



PROFESSIONAL SERVICES SUBCONTRACTOR SECURITY ADDENDUM

NOT FOR EDITING

Last Updated: October 16, 2026

Download as PDF

This **Professional Services Subcontractor Security Addendum** (“**Subcontractor Security Addendum**”) forms part of and is subject to the agreement between Subcontractor and ClickHouse for the delivery of the Services and Deliverables provided by Subcontractor to ClickHouse (the “**Agreement**”). This Subcontractor Security Addendum sets forth additional terms and conditions related to Subcontractor’s protection of ClickHouse Confidential Information accessed by Subcontractor in connection with the delivery of the Services and Deliverables. Capitalized terms not defined in this Subcontractor Security Addendum shall have the meanings set forth in the Agreement. This Subcontractor Security Addendum is hereby incorporated into and made a part of the Agreement by reference.

For purposes of this Subcontractor Security Addendum: “**ClickHouse Data**” means all data or information of any type (including all software, data, text, audio, video, or images) that Subcontractor develops, accesses, processes, or stores in connection with the Services, including Customer Data and other Confidential Information of ClickHouse’s Customers “**ClickHouse Systems**” means any infrastructure, networks, systems, or applications owned, controlled or managed by ClickHouse or a ClickHouse Customer (including those licensed by ClickHouse or the ClickHouse Customer) that access, transmit, process, or store ClickHouse Data. “**Subcontractor Personnel**” means the employees or contractors providing the Services through a Statement of Work. “**Subcontractor Systems**” means the infrastructure, systems, and applications that access or support the Services or that access, process, or store ClickHouse Data.

1. SECURITY MANAGEMENT

1.1. Information Security Program. Subcontractor shall develop, maintain and adhere to an information security program that is designed to protect the security, confidentiality, and integrity of Confidential Information (the “**Subcontractor Information Security Program**”). The Subcontractor Information Security Program will be implemented on an organization-wide basis, and shall substantially conform to SOC 2 Type II, ISO/IEC 27001, and ISO/IEC 27701 standard. The Subcontractor Information Security Program shall be designed to ensure Subcontractor’s compliance with data protection laws and regulations applicable to Subcontractor’s performance under the Agreement and shall at a minimum include the implementation of safeguards that substantially conform to the ISO/IEC 27002, taking into consideration Subcontractor’s specific information security risk environment. Certain required baseline safeguards are discussed throughout the remainder of this Subcontractor Security Addendum.

1.2. Information Security Program. Subcontractor shall develop, maintain and adhere to its own written, comprehensive set of information security policy documents, which act as the rules and guidelines for dealing with the protection of Confidential Information (“**Policy Documents**”). Policy Documents must be approved by management, communicated and acknowledged by all employees of Subcontractor, and reviewed and updated at planned intervals, no less than annually (or if significant changes occur) to maintain their continuing suitability, adequacy, and effectiveness. Policy Documents shall, at a minimum, address data classification (based on data criticality and sensitivity), data retention and secure destruction, asset identification and ownership, acceptable use, access control, incident response, and business continuity.

2. ORGANIZATION CONTROLS

2.1. Governance. Subcontractor assigns to an individual or a group of individuals appropriate roles for developing, coordinating, implementing, and managing ClickHouse’s administrative, physical, and technical safeguards designed to protect the security, confidentiality, and integrity of Customer Data.

2.2. Risk Assessments. Subcontractor conducts periodic risk assessments designed to analyze existing information security risks, identify potential new risks, and evaluate the effectiveness of existing security controls.

2.3. Risk Prioritization. Subcontractor maintains risk assessment processes designed to evaluate likelihood of risk occurrence and material potential impacts if risks occur.

2.4. Information Security Policies. Subcontractor creates information security policies, approved by management, published and acknowledged by all employees.

2.5. Information Security Policy Review. Subcontractor reviews and updates policies at planned intervals to maintain their continuing suitability, adequacy, and effectiveness.

2.6. Data Classification. Subcontractor maintains a data classification standard based on data criticality and sensitivity.

