Directive

Information Security Directive for External Companies and Partners

Content

Overview	
Short description	Directive for Information Security Directive for Ex-ternal Companies and Partners
Key words	Internal;InfoSec External;
Area of application	PublicGLO - Global
Main process	Informationstechnologie managen / information technology management;
Related to process	-
Information class	Public-
Translated document	NO

Control data

Author	TaubenthalerJuergenKPO-IS
Creation date	02-02-2018
Verifier	MenschelConniQM1
Verification date	02-02-2018
Approver	ZieglerManfredIG
Approval date	02-02-2018
Version	01
Translation approver	-
Translation approval date	-

1. Purpose

The purpose of this directive is to describe and organize the required information security at the Partner Companies …

2. Area of application

GLO - GlobalThe area of application extends to **all companies and their employees who have business relations with the Draexlmaier Group in which they are bound by Non-Disclosure agreement. They shall hereafter be referred to as Partner Companies. This directive is valid worldwide.**

Partner Companies are external service providers, consultants assigned with projects, machine manufacturers with maintenance access, sub-contractors, joint venture and automotive partners.

At the same time, the applicable national laws and regulations have to be adhered to.

3. Definition of terms, abbreviations & roles

Term	Definition
Abbreviations	All relevant abbreviations you can find in the D-World abbreviations list D-World -> Worldwide -> Service -> Abbreviations

4. Content of the directive

4.1 Personal Security

All those who receive, process and use information within the scope of business objectives of the Draexlmaier Group, are underlying the confidentially agreements with the partner company. All data records are deemed as being the ideas of the Draexlmaier Group or its clients. They may be received, processed and used only within the scope of their task assignment.

Any exceptional incidents, such as e.g. unusual system performance, suspected misuse, viruses, offensive or harassing contents as well as pornography and glorification of violence are forbidden and must reported to Information Security without delay.

4.2 Using Hardware and Software Components of the Draexlmaier Group

All Partner Companies that use hardware and software component of the Draexlmaier Group have to adhere to the following instructions.

4.2.1 Hardware & Software

All changes to hardware configurations and software installations and/or updates may only be made by specialized IT staff of the Draexlmaier Group or the staff of the Partner Company with approval from IT staff of the Draexlmaier Group. This also applies to users with local administration rights.

4.2.2 E-Mail and Use of Internet

Rule-based forwarding of e-mails (e.g. in the case of absence due to vacation) to an external/private e-mail address is not permitted. In this connection, confidential information may be subjected to the unsecured transmission and saving of data by third parties. Sending chain mail using e-mail addresses of the Draexlmaier Group is also forbidden.

4.2.3 Virus Protection

All the data areas of the Draexlmaier Group are automatically checked for viruses. All the employees of the Partner Companies who deal with the IT systems of the Draexlmaier Group have to make sure that the provided IT systems have active, up-to-date virus scanners.

4.2.4 Username and Password

Each user is solely responsible for keeping his/her username with password confidential. A password has to have at least eight symbols, consisting of letters, numbers and special characters, and may not contain any personal data, such as e.g. car registration numbers, date of birth, names of pets etc. Passwords may not be conveyed to anyone (e.g. vacation replacements).

4.2.5 Locking workstation

The workstation has to be locked on being left or the screen-saver has to be activated by means of the password. If possible, care should be taken to ensure that access to the workstations is granted only to authorized persons, e.g. by locking the office

4.2.6 Use of Private Equipment / Company Data on Private Equipment

This includes hardware and software components that are the private possession of employees of the Partner Companies.

The use of private equipment in the company network of the Draexlmaier Group is not permitted under any circumstance. Furthermore, saving and filing company data of the Draexlmaier Group on private equipment is not permitted.

4.2.7 Simultaneous Connection to the Network of the Draexlmaier Group and the Mobile Internet

Any IT system which already has active connection to the network of the Draexlmaier Group may not under any circumstance be simultaneously connected to the mobile Internet or establish connection via a local Internet connection.

This primarily applies to Notebooks/PCs with expansion boards for the mobile Internet and Smartphones. In any case, simultaneous connection by way of a corresponding adapter configuration is prohibited.

By the same token, routine functions may not be activated on these devices under any circumstance. This would cause considerable restrictions to the security and stability of the network.

