Schedule Information Security Requirements
Version C

1. The terms used in this Schedule Information Security Requirements shall mean the following:

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.

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.

2. 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 to Carlsberg.

Carlsberg places great emphasis on the security and reliability of the supplied products/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.

2.1. 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.

Угода про вимоги з інформаційної безпеки
Версія «С»

1. Терміни, що використовуються в цій Угоді, означають наступне:

Застосовне законодавство - будь-яке наднаціональне, національне або місцеве законодавство, нормативно-правовий акт, регуляторна політика (включаючи будь-які вимоги чи повідомлення будь-якого контролюючого органу) або обов'язкові до виконання вказівки контролюючого органу, що застосовуються до **Carlsberg***.

Активи - будь-який пристрій, програма, система, сервер, мережевий компонент або послуга, інфраструктура, програмне забезпечення.

Дані Carlsberg - будь-яка інформація, дані, що належать або надаються Carlsberg

Результати – конкретні результати, завдання або функції, які **Постачальник**** зобов'язаний надати згідно з Договором, включаючи як товар, так і роботи/послуги.

Інцидент інформаційної безпеки - реальна або гіпотетична загроза несанкціонованого доступу, використання, розкриття, порушення безпеки, зміни, викрадення, втрати, пошкодження або знищення інформації, а також втручання в роботу інформаційних технологій.

Персональні дані - будь-які відомості або дані про фізичну особу, яку ідентифіковано, або може бути ідентифіковано за цими даними.

Обробка - будь-яка операція або сукупність операцій, що здійснюються з інформацією, за допомогою автоматизованих засобів або без них, такі як збирання, реєстрація, захист, систематизація, зберігання, адаптація або зміна, надання доступу, отримання, використання, розкриття, стирання або знищення.

Заходи безпеки - це будь-які організаційні, технічні, фізичні або процедурні дії, спрямовані на запобігання, виявлення та усунення загроз або інцидентів, що можуть вплинути на конфіденційність, цілісність чи доступність інформації.

Вимоги безпеки - набір обов'язкових заходів контролю, стандартів і практик, призначених для захисту систем, даних і операцій від несанкціонованого доступу, розголошення, зміни або знищення.

Субпідрядник - будь-яка третя сторона, залучена Постачальником для поставки товарів/робіт/послуг. Субпідрядники повинні дотримуватися всіх умов цієї Угоди.

2. Вступ до вимог безпеки

Метою цієї Угоди з безпеки є визначення мінімальних вимог безпеки, що застосовуються до Постачальника у зв'язку з наданням послуг або постачанням продуктів для Carlsberg.

Carlsberg приділяє значну увагу безпеці та надійності поставлених товарів/робіт/послуг. У зв'язку з цим Постачальник зобов'язаний вживати обґрунтовано необхідних заходів для захисту даних і майна Carlsberg від несанкціонованого доступу, крадіжки або пошкодження, які можуть поставити під загрозу конфіденційність, цілісність та доступність даних і активів Carlsberg. Постачальник несе відповідальність за забезпечення дотримання всіх вимог цієї Угоди також субпідрядниками, з якими він укладає договори або з якими пов'язаний.

2.1. Дотримання Постачальником вимог безпеки.

Постачальник відповідає за повне дотримання вимог, викладених у цій Угоді з безпеки.

Якщо Постачальник виявляє будь-які випадки невідповідності цим вимогам, він зобов'язаний, без невиправданої затримки, вжити всіх доцільних та достатніх коригувальних заходів для відновлення відповідності.

2.2.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.

2.3. 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.

3. 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.

4. Requirements

4.1 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.

4.2. 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.

4.3. 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.

4.4. 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).

2.2. Повідомлення про невідповідності.

Постачальник повинен своєчасно повідомляти Carlsberg про будь-які суперечності або невідповідності між вимогами, стандартами чи документами, на які є посилання в цій Угоді з безпеки. Carlsberg визначає належний спосіб їх вирішення, а Постачальник зобов'язаний діяти відповідно до нього.

2.3. Регуляторні вимоги.

Постачальник повинен проактивно реагувати на загрози, що мають безпосереднє відношення до поставки товарів/робіт/послуг та/або даних чи активів Carlsberg, а також дотримуватись вимог інформаційної безпеки, вимог щодо захисту конфіденційності та персональних даних відповідно до Застосовного законодавства, нормативно-правових актів і розпоряджень державних органів. Будь-які виявлені випадки невідповідності таким вимогам мають бути задокументовані та усунені.

3. Контактна особа

Постачальник призначає одну контактну особу для взаємодії з Carlsberg з усіх питань, пов'язаних з інформаційною безпекою та захистом конфіденційності у зв'язку з поставкою товарів/робіт/послуг.