2.7. Data Retention and Destruction. Subcontractor maintains policies establishing data retention and secure destruction requirements.

2.8. Asset Ownership. Subcontractor implements procedures to clearly identify assets and assign ownership of those assets.

2.9. Compliance. Subcontractor establishes procedures designed to ensure all applicable statutory, regulatory, and contractual requirements are adhered to across the organization.

3. RISK MANAGEMENT

3.1. General Requirements. Subcontractor shall maintain appropriate safeguards and controls and exercise due diligence to protect Confidential Information against unauthorized access, use, and/or disclosure, considering all of the factors below. In the event of any conflict or inconsistency, Subcontractor shall protect Confidential Information in accordance with the highest applicable requirement:

3.1.1 Legal and regulatory requirements;

- 3.1.2 Information technology and industry best practices;
- 3.1.3 Sensitivity of the Confidential Information;
- 3.1.4 Relative level and severity of risk of harm should the confidentiality, integrity, or availability of the Confidential Information be compromised, as determined by Contractor's overall risk management program;
- 3.1.5 ClickHouse's information security requirements, as set forth in this Subcontractor Security Addendum, the due diligence process, and/or the Agreement; and
- 3.1.6 Any further information security requirements which are included in a statement of work, DPA, or similar document which is attached to or relates to the Agreement.

4. SECURITY EVALUATIONS

- 4.1. Subcontractor shall periodically, but no less than annually, evaluate its processes and systems to ensure continued compliance with obligations imposed by law, regulation, or contract with respect to the confidentiality, integrity, and availability of Confidential Information. Subcontractor shall periodically, but no less than annually, have a reputable third-party perform an independent audit of the Subcontractor Information Security Program. Subcontractor shall document the results of these audits and any remediation activities taken in response to such evaluations and make such documentation available to ClickHouse upon written request on up to an annual basis.

5. INTERNAL RECORDS

- 5.1. Subcontractor shall maintain mechanisms to capture, record, and examine information relevant to Security Breaches and other security-related incidents. In response to such events, Subcontractor shall take appropriate action to address and remediate identified vulnerabilities to Confidential Information.

6. PERSONNEL SECURITY

- 6.1. Access to Confidential Information. Subcontractor uses data security personnel that are sufficiently trained, qualified, and experienced to be able to fulfill their information security-related functions. Subcontractor shall require its employees, contractors and agents who have, or may be expected to have, access to Confidential Information to comply with the provisions of the Agreement, including this Subcontractor Security Addendum and any nondisclosure agreement(s) binding upon Subcontractor. Subcontractor shall remain responsible for any breach of this Subcontractor Security Addendum by its employees, contractors, and agents.
- 6.2. Personnel Agreements. Subcontractor requires Subcontractor Personnel to sign confidentiality agreements and acknowledge Subcontractor's information security policy, which includes acknowledging responsibilities for reporting security incidents involving Confidential Information.
- 6.3. Security Awareness. Subcontractor shall ensure that all employees undergo security awareness training on an annual basis, remain aware of industry standard security practices, and their responsibilities for protecting Confidential Information under this Subcontractor Security Addendum.
- 6.4. Supervision of Workforce. Subcontractor shall maintain processes for authorizing and supervising its employees, temporary employees, and independent contractors and for monitoring access to Confidential Information.
- 6.5. Background Checks. Subcontractor shall maintain processes to determine whether a prospective member of Subcontractor's workforce is sufficiently trustworthy to work in an environment which contains Confidential Information, to the extent permitted by local law.
 - 6.5.1 Subcontractor shall ensure that all its employees and contractors are subject to the following background check requirements:
 - 6.5.1.1 Identity verification;
 - 6.5.1.2 Criminal, including a multi-jurisdiction criminal records search covering each jurisdiction in which the individual resided, including a search of applicable national or multi-source criminal record databases and sex offender registry (7 years);
 - 6.5.1.3 OFAC (Office of Foreign Asset Control including Denied Parties List); and
 - 6.5.1.4 Employment Verification (most recent 5 years).

