Schedule Information Security Requirements

Version C

1 Introduction to Security Requirements

The purpose of this security schedule is to outline minimum Security Requirements applicable to the Vendor in connection with the delivery of services or products ("Deliverables") to Carlsberg. Carlsberg places great emphasis on the security and reliability of the supplied products and services. The Vendor is therefore obliged to take the reasonably required measures to protect the data and property of Carlsberg against unauthorized access, theft or damage which could compromise the confidentiality, integrity, availability of Carlsberg Data and Assets. It is the responsibility of the Vendor to ensure that compliance with all requirements stated in this schedule extends to Subcontractors who the Vendor may enter into agreement with or is affiliated with.

1.1 The Vendor's Compliance with Security Requirements

The Vendor is responsible for ensuring full compliance with the requirements set forth in the security schedule. If the Vendor identifies any non-compliance with the requirements herein, it shall, without undue delay, implement all necessary and proportionate corrective actions to restore compliance.

1.2 The Vendor's Notification of Inconsistency

The Vendor shall promptly notify Carlsberg of any conflicts or inconsistencies between the requirements, standards, or referenced documents in this security schedule. Carlsberg shall determine the appropriate resolution, and the Vendor shall comply accordingly.

1.3 Regulatory Requirements

The Vendor shall proactively address threats with immediate relevance to the Deliverables and/or Carlsberg Data, or Assets and comply with information Security Requirements and requirements concerning privacy protection and protection of Personal Data in accordance with Applicable Laws, regulations and governmental authority orders. Any identified non-compliance with such requirements shall be documented and addressed.

2 Point of contact

The Vendor shall designate one point of contact for Carlsberg regarding all matters related to information security and privacy in connection with the fulfilment of the Deliverables. This contact shall serve as the major liaison with Carlsberg on security-related issues and be available to respond to inquiries, incidents and coordination requests as needed.

3 Requirements

3.1 Security Governance and Risk Management

Vendor shall establish appropriate security governance with clear roles and responsibilities for information security, maintain an information security policy and appropriate documentation on Security Controls. Vendor shall, based on regular documented risk assessments, implement and maintain reasonable and proportionate administrative, technical and physical Security Controls, aligned to recognised industry practice, appropriate to the Services and the sensitivity of Carlsberg Data.

3.2 Data Use and Confidentiality

Vendor shall use Carlsberg Data only to perform the services, keep it confidential, and protect it from unauthorised access, disclosure, alteration or loss.

3.3 Access Control

Vendor shall maintain identity and access management procedures, restrict access to Carlsberg Data and (if applicable) Carlsberg systems to authorised personnel on a need-to-know and least-privilege basis, promptly remove access for leavers, and use multi-factor authentication for any access to systems that store or access Carlsberg Data or to Carlsberg systems.

3.4 Asset Management

Vendor shall maintain an inventory of, and assign ownership for, all Assets used to provide the Deliverables or that Process Carlsberg Data or connect to Carlsberg systems. Vendor shall keep Assets securely configured and current (including timely patching and anti-malware as appropriate).

3.5 Data Handling

Vendor shall transmit Carlsberg Data securely and, where Vendor stores/hosts Carlsberg Data, appropriately protect it at rest. Upon Carlsberg's request or upon termination, Vendor shall promptly return or securely delete Carlsberg Data.

3.6 Third Party Risk Management

Vendor shall ensure that any subcontractor that accesses Carlsberg Data or Carlsberg systems is screened for their security risk and is bound by written security obligations no less protective than this clause

3.7 Incident Management

Vendor shall maintain incident management procedures and notify Carlsberg without undue delay (and in any event within 24 hours) after becoming aware of any actual or suspected Information Security Incident affecting Carlsberg Data or the Deliverables. Vendor shall cooperate in investigation and remediation and preserve relevant evidence. Notification shall take place to the engagement owner and Carlsberg incident response team at ThirdPartyIncidentNotification@carlsberg.com.

3.8 Business Continuity

Vendor shall maintain reasonable and proportionate business continuity arrangements to ensure continuity of the Deliverables and availability of Carlsberg Data. Vendor shall periodically test its business continuity arrangements.

3.9 Assurance

On request (no more than once annually), Vendor shall provide concise evidence of the effectiveness of the security program (e.g., a written assurance attestation, or available certifications).

3.10 Compliance

Vendor shall ensure its employees and subcontractors engaged in the provisioning of Deliverables comply with the Security Requirements and with applicable laws (including data-protection laws) relevant to the Deliverables.

4 Glossary

Term	Definition
Applicable Law	Any supranational, national, or local law, ordinance, regulatory policy (incl. any requirement or notice of any regulatory body), or compulsory guidance of a regulatory body applicable to Carlsberg or its subsidiaries.
Assets	Any device, application, system, server, network component or service, infrastructure, software
Carlsberg Data	Any information, data belonging to or provided by Carlsberg
Deliverables	The specific outputs, tasks, or functions the Vendor is obligated to provide under the Agreement, including both tangible products and ongoing services.
Information Security Incident	A successful or imminent threat of unauthorized access, use, disclosure, breach, modification, theft, loss, corruption or destruction of information, or interference with information technology operations.
Personal Data	Any information which are related to an identified or identifiable natural person.
Process	Any operation or set of operations that is performed upon information, whether or not by automatic means, such as collection, recording, securing, organising, storing, adapting or altering, access to, retrieval, use, disclosure, erasure or destruction
Security Control	Any administrative, technical, physical, or procedural measure, to prevent, deter, detect, correct, or recover from threats, vulnerabilities, incidents or non-compliance affecting the confidentiality, integrity or availability of information. Control, safeguard, or risk management measure are used as synonyms.
Security Requirements	The set of mandatory controls, standards, and practices designed to protect systems, data, and operations from unauthorized access, disclosure, alteration, or destruction.
Subcontractor	Any third party engaged by the Vendor to perform part of the Services or Deliverables. Subcontractors must comply with all applicable terms of this Schedule.