DRÄXLMAIER

Directive

[Information Security for external parties]

Content

1. Purpose

In order to ensure security of DRÄXLMAIER information, this directive defines requirements for external parties (suppliers and other business partners) that are granted access to information technology (IT) services rendered by or on behalf of DRÄXLMAIER.

The external party has to ensure that all technical and organizational measures defined in this directive are implemented and that personnel is properly instructed before accessing DRÄXLMAIER IT services.

2. Area of application

This directive applies to all external parties that are granted access to DRÄXLMAIER IT services. 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 trough 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 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 others suppliers, customers, research facilities, authorities.
DRÄXLMAIER contact	Ordering person and/or buyer at DRÄXLMAIER

4. Content of the directive

4.1 Information Security Management

The external party must implement policies, procedures and organizational responsibility to ensure security of DRÄXLMAIER information. The organization, policies and procedures shall be based on corresponding industry security frameworks, e.g. ISO 27001 or NIST cybersecurity framework and effectively support the protection of DRÄXLMAIER information in the context of the business partnership.

4.2 Instruction of personnel

All personnel of the external party with access to DRÄXLMAIER IT services must be instructed according to Annex A “Information Security instructions for external parties” and the regulations set out by this agreement. The external party takes on the responsibility to ensure the successful instruction and training of the instructions stated above to its employees . 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 Information

DRÄXLMAIER practices Information Classification as defined by the VDA White Paper “Harmonization of Classification Levels”. If not indicated otherwise, the external party shall assume default classification for DRÄXLMAIER information as “confidential”.

4.4 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:

4.4.1 Account management

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 in order to ensure need-to-know principle.

4.4.2 Credential handling

Sharing individually assigned access credentials (password, security token) is not allowed. The external party has to support secure handling of access credentials by providing processes and tools to its personnel to allow correct handling.

4.4.3 Information extraction

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.

4.4.4 Intended use

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

4.5 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 an effective anti-malware protection, a defined security configuration, that security updates are applied regularly and that device integrity is monitored.

4.6 Integration of IT equipment

Integration of non-DRÄXLMAIER owned IT-equipment in the DRÄXLMAIER network is not allowed. If the business relation involves delivering / installing such equipment, its integration and use is subject to the “General Technical Delivery Specifications (GTDS) DRÄXLMAIER Group”.

4.7 Securing communication

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, external party shall reach out to the contact person at DRÄXLMAIER.

4.8 Onsite visits

Personnel of the external party visiting or working at a DRÄXLMAIER site must fully comply to 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.

4.9 Reporting of security incidents

A security incident is any event that might endanger the confidentiality, integrity or availability of DRÄXLMAIER information including provided access credentials. If the external party has reason the believe that a security incident occurred on their side where it cannot be excluded that DRÄXLMAIER is affected, the DRÄXLMAIER contact and itcc@draexlmaier.com must be immediately notified.

4.10 Right to audit

DRÄXLMAIER reserves the right to audit the external party on compliance to the regulations set out in this directive and applicable documents. The audit might take place at the external companies site, at DRÄXLMAIER sites or remote. The audit might be carried out by an authorized third party on behalf of DRÄXLMAIER. The external party has to support all audit activities accordingly. If applicable, DRÄXLMAIER will also accept security certificates of independent audit bodies as compliance statement.

4.11 Involvement of subcontractors

The involvement of subcontractors follows the general terms and conditions set out as part of the business partnership. If subcontractors are provided access to DRÄXLMAIER IT services under guidance of the external party, it must ensure contractual commitment to regulations set out in this directive. Forwarding of information from DRÄXLMAIER IT services as agent (extracting data and forwarding it to the subcontractor) is not allowed (see section 4.4.3).

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.

4.13 Liability

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

5. Applicable documents

Name	Description
ISEP	Information Security instructions for external parties

6. Change history

Last Change:

Replacing former directive „DR_Information_Security_for_External_Companies_and_Partners“ with a focus on external access to DRÄXLMAIER IT systems.

Version	Change description	Changed by	Change date
1	Initial issuing	R. Pöhlmann	01.12.2021