

## Fazer Information Security Requirements for Suppliers

<b>1. General</b>
<p>The Supplier and/or Affiliate(s) (incl. their subcontractors, if any) shall manage or otherwise process information (hereinafter the Information) in connection with fulfilment of the Agreement between the Supplier and Oy Karl Fazer Ab and/or its Affiliate(s) (hereinafter Fazer).</p> <p>This document contains Fazer's high-level information security requirements. The Supplier shall comply with the requirements set forth herein in order to secure that the Information is protected on an adequate level when managing or otherwise processing the Information under the Agreement.</p> <p>This document is not an exhaustive description of the applicable information security requirements. The Supplier shall therefore, without additional compensation, take any other measures required to maintain at least good industry practise level for security of the Information.</p>
<b>2. Scope</b>
<p>These information security requirements apply to the Information (including but not limited to project, service, delivery and product related information as well as personal data) that is managed or otherwise processed by the Supplier under the Agreement.</p> <p>The Supplier is fully responsible for its subcontractors complying with the same requirements as set out in this document.</p>
<b>3. Information Security Policy</b>
<p>The Supplier must have an internal information security policy to which the top management has committed and that is implemented across the Supplier's organisation. The policy shall cover relevant areas of common standards and standards relevant in each case (such as ISO27001, SOC2, NIST CSF). The Supplier shall regularly assess and revise the policy.</p>
<b>4. Information Security Organization</b>
<p>The security responsibilities within the Supplier's organization shall be assigned by senior management to nominated individuals. The responsibilities shall include (but are not limited to) overall security, risk management, privacy, and controls for managing the Information (as defined by the applicable legislation and the Data Protection Terms of the Agreement). The nominated individuals shall be notified to Fazer on request. The Supplier shall have a documented process for reviewing the implementation of security within its organization.</p> <p>Unless agreed otherwise, the Supplier shall report any security and/or privacy related matters for Fazer in connection with the other reporting under the Agreement.</p>
<b>5. Risk Management</b>
<p>The Supplier must have formal ICT related risk management processes in place and be able to demonstrate that the Supplier can identify, assess and mitigate the risks related to the Information. The Supplier shall identify and assess risks on a regular basis and shall use the related results as an input to review and improve information security controls. The Supplier shall, on Fazer's request, submit the latest risk identification and assessment report to Fazer (at least the parts that concern Fazer's information).</p>
<b>6. Information Security Controls</b>
<p>The Supplier shall protect the Information by implementing necessary information security controls (based on e.g. risk identification and assessment analysis and applicable data security standards).</p> <p>The controls shall be in place when the Information is created, in use, at rest, in transit and at disposal. Specific care must be taken to ensure that the Information is also appropriately protected in other environments (such as test and development environments) than in production environment.</p> <p>The controls shall be maintained by the Supplier to ensure compliance with the requirements under the Agreement and the applicable legislation, concerning especially information security and data protection.</p> <p>The Supplier shall regularly assess and evaluate the effectiveness of information security controls for ensuring that the implemented security controls are up to date and relevant in order to secure the information. If requested by Fazer, Information security related topics shall be regularly addressed between Fazer and the Supplier.</p>

The Supplier shall, on Fazer's request, submit a description of the implemented information security controls (e.g. a description of the information security solution and/or processes) or the latest security audit report to Fazer (at least the parts that concern Fazer's information).

#### **7. Personnel Security and Awareness**

The Supplier shall ensure that its individuals (incl. the subcontractors' individuals) are bound by statutory or contractual confidentiality obligations prior to accessing the Information.

The Supplier shall conduct security and privacy awareness training in connection with induction (and refresher sessions at least annually) for all employees participating in fulfilment of the Supplier's obligations under the Agreement. Due emphasis shall be given to client confidentiality, understanding the agreed confidentiality obligations and specifically the sensitivity of personal data.

If the Supplier's individual is working physically at Fazer's premises, the Fazer Group Information Security Policy and Guidelines will apply. In such a case, the Supplier's is responsible for ensuring that the individual signs Personal Confidentiality Undertaking presented by Fazer.

#### **8. Encryption**

If and as applicable, the Supplier shall encrypt the Information managed or processed for fulfilling the Supplier's obligations under the Agreement by using current industry-standard strong encryption, key management and related standards (e.g. AES-256 / SHA-246, TLS1.2 and above or NIST latest recommendations).

#### **9. Physical Security**

Adequate physical security perimeters shall be ensured by the Supplier to prevent unauthorized persons from gaining physical access to premises, buildings, or rooms where the Information is managed.

#### **10. Access Rights Management**

The Supplier shall restrict accesses to systems used to fulfil the Supplier's obligations under the Agreement for authorized individuals whose role requires such access, based on the principle of least privilege.

The Supplier shall provision named user accounts for all authorized individuals of the Supplier. Passwords shall be of sufficient strength, minimally adhering to NIST SP800-63B password guidelines. Multifactor authentication (MFA) shall be required for all user accounts of the Supplier's individuals.

