Baseline Information Security Requirements for Suppliers

Change History:

Date	Version	Updated By	Approved By	Description of Change
09.09.2022	1.1	Nikolay Barakov	CIO AIM	Changelog

Table of Contents

1 PREFACE

1.1 Purpose

The purpose of this document is to represent the information security requirements which 3rd parties like service providers, contractors, suppliers and cooperation partners shall comply with it.

1.2 Scope

The scope of this document covers all 3rd Parties (i.e. service providers, contractors, suppliers and cooperation partners) who have legitimate business requirements to access any data owned or controlled by the Group that is stored, processed or transmitted through or within its premises or information systems.

1.3 Responsibility

- Reviewing and updating the document periodically: CISO
- Implementing the document: All employees of the Group and 3rd parties like service providers, contractors, suppliers and cooperation partners
- Approving document changes: CIO AIM
- Performance and compliance with the document requirements: CISO

1.4 Intended Audience

All employees and 3rd parties like service providers, contractors, suppliers and cooperation partners.

1.5 Definitions

The **Group** – all companies that belong to Röchling

EBRG – Executive Board Röchling Group

CISO – the accountable employee for Information Security for the Group appointed by the EBRG

CIO AIM – Chief Information Officer of Röchling SE & Co. KG

Personally Identifiable Information (personal data): Any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2 General requirements

- Supplier shall protect Group's information by implementing applicable controls as set forth in this document and must ensure that this information is not at risk.
- Supplier shall regularly consider all information security controls stated below in this document and take conscious decisions as to if a specific control should be implemented fully, partly, or not at all, or, if alternative protection measures should be implemented.
- The Group must approve in advance all alternative measure including those which are partly or not at all.
- The Supplier shall sign a NDA as part of the contract.
- A confirmation of compliance with the security requirements must be signed by the Supplier before the respective company has access to Group's networks, systems or data.

2.1 Organization of Information Security

- Supplier shall appoint from their organization a contact person with relevant information security experience.
- Supplier shall maintain "Segregation of Duties" where possible, ensuring that at least two individuals are responsible for separate parts of any task, so that no single role or account, can access, modify or use Group's Information without authorization or detection.

2.2 Human resource security

The Supplier shall:

- Ensure that all personnel with access to Group's information has signed a Non-Disclosure Agreement (NDA) with the Supplier.
- Have an onboarding process that includes verifying the identity of personnel (the background and skills they state).
- Have a personnel termination process that includes revoking access rights, seizing IT equipment, invalidating company access card (if applicable) as well as notification of continuous confidentiality obligations.

2.3 Asset management

The Supplier shall:

- Not takeout any assets from Group's premises without prior authorization.
- Not to connect their own equipment to the Group infrastructure without prior authorization.
- Treat all Group information at least as "Confidential" information.
- Not excessively store, print, copy, disclose or process by other means outside the purpose for using any Group's information.
- Process and store Group's information logically separated from their own information.
- Upon conclusion or termination, the Supplier shall sanitize and securely destroy (or return to the Group) all copies of all Group's information, including all backup and archival copies, in any electronic or non-electronic form (exception is possible based on legal requirements). If the destruction takes place on external party's site, a signed written statement shall be sent specifying the items or information destroyed, the method of destruction, the date / time and the person performing the destruction.

2.4 Access control

- Access to Group's information shall be restricted to personnel individually and on a need to know basis.
- The Supplier shall provide a list of all their employees who need access to Group systems or applications, including the associated rights and privileges.
- Remote access to the Group's infrastructure is only allowed through communication channels and technologies approved by the Group (VPN, leased line, two factor authentication).
- Access to the Group's infrastructure shall be made using access and identity management controls:
    - ➢ Using unique User IDs
    - ➢ Authorizing and administering access rights and access privileges
    - ➢ Ensuring that access rights and access privileges remain appropriate
    - ➢ Checking that obsolete access rights have been deleted
    - ➢ Review whether the access rights granted are in line with business and security requirements. The review process shall be made at least yearly or when a significant change occurs.
    - ➢ Records shall be kept in an auditable manner showing which Group information has been accessed, modified, disclosed or disposed.
- Suppliers who might have tasks to manage some part of the Group infrastructure shall apply and enforce the password requirements adopted by the Group.

2.5 Cryptography

- The e-mail communication with the Group shall be performed securely using industry standard encryption techniques.
- Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.
- Group's information shall be protected using encryption techniques or equivalent protection measures when the information is in transit and in rest.

2.6 Physical and environmental security

- All suppliers entering Group's premises shall carry their badges/cards in clearly visible places for identification.
- Group information and/or equipment shall be monitored at all times and shall not be left unattended in public places if taken outside Group's premises.

2.7 Operations security

Suppliers providing services that support Group's information systems shall implement the following controls:

- Systems shall be provisioned with enough capacity to ensure continued availability.
- Changes to the systems or the infrastructure shall follow the Change management process implemented in Group.
- Malware protection on the devices connected to the Group infrastructure shall be deployed and kept up to date.
- All privileged user actions shall be logged. Any changes to these logs by a system, privileged or end user must be detectable. Security-related events shall be recorded in logs including event

types such as failed log-on, system crash, changes of access rights and event attributes such as date, time, User ID, file name and IP address, where technically feasible.

- Logs shall be reviewed periodically and be kept for at least 90 days and made available to the Group when requested.
- Backups shall be performed and maintained to ensure continuity. The frequency and the type of the backups shall be agreed with the Group.
- Vulnerability and patch management process shall be in place to prioritize and remediate vulnerabilities based on their severity, according to the requirements stated in the vulnerability management policy adopted in the Group.

2.8 Network security

- Supplier networks used to access Group's information or networks shall have security controls that can prevent unauthorized access, e.g. firewalls, intrusion detection/prevention systems.
- Supplier wireless network connections transferring Group's information shall be encrypted according to best practices.

2.9 Incident management

- Supplier shall have a documented security incident management process to detect and handle incidents.
- Supplier shall report immediately security incidents or weaknesses related to their own infrastructure or to information/systems owned by the Group.

2.10 Business continuity management

- If requested, the Supplier together with representatives from the Group shall conduct yearly a risk assessment based on Group information security risk management process to identify and mitigate potential threats.

2.11 Compliance

- Supplier shall ensure protection and privacy of personal identifiable information in accordance with relevant data protection legislation and the applicable local laws.
- Upon request from the Group, the Supplier shall be able to demonstrate compliance with the security requirements stated in this document.

Editorial Notes

Document Type	REQ	Requirements
Document Number	ISMS-REQ-15	
Created by	Nikolay Barakov	
Valid From	For Röchling SE & Co. KG and Automotive division from 1st of October 2021, for Medical and Industrial divisions from 1st of January 2022	

Approval Signatures

Mannheim, 20.09.2022

CIO AIM, Signature