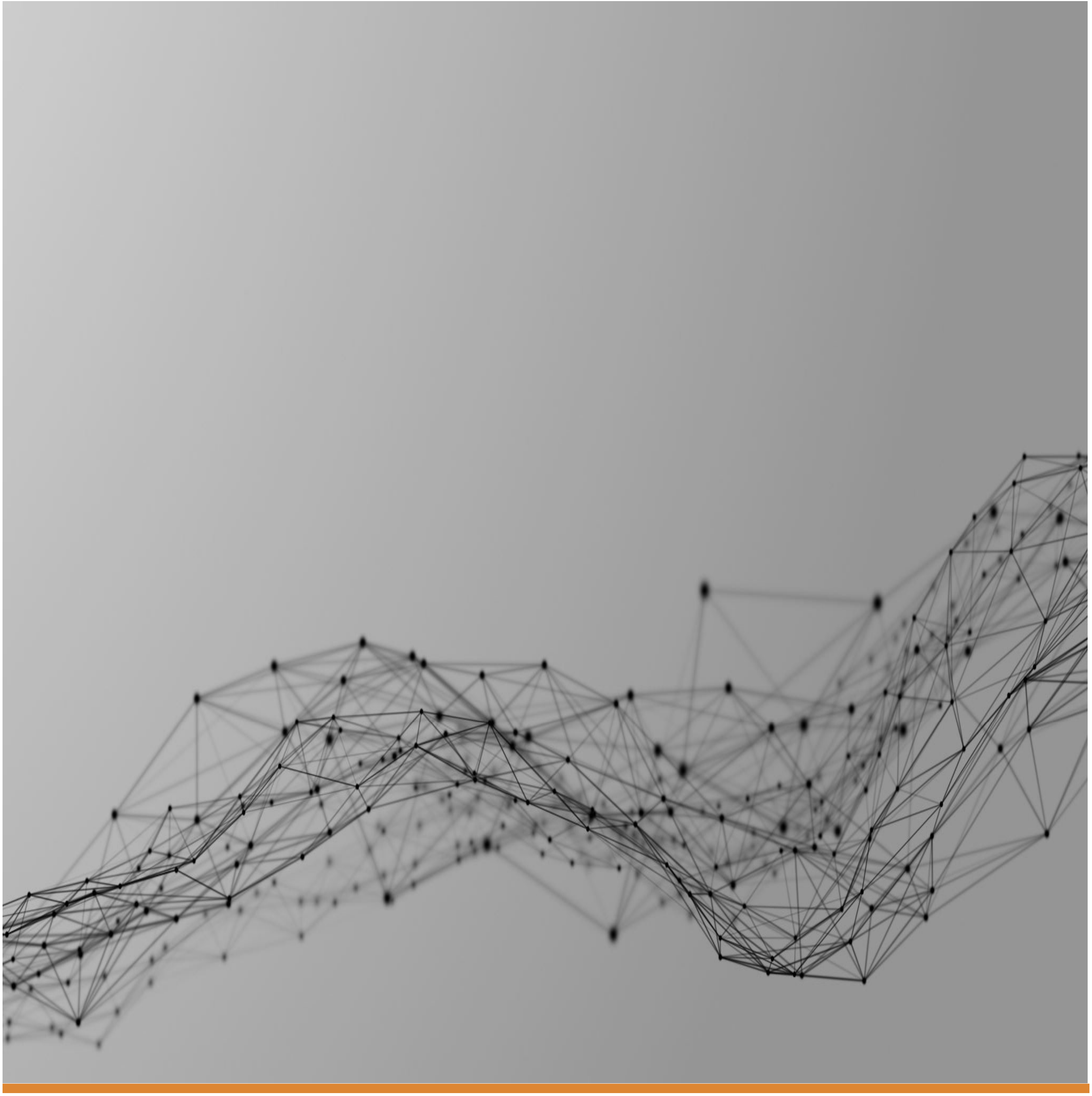

INFORMATION SECURITY

Requirements for Suppliers

2025 - MAY

Coor Group Chief Information Security Officer & Coor Group Head of IT Security

Table of Contents

Changes

VERSION	SECTION	DESCRIPTION
JUNE 2023	Section 2	Removed (scope)
	All section	Minor wording / editing for correctness
	Section 2 & 7	24h changed to 72h
	Section 9	Updated requirements regarding encryption
	Section 6	Updated requirements regarding sub-supplier risk assessment
	Section 11	New /updated requirements regarding information security in development/procurement. Updated requirement regarding use of test data.
MAY 2025	All sections	Minor wording / editing for correctness
	Section 2.4 and 7.2	Incident reporting changed to “relevant” from “any incident”
	Section 3	Clearer reference to frameworks and standards
	Sections 9.4 and 9.5	Updates to requirements (clarity)

1. DESCRIPTION

The Supplier shall maintain technical, physical, and governing processes to ensure the confidentiality, integrity, and availability of Coor's information and, in cases where the Supplier acts as a sub-supplier to one of Coor's customers, the End Customer's information. The Supplier shall also ensure the delivery of agreed services. The minimum level of safeguards required are stated in this document.

2. THE SUPPLIERS OVERALL RESPONSIBILITY

The Supplier:

2.1 is fully responsible for the Supplier Personnel's compliance with this document and shall implement the control measures required before delivery.

2.2 shall guarantee that any processing of Coor's and/or End Customer's Information will be compliant with this document and GDPR regulation.

2.3 shall on request inform Coor on how the Supplier complies with this document's requirements.

2.4 shall notify Coor of any relevant security incident (including but not limited to incidents regarding Personal Data) as soon as possible but no later than within 72 hours after an identified security incident.

2.5 shall on termination of the Agreement securely delete any Coor and/or End Customer's Information and the copies thereof as determined by Coor. The Supplier shall confirm in writing to Coor that the Supplier has met this requirement on termination of the Agreement or at the request of Coor.

2.6 shall not allow any access to Coor's and/or End Customer's Information (it may also concern new, extended, updated, prolonged or in any other way changed real-time network access) in breach of the Agreement to any party without prior written approval by Coor.

3. COMPLIANCE