Ця особа є контактною особою з питань безпеки та повинна бути доступною для реагування на запити, інциденти і координації дій, у разі потреби.

4. Вимоги

4.1 Управління безпекою та ризиками.

Постачальник повинен впровадити належну систему управління інформаційною безпекою з чітким розподілом ролей і відповідальності, затвердити політику інформаційної безпеки та вести відповідну документацію щодо Заходів безпеки.

Постачальник зобов'язаний на основі регулярних задокументованих оцінок ризиків впроваджувати та підтримувати доцільні та достатні адміністративні, технічні та фізичні Заходи безпеки, які відповідають визнаній галузевій практиці та є належними для Послуг і рівня конфіденційності Даних Carlsberg.

4.2. Використання даних і конфіденційність.

Постачальник зобов'язаний використовувати Дані Carlsberg виключно з метою надання послуг, зберігати їх у таємниці (забезпечувати їхню конфіденційність) та захищати їх від несанкціонованого доступу, розкриття, зміни або втрати.

4.3. Контроль доступу

Постачальник зобов'язаний підтримувати процедури управління ідентифікацією та доступом, обмежувати доступ до Даних Carlsberg та (за наявності) систем Carlsberg, лише для уповноважених осіб, за принципами «виробничої необхідності» та «мінімально необхідних прав доступу», своєчасно припиняти доступ для уповноважених осіб, які припинили роботу/звільнені, а також використовувати багатофакторну автентифікацію для будь-якого доступу до систем, що зберігають Дані Carlsberg чи здійснюють доступ до них, або безпосередньо до систем Carlsberg.

4.4. Управління активами.

Постачальник веде облік та призначає відповідальних осіб за Активи, що використовуються для поставки товарів/робіт/послуг або обробки даних Carlsberg чи підключення до систем Carlsberg. Постачальник зобов'язаний підтримувати Активи безпечно налаштованими та в актуальному стані (включаючи своєчасне встановлення патчів та використання антивірусного ПЗ, за необхідності).

4.5. 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.

4.6. 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.

4.7. 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 incident response team at:
ThirdPartyIncidentNotification@carlsberg.com

4.8. 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.

4.9. 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).

4.10. 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.

4.5. Обробка даних.

Постачальник зобов'язаний безпечно передавати Дані Carlsberg і, якщо Постачальник зберігає/розміщує Дані Carlsberg, належним чином захищати їх у «стані спокою». На запит Carlsberg або після розірвання договору Постачальник зобов'язаний негайно повернути або безпечно видалити Дані Carlsberg.

4.6. Управління ризиками третіх сторін.

Постачальник повинен забезпечити, щоб будь-які субпідрядники, які мають доступ до Даних або систем Carlsberg, проходили оцінку ризиків безпеки та були зобов'язані виконувати письмові зобов'язання щодо безпеки не менш суворі, ніж передбачено цією Угодою.

4.7. Управління інцидентами.

Постачальник зобов'язаний мати процедури управління інцидентами та повідомляти Carlsberg без невиправданої затримки (і в будь-якому випадку протягом 24 годин) після того, як йому стало відомо про будь-який фактичний або підозрюваний Інцидент інформаційної безпеки, що впливає на Дані Carlsberg або стосується товарів/робіт/послуг, що постачаються.

Постачальник зобов'язаний співпрацювати в розслідуванні та усуненні наслідків, а також зберігати відповідні докази.

Повідомлення надсилається «власнику» контракту (керівнику проекту) та команді реагування на інциденти за адресою: ThirdPartyIncidentNotification@carlsberg.com

4.8. Безперервність бізнесу.

Постачальник зобов'язаний підтримувати доцільні та достатні заходи забезпечення безперервності бізнесу для гарантування безперервності постачання товарів/робіт/послуг та доступності Даних Carlsberg. Постачальник зобов'язаний періодично тестувати свої заходи забезпечення безперервності бізнесу.

4.9. Підтвердження.

На запит (не частіше одного разу на рік) Постачальник зобов'язаний надати стислі докази ефективності програми безпеки (наприклад, письмове підтвердження/атестацію або наявні сертифікати).

4.10. Дотримання вимог.

Постачальник зобов'язаний забезпечити, щоб його працівники та субпідрядники, залучені до поставки товарів/робіт/послуг, дотримувалися Вимог до безпеки та застосовного законодавства (включаючи закони про захист даних), що стосується поставки товарів/робіт/послуг.

Carlsberg* - ПрАТ «Карлсберг Україна», або будь яка компанія, що входить до Carlsberg Group

Постачальник** - контрагент, що постачає товари, надає послуги, або виконує роботи (згідно Цивільного кодексу України), та постачальник товарів/послуг(в т.ч. робіт) (згідно Податкового кодексу України).