INFORMATION SECURITY

Requirements for Suppliers

MAY 2022

Table of Contents

Changes Sep 2021 - May 2022

SECTION	DESCRIPTION
All sections	Added table of contents and numbering of sections for reference
3 and 5	GDPR reference to DPO clarified
8	Security Incident Management detailed
8.5	(new) Cyber forensic responsibility clarified
10	Technical Safeguards – requirement specific to GDPR removed (managed in DPA)
10.4	Updated wording
10.4.8	(New) Network segmentation in development environments
12	Add 12.6 (security by design), 12.7 (privacy by design) and 12.8 (best practise knowledge)

1. DESCRIPTION

The Supplier shall maintain technical, physical, and governing processes to ensure confidentiality, integrity, availability of Coors and/or (in case where Supplier is a sub-supplier to one of Coor's customer "End Customer") End Customer's data and ensure delivery of agreed services.

The minimum level of safeguards required are stated in this document. However, the Supplier shall actively ask Coor for possible additional requirements regarding safeguards of sensitive information and critical business processes if the Supplier has not received such requirements.

Certification in accordance with ISO-27001 and security controls implemented from frameworks as CIS-20, NIST, etc., is strongly advised.

2. SCOPE

This document applies when one or more of the following conditions apply:

The supplier will:

- Access and or process Coor's and/or End Customer's information,
- Access Coor's and/or End Customer's IT infrastructure, equipment, and systems (on location/remote), or
- Deliver sensitive services/products as identified by Coor in a relevant agreement

3. THE SUPPLIERS OVERALL RESPONSIBILITY

The Supplier:

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

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

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

3.4 shall notify Coor of any Security Incident (including but not limited to incidents regarding Personal Data) as soon as possible but no later than within 24 hours after an identified Security Incident

3.5 shall return or destroy any Coor's and/or End Customer's Data 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.

3.6 shall not allow any access to Coor's and/or End Customer's Data (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.

4. COMPLIANCE

On request, the Supplier shall provide Coor with a compliance status report with regards to these requirements without any unjustified delay.

Any findings showing deviations from the applicable requirements according 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 has the right to audit how the Supplier and its sub-suppliers fulfil the requirements.

5. SECURITY GOVERNANCE MEASURES

5.1 SECURITY RISK MANAGEMENT

The Supplier shall identify and evaluate security risks related to confidentiality, integrity, and availability and implement appropriate technical and organizational measures to ensure a security level appropriate to the risk. [5.1.0]

The Supplier shall:

5.1.1 can ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services

5.1.2 be able to restore the availability and access to Coor's and/or End Customer's Data promptly in the event of a physical or technical incident

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

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

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

5.2 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. [5.2.1]

The Supplier shall periodically review and update security policies and procedures to ensure compliance with this document. [5.2.2]

5.3 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.

6. HUMAN RESOURCE SECURITY

The Supplier shall ensure:

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

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

6.3 that Supplier Personnel with security responsibilities is adequately trained to carry out security-related duties.

6.4 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 the 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)

Coor has the right to request a signed receipt from Supplier Personnel stating that he or she has understood and will comply with the Security Requirements and the approved use of information, systems, and facilities. [6.10]

7. SUPPLIER RELATIONSHIP WITH SUB-SUPPLIERS

The Supplier shall reflect these requirements' content in its agreements with sub-suppliers that perform tasks assigned under the Agreement. The Supplier shall regularly monitor, review, and audit sub-supplier compliance with these requirements. [7.1]

The Supplier shall, at the request of Coor, provide Coor with evidence regarding sub-supplier's compliance with the requirements. [7.2]

8. SECURITY INCIDENT MANAGEMENT

The Supplier shall have established procedures for Security Incident management that includes routines for; [8.1]

- 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 Security Incident (including but not limited to incidents concerning the processing of Personal Data) as soon as possible but no later than within 24 hours after the Security Incident has been identified. [8.2]

All reporting of security-related incidents shall be treated as confidential information and be encrypted. [8.3]

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

- Notwithstanding the requirement for immediate notification, the Supplier shall comprise 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. [8.4] When supplier have 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 Coors customer data and supplier have no forensic support, Coor has the right to involve Coors IT cyber-forensic partner(s). If supplier is responsible for the incident the cost is financed by the Supplier. [8.5]

9. BUSINESS CONTINUITY MANAGEMENT

The Supplier shall ensure:

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

9.2 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

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

10. TECHNICAL SAFEGUARDS

The following sections applies when the Supplier is managing information for Coor or Coors customers or the Supplier handle information that is critical for the delivery of the service from devices or

10.1 ASSET MANAGEMENT

10.1.1 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 data, access rights, software, and configuration.

10.1.2 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).

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

10.2 AUTHENTICATION

Supplier implements suitable measures to prevent their data processing systems from being used by unauthorized persons, including but not limited to:

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

10.2.2 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

10.2.3 Supplier shall have an implemented and documented password policy that require renewal at least every four months. User passwords shall at least be nine characters long.

10.2.4 Authorization for privilege access is secured with MFA and has preferably timed-based access rules enforced.

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

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

10.2.7 Automatic temporary lock-out of the user-ID when several erroneous passwords are entered, log file of events, monitoring of break-in-attempts (alerts)

10.3 ACCESS CONTROL

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

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

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

10.3.3 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.

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

10.3.5 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.

10.3.6 Use of adequate encryption technologies for data in rest or transit.

10.4 OPERATIONS SECURITY

The Supplier shall:

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

10.4.2 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

10.4.3 backup all information and regular test back-up copies to ensure that the information can be restored as agreed with Coor. Backup are separated from information storage in different geolocations.

10.4.4 log and monitor activities, such as create, reading, copying, amendment and deletion of processed data, as well as exceptions, faults and information security events and regularly review these. Furthermore, the Supplier shall protect and store (for at least 6 months) Log information, and on request, deliver monitoring data to Coor. Anomalies / incidents / indicators of compromise that has impact to Coor shall be reported according to the security incident management requirements.

10.4.5 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.

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

10.4.7 ensure that the development, test, and production environments is segregated and maintained from each other.

10.4.8 ensure that development environments are logically segregated from production on network level.

10.5 COMMUNICATION SECURITY

The Supplier shall:

10.5.1 Networks shall be managed and controlled to protect information in systems and applications.
10.5.2 Groups of information services, users and information systems shall be segregated on networks.
10.5.3 The Supplier shall ensure that communication classified, as confidential and strictly confidential (as further detailed below) or by specific requirements by Coor, is secure which means that un-encrypted communication may not be used.

11. PHYSICAL AND ENVIRONMENTAL SECURITY

11.1 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. [11.1.1]
Only authorized users shall have access to facilities processing information. [11.1.2]

11.2 PC'S AND DEVICES

The Supplier shall:

11.2.1 Automatic temporary lock-out of user device if left idle, identification, and password required to reopen.
11.2.2 Laptops and mobile devices shall be hard drives encrypted if Coor's information is stored on the device.
11.2.3 Laptops and PCs shall have automatic patch updates and antivirus installed.
11.2.4 Supplier shall have a mobile device management system if Coor's data is stored on the mobile device.

12. SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

The Supplier shall:

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

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

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

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

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

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

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

12.8 show that security and setup experience and best practice knowledge on all platform supported by the supplier

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

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

13. DEFINITIONS

Coor's Data	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 data. Coors data can also include Coor's customers' data.
Data breach	a security incident that results in a confirmed disclosure of data 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 counter-party 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