In addition to the security requirements outlined in this document, the Supplier shall manage information security in alignment with the principles of ISO/IEC 27001:2022 or other recognized international control frameworks of equivalent scope and rigor. The supplier must be able to fulfil the requirements as part of the supply chain for NIS2-regulated entities/sectors.

The Supplier may use ISO/IEC 27001 certification, SOC 2 Type II or ISAE assurance reports to demonstrate compliance with Coor's cybersecurity requirements.

On request, the Supplier shall provide Coor with a compliance status report regarding these requirements without any undue delay.

Any findings showing deviations from the applicable requirements according to the Agreement shall be noted in writing and the Parties shall agree upon an action plan with an appropriate time schedule in relation to the severity in the deviation.

Coor reserves the right to audit the Supplier's compliance with the requirements specified in this document, including the Supplier's oversight of subcontractor compliance.

4. SECURITY GOVERNANCE MEASURES

4.1 SECURITY RISK MANAGEMENT

The Supplier shall identify and evaluate security risks related to confidentiality, integrity, and availability of information and implement appropriate technical and organizational measures to ensure a security level appropriate to the risk. [4.1.0]

The Supplier shall:

4.1.1 ensure confidentiality, integrity, availability, and resilience of processing systems and services.

4.1.2 be able to restore the availability and access to Coor’s and/or End Customer’s Information promptly in the event of a physical or technical incident.

4.1.3 have documented processes and routines for handling risks within its operations and processing Personal Data on behalf of Coor and/or End Customer

4.1.4 periodically assess the risks related to information systems and processing, storing, and transmitting information

4.1.5 Comply with GDPR when personal data is processed according to agreed Data Processing Agreement (DPA)

4.2 INFORMATION SECURITY POLICIES

The Supplier shall have management-approved, documented routines for managing information security, including an information security policy and procedures. They shall be published and communicated to the Suppliers Personnel. [4.2.1]

The Supplier shall periodically review and update security policies and procedures to ensure compliance with this document. [4.2.2]

4.3 ORGANIZATION OF INFORMATION SECURITY

The Supplier shall have defined and documented security roles and responsibilities within its organization. The Supplier shall appoint at least one person with appropriate security competence and overall responsibility for implementing the security measures under these requirements.