7. ACCESS CONTROL

- 7.1. Identification and Authentication. All access to any Confidential Information shall be Identified and Authenticated as defined in this Section. "**Identification**" refers to processes which establish the identity of the person or entity requesting access to Confidential Information. "**Authentication**" refers to processes which validate the purported identity of the requestor. For access to Confidential Information, Subcontractor shall require Authentication by the use of an individual, unique user ID and an individual password and/or other appropriate Authentication technique. Subcontractor shall maintain procedures to ensure the protection, integrity, and soundness of all passwords created by Subcontractor and/or used by Subcontractor in connection with the Agreement. Shared or generic accounts shall not be used to access Confidential Information. Subcontractor shall require multi-factor authentication for all access to Confidential Information, including all remote access, all privileged access, and all access to any ClickHouse system or ClickHouse customer environment.
- 7.2. Account Administration. Subcontractor shall maintain appropriate processes for requesting, approving, and administering accounts and access privileges for access to Confidential Information, and shall include procedures for granting and revoking access to Confidential Information. Without limiting the foregoing, Subcontractor shall (i) review access rights to Confidential Information on a regular and periodic basis, and no less than quarterly for any access to ClickHouse production environments or Customer Data; and (ii) revoke an individual's access to Confidential Information within twenty-four (24) hours after the termination of such individual's employment or engagement (and promptly upon any change in role that removes the need for such access), and promptly notify ClickHouse where such individual held access to any ClickHouse system.
- 7.3. Access Control. Subcontractor shall maintain appropriate control mechanisms to prevent all access to Confidential Information except by (i) specified users expressly authorized by ClickHouse and (ii) Subcontractor Personnel who have a "need to know" to perform a particular function in support of Subcontractor's performance under the Agreement. The access and privileges granted shall be limited to the minimum necessary to perform the assigned functions. Privileged access to Confidential Information shall be restricted to authorized users with a documented business need.
- 7.4. Use of ClickHouse Systems and Customer Data Location. Where Subcontractor is granted access to ClickHouse Systems, networks, or ClickHouse customer environments (including customer-managed cloud accounts), Subcontractor shall (i) access them only through ClickHouse-issued or ClickHouse-approved accounts, devices, and methods; (ii) comply with ClickHouse's information security policies and access requirements as communicated to Subcontractor; and (iii) not copy,

download, export, or transfer Customer Data out of ClickHouse-managed or customer-managed systems, or to any cloud provider, region, or location other than that specified by ClickHouse or its customer, except as expressly authorized in writing by ClickHouse.

7.4.1 Where ClickHouse requires Subcontractor Personnel only access Customer Data from a particular jurisdiction or that certain Customer Data only be accessed by persons of a certain nationality (e.g., United States persons or citizens), Subcontractor shall comply with such restrictions. In no event will Subcontractor (a) provide Services or access ClickHouse Data or ClickHouse Systems from (i) the Crimea region of the Ukraine, Cuba, Iran, North Korea, Sudan, Syria, or (ii) any other country or region that becomes subject after the effective date of the Agreement to a comprehensive embargo or other restriction that prohibits such access or (b) use Subcontractor Personnel who are prohibited from accessing export controlled technology.

8. CRYPTOGRAPHY

8.1. Subcontractor shall develop and implement cryptographic controls to ensure protection of Confidential Information. Such cryptographic controls shall ensure that all Confidential Information is encrypted in transit using a minimum of SSL with SHA 256 or TLS 1.2 with strong ciphers and at rest using a minimum of AES-256 bit ciphers with strong ciphers. Subcontractor shall maintain documented cryptographic key management procedures, including secure generation, storage, access restriction, and rotation of encryption keys at least annually.

9. PHYSICAL SECURITY

9.1. Subcontractor shall maintain appropriate physical security controls (including facility and environmental controls) to prevent unauthorized physical access to Confidential Information. To the extent Subcontractor relies upon the use of Infrastructure as a Service (IaaS) or Software as a Service (SaaS) providers, Subcontractor shall ensure that (i) it uses hosting service providers that implemented controls designed to restrict unauthorized physical access to areas containing equipment used to provide the IaaS or SaaS and (ii) services are hosted in physical locations that are designed to be protected from natural disasters, theft, unlawful and unauthorized physical access, problems with ventilation, heating or cooling, and power failures or outages.

