Personnel of the external party visiting or working at a DRÄXLMAIER site must fully comply with instructions provided to them as visitors during initial registration. It is not allowed to bring in additional personnel without proper registration nor to take pictures, video, or audio recordings.

## 4.7 Reporting of security incidents

If the external party has reason to believe that a security incident occurred (e.g. due to data breach, cyber-attack) on their side where it cannot be excluded that DRÄXLMAIER is affected, especially in case of an unauthorized access to DRÄXLMAIER information (including credentials) or systems, or in case of potential

disruptions in the supply chain, the external party has to inform DRÄXLMAIER immediately via isim@draexlmaier.com.

In addition, the external party agrees to take all necessary actions to analyze the security incident, limit the potential damage, and accepts all appropriate measures taken by DRÄXLMAIER to protect the IT infrastructure of the DRÄXLMAIER Group (e.g., disconnecting the external party from DRÄXLMAIER IT systems). Further, the external party agrees to provide detailed information about the security incident, especially Indicator of Compromised (IOCs), Tactics, Techniques and Procedures (TTP) and a final incident report to isim@draexlmaier.com as soon as available.

Before the reconnection of the external party to the DRÄXLMAIER IT infrastructure, the external party must provide a written statement that no further risk for DRÄXLMAIER due to this security incident exists.

## 4.8 Proof of Information Security Compliance

To ensure the adequate implementation of information security at the external party, especially for the protection needs of exchanged sensitive information and the supply capability of critical supplier, DRÄXLMAIER reserves the right to request proof (via appropriate information security certification, such as TISAX) from the external party without additional compensations. The parties may agree on a reasonable period of time for the initial assessment of a site in accordance with the agreed information security proof (e.g. TISAX certification).

## 4.9 Right to audit

DRÄXLMAIER reserves the right to audit the external party on compliance to the regulations set out in this directive and to other information security agreements between DRÄXLMAIER and the external parties when at least one of the following conditions is met:

- The external party is not able to prove the implementation of the information security requirements stated in this directive (as described in 4.8).
- DRÄXLMAIER receives information that the external party violates the regulations from this directive and from other information security agreements between DRÄXLMAIER and the external party, or if there are justified indications for such violations.
- DRÄXLMAIER receives information about a security incident at the external party, which might negatively affect DRÄXLMAIER, or if there are justified indications for a security incident at the external party, and there are justified indications that the incident is due to gross negligence, intent, or non-compliance with DRÄXLMAIER requirements.

The audit might take place at the external company's site, at DRÄXLMAIER sites or remote. The audit might be carried out by an authorized third party on behalf of DRÄXLMAIER, given that this third party is bound to secrecy. The external party must support all audit activities accordingly.

## 4.10 Subcontractors

The external party must ensure that its subcontractors are required to comply with the regulations stated in this directive via contractual agreements and that these regulations are forwarded by its subcontractors throughout the whole supply chain. In addition, forwarding of DRÄXLMAIER information to subcontractors is per default not allowed and requires a written approval from DRÄXLMAIER.

## 4.11 Information security contact

If applicable and available, the external party agrees to maintain their information security contact (e.g., CISO) within the DRÄXLMAIER Supplier Portal and will proactively update this information when the information security contact person changes. For this, the external party will create a new contact and set the attribute “Function” to “Information Security”.

## 4.12 End of business relation

In the event the business relation ends (e.g., all services / goods delivered), authorization to access DRÄXLMAIER IT services is withdrawn. DRÄXLMAIER will initiate procedures upon notification to deactivate relevant accounts while the external party must inform its personnel not to use the access anymore and return all assets provided (e.g., IT equipment, access cards etc.) to DRÄXLMAIER. Further, the external party will provide written confirmation that all DRÄXLMAIER data has been deleted.

### 4.13 Liability

The external party shall be liable for and reimburse and compensate DRÄXLMAIER for all damages, costs and expenses incurred by DRÄXLMAIER, resulting from any, at least, negligent violations against the obligations of this directive.

# 5 Change history

| Version | Change description | Changed by | Change date |
|---|---|---|---|
| 1.0 | Complete rework and migration to CDMS | Leon Beckmann | 08.01.2024 |
| | | | |
| | | | |
| | | | |