5. HUMAN RESOURCE SECURITY

The Supplier shall ensure:

5.1 that information is handled in accordance with the level of confidentiality required under the Agreement.

5.2 that relevant Supplier Personnel is aware of the approved use of information, facilities, and systems under the Agreement.

5.3 that Supplier Personnel with security responsibilities are adequately trained to carry out security-related duties.

5.4 The Supplier shall provide or ensure periodic security awareness training to relevant Supplier Personnel. Such Supplier training shall include, without limitation:

- How to handle customer information security (i.e., the protection of confidentiality, integrity, and availability of information)
- Why information security is needed to protect customers' information and systems.
- The common types of security threats (such as identity theft, malware, hacking, information leakage, and insider threat)
- The importance of complying with information security policies and applying associated standards/procedures
- Personal responsibility for information security (such as protecting customer privacy-related information and reporting actual and suspected Security Incidents)

6. SUPPLIER RELATIONSHIP WITH SUB-SUPPLIERS

The Supplier shall perform security risk assessments and reflect these requirements' content in its agreements with sub-suppliers that perform tasks assigned under the Agreement. [6.1]

The Supplier shall regularly monitor, review, and audit sub-supplier compliance with these requirements. [6.2]

The Supplier shall, at the request of Coor, provide Coor with evidence regarding the sub-supplier's compliance with the requirements. [6.3]

7. SECURITY INCIDENT MANAGEMENT

The Supplier shall have established procedures for Security Incident management that includes routines for; [7.1]

- Preparation- incident response planning
- Identification- process to evaluate type of incident.
- Containment- contain and isolate the breach.
- Eradication- find and eliminate the root cause.
- Recovery- process of restoring and returning affected systems.

The Supplier shall inform Coor at it.support@coor.com about any relevant Security Incident (including but not limited to incidents concerning the processing of Personal Data) as soon as possible but no later than within 72 hours after the Security Incident has been identified. [7.2]

All reporting of security-related incidents shall be treated as confidential information and be encrypted. [7.3]

The security incident report shall contain at least the following information: [8.4]

- Notwithstanding the requirement for immediate notification, the Supplier shall produce a written preliminary report to Coor of any security incident that could affect Coor or Coor's assets in any imaginable way.
- Sequence of events, including actions taken during the incident handling
- Affected portions of the infrastructure, systems, and information
- Estimated (or, upon a high level of uncertainty, worst-case) consequences/impact.
- Consequence reducing measures already implemented.
- Risk-reducing measures already implemented.
- Consequence reducing measures to be implemented, including implementation plan (date; responsible; dependencies)
- Risk reducing measures to be implemented, including implementation plan (date; responsible; dependencies)
- Experience's summary

The Supplier shall provide Coor with support in case of a cyber-forensic investigation. [7.4] When supplier has the responsibility for hosting and infrastructure maintenance the Supplier shall have forensic support capabilities (own capabilities or contracted). In case of a cyber incident that impacts Coor, or Coor's customer information and supplier have no forensic support, Coor has the right to involve Coor's IT cyber-forensic partner(s). If the supplier is responsible for the incident the cost is financed by the Supplier. [7.5]

8. BUSINESS CONTINUITY MANAGEMENT

The Supplier must ensure that business continuity planning is part of Supplier’s general information security management

The Supplier shall ensure:

8.1 The Supplier shall identify business continuity risks and take the necessary actions to control and mitigate such risks.

8.2 The Supplier shall have documented processes and routines for handling business continuity. The Supplier shall ensure that information security is embedded into the business continuity plans.