The Supplier shall have a process for requesting, approving, deploying and removing access rights concerning the Information. All such requests and the related approvals shall be logged by the Supplier for audit purposes.

The Supplier should perform a periodic system access review to ensure that the Supplier's personnel maintain appropriate access rights. The Supplier shall disable user accounts and other access rights to the systems used to fulfil the obligations of the Supplier under the Agreement after the termination of such individuals' employment or assignment.

User level accounts provided by Fazer in order to access system(s) in the Fazer corporate network are always personal and cannot be shared within the Supplier's organization. The Supplier shall be responsible for notifying Fazer without undue delay in case an individual does not need the access rights for fulfilling the Supplier's obligations under the agreement.

#### **11. Information Security Reviews**

Unless specifically agreed otherwise in the Agreement, Fazer or a third-party auditor (not a direct competitor of the Supplier) appointed by Fazer, shall be entitled to audit, and inspect that the Supplier's (and its subcontractors', where relevant) level of information security complies with the requirements set out in this document as well as the EU General Data Protection Regulation (GDPR), other applicable data protection laws and the Data Protection Terms between Fazer and the Supplier, if any, or otherwise agreed by the Parties.

In such cases, each Party shall bear their own costs regarding the audit. The primary method of the audit shall be based on interviews and review of relevant documentation provided by the Supplier.

The Supplier shall cooperate to a reasonable extent with the auditors performing the audit to ensure that the auditors are able to form a correct view of the Supplier's aforesaid compliance. The Supplier shall be obliged to correct potential findings at its own cost. Any possible audit carried out by Fazer shall in no way limit the Supplier's liability under the Agreement.

## 12. Security Incident Management

The Supplier shall have adequate and documented incident management procedures and nominated persons to timely react and prevent any further damage caused by security, privacy or any other compliance issues, vulnerabilities, or incidents. The Supplier shall at all times maintain the capability to prevent, monitor, detect, investigate, and respond to security and privacy incidents.

The Supplier shall inform Fazer without delay in case of any Fazer related security incidents to Fazer's appointed contact person and/or contact point. The Supplier shall ensure the ability to restore the availability and access to the Information in a timely manner in the event of an information security incident.

In case of a major data breach incident, the Supplier shall inform Fazer without undue delay to [databreach@fazer.com](mailto:databreach@fazer.com) and Fazer's appointed contact person and/or contact point.

## 13. Business Continuity

The Supplier shall have business continuity and disaster recovery plans documented and implemented for minimizing the impact of a realized risk event (e.g. natural disasters, accidents, equipment failures, cyber attacks or sabotage) on the Supplier's and subcontractors' organizations, as needed for fulfilling the obligations of the Supplier under the Agreement.

The Supplier shall demonstrate the functioning of the aforesaid plans by conducting regular tests and exercises. At Fazer's request, the Supplier shall provide reports on the tests and exercises it has undertaken to verify its ability to recover from a realized risk event (at least for the parts that concern the obligations of the Supplier under the Agreement).

The Supplier shall facilitate the recovery of information assets through a combination of preventive and recovery controls. Said controls shall be in accordance with applicable statutory, regulatory, and legal requirements and consistent with industry standards and best practices.

The Supplier shall enforce a documented backup policy that supports the Supplier in ensuring the capability to fulfil the obligations under the Agreement and continuity requirements during emergency situations. The backups shall be stored in a secure storage. Actual restoration of the backups must be tested by the Supplier regularly to ensure their usability.

## 14. Secure Software Development

The Supplier shall ensure that the Software used or delivered under the Agreement, if any, have been developed in accordance with principles of secure software development consistent with industry best practices, including, security design review, secure coding practices, risk-based testing and remediation requirements.

The Supplier shall have a process to ensure the systems used in the software development environment(s) are properly and timely patched.

The Supplier shall maintain a software bill of materials (SBOM) of all the open source and third-party components used to identify and mitigate risks associated with open source and third-party components.

## 15. Patch and Vulnerability Management

The Supplier shall maintain a standard maintenance window to apply patches and other fixes for systems used to fulfil the Supplier's obligations under the Agreement. If a critical update is necessary for security purposes, the Supplier shall notify Fazer and take action to perform the updates as soon as possible irrespective of the standard maintenance windows.

The Supplier must develop and maintain an up-to-date cybersecurity vulnerability management plan for systems used to fulfil the Supplier's obligations under the agreement. Such plan shall aim at promptly identifying, preventing, investigating and mitigating any cybersecurity vulnerabilities and performing any required recovery actions to remedy the impact.

The Supplier shall notify Fazer within a reasonable period, in no event exceeding five (5) business days after discovery, or shorter if required by applicable law or regulation, of any high/critical vulnerabilities detected in connection with the delivery under the Agreement. Within a reasonable time thereafter, the Supplier shall take the necessary reasonably available actions (such as security patching) at no extra charge, necessary to remediate the aforesaid cybersecurity vulnerability.