4.2.8 Securing the Wide Area Networks (WAN)

Transmitting data via public and private networks is an operational necessity nowadays. At the same time, there are a series of security aspects that have to be observed:

- Private connections are preferable to public connections. The preferred connections include MPLS and ENX/ANX.
- When using connections via public networks, make sure that the data cannot be manipulated or tape-recorded during authentication and transmission. This requires TLS/SSL and VPN with codes at least 512 bits long. This is also ensured as the best available technology for site to site connections.
- Remote access: this refers to dialing in company equipment, usually Notebooks, via a public network. The access ranges over the same resources as if the connection were being made directly, geographically in the area of the company network.

4.2.9 Securing the Wireless Local Area Networks in the Company Network (WLAN)

For security reasons, it is always preferable to use cable-based connections and to switch off WLAN access points. This provides the greatest protection against misuse by third parties.

For reasons of security and compatibility, WLAN connections may only be operated and used with the following settings.

Detailed configuration:

- Ad-Hoc mode may not be activated;
- The log-in password for the WLAN access point has to contain at least 12 symbols and may not be disclosed to third parties;
- WPA2 with a preshared key and AES data enciphering or certificate-based encryption are considered as safe network authentication and data enciphering.

4.2.10 Use of Network Analyses and Hacker Tools

It is strictly forbidden to use any hacker tools or technical equipment to unlawfully gain access to or spy out confidential data.

4.2.11 Central Internet Access

Generally speaking, if Internet access is needed in computers connected to the Draexlmaier network, then all Internet traffic has to run via the central Internet accesses of the Draexlmaier Group.

4.3 Integrating Hardware and Software Components of the Partner Companies

All Partner Companies that integrate hardware and software components into the network of the Draexlmaier Group are required to observe the following instructions.

4.3.1 Integrating PC and Notebook Workstations

This includes PC and Notebook workstations that are required for external service providers. They are e.g.: Systems for external temporary designers or external developers / project members. In order to meet the demands of network access, security, support and service optimally, these systems have to be connected to the network of the Draexlmaier Group according to the following procedure.

1. Primarily hardware and software components of the Draexlmaier Group are to be held available and/or purchased.

2. In the event that option 1 is not feasible for cost or time reasons, external equipment that complies with the hardware standards of the Draexlmaier Group has to be re-started with Unattended Setup and integrated into the network.

3. In the event that options 1 and 2 are not feasible for software or contract reasons, the following procedure shall apply:

a. Check by the owner using an installed, updated virus scanner before connection is made to the network of the Draexlmaier Group.
b. Written confirmation by the owner to the responsible person / project manager of the Draexlmaier Group for independent, weekly updating of the virus definition file (pattern file).
c. Issue and rename using a compliant computer name of the Draexlmaier Group.
d. The Partners are required to provide appropriate software licenses for all the pre-installed software products that are subject to license.
e. All pre-installed software products that are subject to license are to be transferred to the Draexlmaier Group when the machines are approved by the Partner

4.3.2 Integrating PC's and Controlling Production Machines

This refers to PC's and controls that are delivered with the machines and production units.

All the Partner Companies that deliver hardware and software components with machines and production units to the Draexlmaier Group have to comply with the following specifications and agree on them with the responsible departments of the Draexlmaier Group:

4.3.2 Interface descriptions of IT systems

(Please cross where applicable)

[ ] IT systems (PCs or servers) are not required for the service provider's solution.

[ ] The service provider's solution contains an IT system, but does not require active connection to the network of the Draexlmaier Group.

[ ] The service provider's solution contains an IT system and requires active connection to the network of the Draexlmaier Group.

The service provider's solution is subject to the following requirements:

- Integration into the ActiveDirectory domain of the Draexlmaier Group has to be possible;
- Support by the manufacturer when security updates are installed by the Draexlmaier Group (operating system + application software) has to be provided in two-week intervals.
- The McAfee virus scanner has to be able to be installed by the Draexlmaier Group with daily updates of the virus signatures.
- If new software is introduced in the Draexlmaier Group due to the solution of the service provider, it should contain an integrated patch management system.
- It has to be possible to avoid plain-text protocols (http,ftp, telnet)
- Data security has to be ensured by means of an appropriate cryptographic procedure such as AES, 3DES or better.

4.4.3 Service and Maintenance

Exchange of old PC's, to ensure the interfaces to the network of the Draexlmaier Group and remote maintenance.
[ ] The supplied IT systems will be maintained at a minimum level for the Draexlmaier Group with regards to up-to-datedness of the software. The costs for this are included in the maintenance contract.