8.3 The Supplier shall periodically assess the efficiency of its business continuity management, and compliance with availability requirements (if any).

9. TECHNICAL SAFEGUARDS

The following sections applies when the Supplier is managing information for Coor or Coor’s customers or the Supplier handle information that is critical for the delivery of the service from devices or systems not controlled by Coor.

9.1 ASSET MANAGEMENT

9.1.1 The Supplier shall have a defined and documented asset management system in place and maintain up-to-date records of all relevant assets and their owners. Information assets include but are not limited to IT systems, backup or removable media containing Coor’s information, access rights, software, and configuration.

9.1.2 The Supplier shall label, treat, and protect information according to a pre-defined information classification system in accordance with valid security standards at that time (including removable media storage, disposal, and physical transfer).

9.1.3 The Supplier shall implement measures to ensure protection against accidental, unauthorized, or unlawful loss, destruction, alteration, or damage to Coor information transmitted, stored, or otherwise processed.

9.2 AUTHENTICATION

Suppliers implement suitable measures to prevent their information processing systems from being used by unauthorized users, including but not limited to:

9.2.1 The supplier shall have a formal and documented user registration and de-registration process implemented to enable correct access rights assignment.

9.2.2 The Supplier shall ensure that the Supplier Personnel has a personal and unique identifier (user-ID), and use an appropriate authentication technique, which confirms and ensures the identity of users.

9.2.3 The Supplier shall have an implemented and documented password policy based on best practices with strong passwords.

9.2.4 Authorization for privileged access is secured with MFA and has preferably time-based access rules enforced with PIM or PAM techniques.

9.2.5 The number of privilege accounts must only be kept to a minimum to maintain the service.

9.2.6 The Supplier shall use strong authentication (multi-factor) for remote access users and users connecting from untrusted networks.

9.2.7 Automatic temporary lock-out of the user-ID when several erroneous passwords are entered, log file of events, monitoring of break-in-attempts.

9.3 ACCESS CONTROL

Supplier commits that the users entitled to use their information processing system are only able to access the information within the scope and to the extent covered by their respective access permission (authorization) and that Coor's information cannot be read, copied, or modified or removed without authorization. This is accomplished by various measures including, but not limited to:

9.3.1 Employee policies and training in respect of each employee's access rights to personal data.

9.3.2 Annual control and review for authorization and access to critical systems.

9.3.3 Adoption of suitable measures to register system administrators access logs to the infrastructure and keep them secure, accurate and unmodified for at least six months.

9.3.4 Regular audits of system administrators' activity to assess compliance with assigned tasks.

9.3.5 Keeping an updated list with system administrators' identification details (e.g., name, surname, function, or organizational area) and tasks assigned and providing it promptly to Coor upon request.

9.3.6 Use of adequate and-up-to-date encryption technologies for data in rest and transit.

9.4 OPERATIONS SECURITY

The Supplier shall:

9.4.1 have an established change management process to make changes to business processes, Information Processing Facilities, and systems. The management system shall include tests and reviews before changes are implemented, such as procedures to handle urgent changes, rollback procedures to recover from failed changes, logs that show what has been changed, when and by whom.

9.4.2 implement malware protection and remediation routines to ensure that any software used for Supplier's provision of the Services to Coor is protected from malware.

9.4.3 ensure that all information is backed up and regularly tested to ensure that it can be restored. Backups are encrypted and separated from information storage in different geolocations.

9.4.4 log and monitor all relevant activities, including the creation, reading, copying, modification, and deletion of processed information, as well as exceptions, faults, and information security events. These logs shall be regularly reviewed. The Supplier shall protect and retain log data for a minimum of six (6) months and, upon request, provide monitoring data to Coor. Any anomalies, incidents, or indicators of compromise that may impact Coor must be reported in accordance with the security incident management requirements.

9.4.5 manage threats and vulnerabilities associated with business applications, systems, and networks by scanning for technical vulnerabilities, maintaining up-to-date patch levels, acting on threat intelligence, and protecting information against targeted cyber-attacks.

9.4.6 establish security baselines (hardening) for all relevant technologies such as operating systems, databases, applications.

9.4.7 ensure that the development, test, and production environments are separated and maintained from each other.

9.4.8 ensure that development environments are logically separated from production on network level.

9.5 NETWORK SECURITY

The Supplier shall:

9.5.1 manage and control networks to ensure the protection of information within systems and applications.
9.5.2 Segregate groups of information services, users, and information systems within networks to prevent unauthorized access and enhance security.
9.5.3 Ensure that any communication classified as confidential or strictly confidential—as defined below—or subject to specific Coor requirements, is transmitted securely with encryption.

10. PHYSICAL AND ENVIRONMENTAL SECURITY

10.1 FACILITIES

The Supplier shall protect Information Processing Facilities against external and environmental threats and hazards, including power/cabling failures and other disruptions caused by failures in supporting utilities. This includes physical perimeter and access protection. [10.1.1]
Only authorized users shall have access to facilities processing information. [10.1.2]

10.2 ENDPOINT DEVICES

The Supplier shall:

10.2.1 enforce automatic temporary lock-out of user device if left idle, identification, and password required to reopen.
10.2.2 ensure that laptops and mobile devices shall be hard drives encrypted if Coor’s information is stored on the device.
10.2.3 laptops and PCs have automatic patch updates and antivirus installed.
10.2.4 have a mobile device management system if Coor’s information is stored on the mobile device.

11. SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

The Supplier shall:

11.1 define information security requirements for all information systems, whether acquired or developed.

11.2 implement rules and routines for the development of the lifecycle of software and systems, including change and review procedures.

11.3 test security functionality during development in a controlled environment separated from production.

11.4 ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities.

11.5 use up-to-date and trusted third-party components for the software developed by the organization.

11.6 perform regular penetration and vulnerability testing to identify security weaknesses.

11.7 show that security by design is an inherent part of the development process.

11.8 show that privacy by design is an inherent part of the development process.

11.9 show that security and setup experience and best practice knowledge on all platforms supported by the supplier.

11.10 Web application development shall at least be tested in accordance with OWASP top10 (The Open Web Application Security Project).

11.11 Coor information or Coor customer information shall not be used in development and test environments.

This section applies when the Supplier develop, deliver, and maintain software and system for Coor or Coor's customers.

12. DEFINITIONS

Coor’s Information	data or other information that Coor, or a person acting on behalf of Coor, makes available to the Supplier, including but not limited to Personal Data, and the result of Supplier’s processing of such information. Coor’s information can also include Coor’s customers’ information.
Data breach	a security incident that results in a confirmed disclosure of information to an unauthorized party
Data Subject	an identified or identifiable living natural person to which Personal Data relates
Information Processing Facilities	any information processing system, services, or infrastructure, including the physical locations housing them
Log	to record details of information or events in an organized record-keeping system, usually sequenced in the order in which the information or events occurred.
Personal Data	any information relating to an identified or identifiable natural person (i.e., a Data Subject- see above). A person can be identified by either their name, ID number, location, an online identifier, or even aspects of their physical, physiological, genetic, mental, economic, cultural, or social identity.
Services	the services to be provided by the Supplier to Coor, or by a person acting on behalf of the Supplier as further defined in the Agreement between the parties.
Supplier	the counterparty who supplies any deliverables to Coor and which is identified as “Supplier,” “Vendor, “Partner,” or the equivalent in the relevant Agreement.
Supplier Personnel	any person working on behalf of the Supplier, such as employees, consultants, contractors, and sub-suppliers.
Security Control	a technical countermeasure, an organizational setup, or a process that helps to maintain IT systems security-quality properties.
Security Incident	a single or a series of unwanted or unexpected security events that have a significant probability of compromising the confidentiality, integrity, or availability of an information asset,
Sensitive Products/Services	any product or Services defined as sensitive by Coor. Sensitive Products or Sensitive Services shall be documented in the applicable Agreement.
Pseudonymization	the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person