[ ] The supplied IT systems will be maintained at a minimum level for the Draexlmaier Group with regards to up-to-datedness of the software. The costs for this are not included in the maintenance contract.

4.3.4 Remote Maintenance

[ ] Remote maintenance is not required.

[ ] Remote maintenance is required.

The service provider's solution results in the following requirements:

- Remote maintenance will be provided via Internet and secured connections with the present buyer's solution only. The service provider requires a broadband Internet connection and current Web Browser with Java and/or ActiveX support. As an alternative, a locally installed Citrix Client can be used.
- Authentication will be made by the user name, password and code generated by a token. This token will be provided by the requestor department.
- In order to switch on the service provider's solution, the Draexlmaier IT staff shall be required to install remote control software.
- For server operating systems, Net Support will be installed on the service provider's solution by the Draexlmaier IT staff.
- For client-based systems, VNC will be installed on the service provider's solution by the Draexlmaier IT staff. Each of these shall be done in the version stipulated by the Draexlmaier IT staff.

4.4 Integrating of a Site from Partner Company

Partner networks and sites that are connected to the network of the Draexlmaier Group are required to observe the following instructions.

The Partner is to ensure adequate fire and access protection.

The layout of the structurally engineered infrastructure is the responsibility of the Partner and has to comply with the standards of the Draexlmaier Group.

The Partner has sole responsibility for the conception and operation of the site with regards to the IT infrastructure (terminal equipment, servers, network components).
Before the network of the Partner Company is connected to the network of the Draexlmaier Group, documentation is to be submitted as requested and subjected to an audit if necessary.

4.4.1 Securing the Network between Draexlmaier Goup and external partner

If the external partner has a direct data connection to the Draexlmaier network, some internal security measures need to be in place.

The external partner must implement internal controls to prevent the unauthorized connection.
Any Routing or NAT of any device, connected to Draexlmaier network is not allowed.

In particular, any addition in devices and/or modification of the topology of the network must be approved first from the Draexlmaier IT staff in order to implement such a change.
This includes connections to any network switches, firewalls, routers inside the main IT server / communication room or inside any network distribution cabinet

4.5 Remote login with Hardware and Software Components of the External Company

All the Partner Companies that dial into the network of the Draexlmaier Group for the purpose of remote maintenance or project order are required to observe the following instructions.

4.5.1 Permanent or Long-Term Remote Maintenance / Maintenance Access Bound by Contract

Remote access for external service providers and maintenance companies has to be installed by way of standard accesses via a terminal server only. It provides safe, uniform access to the IT systems of the Draexlmaier Group.

Apart from that, machine-control PC's or special machine PC's that are supplied as a part of an overall solution by the machine manufacturer can receive remote maintenance.
This requires the possibility of installing the VNC program on PC's or Net Support program on servers.

Dial-in by the maintenance company is done by the Citrix WebGateway with a one-time password (OTP) and enables two dial-in procedures, depending on the agreed on response and availability times:

The maintenance company can dial into the Draexlmaier network immediately without requiring the approval of a Draexlmaier employee.
Dial-in by the maintenance company requires the approval of an employee of the Draexlmaier Group.

Homepage for Citrix Maintenance TSE
https://login.draexlmaier.com

Name of the published application for external service providers:
"Remote Login for external service providers"

4.5.2 Support Request on Short Notice/ AdHoc

Problems on short notice that cannot be solved by employees of the Draexlmaier Group themselves and which require DesktopSharing by the Partner Company can also be managed like e.g. Teamviewer as an alternative.

4.6 Responsibility

This directive is to be applied and adhered to by all Partner Companies. Any breaches of this directive will be reviewed individually according to the effective legal situation and punished accordingly.

4.7 Audits

Partner Companies have to enable the Draexlmaier Group to adhere to the specifications, either by way of self-assessment or by on-site audit by the Draexlmaier Group.

4.8 Key Contacts

Support queries are to be directed to the central User Service:
Tel: +49 (0)8741/ 473333 E-mail: DRX-Userservice@draexlmaier.com
Exceptions to this directive have to be approved in writing by Information Security: E-mail: Information-Security@draexlmaier.com

5. Change history

Last change:
Upload into document management system. Version starts again at 1 (J.Taubenthaler 29.01.18)

Version	Change description	Changed by	Change date