10. OPERATIONS SECURITY

10.1. Change Management. Subcontractor shall ensure that changes to the organization, business processes, information processing facilities and systems that affect information security are controlled through a defined and implemented change control process, including testing, evaluation, and authorization of material changes to information systems that process Confidential Information prior to implementation.

10.2. Backups. Subcontractor shall ensure all Confidential Information that it processes or stores is adequately backed-up to prevent a loss of confidentiality, integrity, or availability. Backups shall be tested periodically and all backup storage media is subject to the safeguards outlined in this Subcontractor Security Addendum.

10.3. Data Destruction. All Confidential Information maintained by Subcontractor shall be returned to ClickHouse or securely destroyed via commercially reasonable processes once it is no longer needed or at the end of the engagement, but no later than at the termination of this Agreement. Upon ClickHouse's request, Subcontractor shall certify in writing that such return or destruction has been completed.

10.4. Workstation Security Protections. Subcontractor shall centrally manage workstations via endpoint security solutions for deployment and management of endpoint protections, including: (i) full-disk encryption; (ii) anti-malware software; (iii) automatic screen lock after 15 minutes of inactivity; (iv) secure VPN; and (v) data loss prevention (DLP) controls for external drives and network shares. All equipment or media on which Confidential Information is stored shall be protected against unauthorized access or modification.

10.5. Mobile Computing and Teleworking. Subcontractor shall maintain and adhere to industry standard baseline policies, standards, procedures, and controls governing the security of information and systems accessed from outside any ClickHouse or Subcontractor facilities as well as the security of information stored on mobile and telecommuting equipment or other removable media.

10.6. Vulnerability Management and Testing.

10.6.1 Subcontractor shall perform periodic network, infrastructure, and application vulnerability testing, and network and application penetration testing at least annually, of systems that store, process, or transmit Confidential Information, and shall use commercially reasonable efforts to document and remediate identified vulnerabilities in timeframes commensurate with their risk. Subcontractor shall periodically review and test its network security controls. Upon request, Subcontractor shall provide ClickHouse with a summary of its most recent penetration test results and remediation status.

10.6.2 Subcontractor shall ensure that all vulnerabilities on Subcontractor Systems are prioritized and remediated based on their potential impact to ClickHouse Data, ClickHouse Systems, and Subcontractor Systems. In any case, upon becoming aware of a vulnerability (including by notice from ClickHouse, or industry knowledge or publication), Subcontractor shall remediate private and public "critical" and "high" vulnerabilities to ClickHouse's satisfaction within thirty (30) calendar days, and "medium" vulnerabilities to ClickHouse satisfaction within ninety (90) calendar days or ClickHouse may terminate the Agreement for material breach upon notice to Subcontractor without any cure period. Subcontractor shall use the National Vulnerability Databases' Common Vulnerability Scoring System (CVSS), or if not applicable, an equivalent industry standard, to assess whether a vulnerability is "critical", "high", or "medium".

10.6.3 If Subcontractor becomes aware of a "medium", "high" or "critical" vulnerability (assessed as set forth in the paragraph above) in a Subcontractor System then, in each such case Subcontractor shall (a) notify ClickHouse without undue delay, and in any case within 72 hours, after becoming aware of the vulnerability and provide ClickHouse with the cooperation described in Section 14.2.1 below.

10.7. Separation of Environments. Subcontractor shall segregate production systems that store or process Confidential Information from development and test environments, shall not use Confidential Information in non-production environments without ClickHouse's prior written consent, and shall logically separate Confidential Information from the data of Subcontractor's other customers.

10.8. Logging and Monitoring. Subcontractor shall monitor access to, and the availability and performance of, systems that store or process Confidential Information, and shall maintain security logs of such access and activity, which shall be reviewed for anomalies, protected against unauthorized modification, and retained for at least one (1) year.

10.9. Secure Development. To the extent Subcontractor develops software, code, or other technical Deliverables for ClickHouse, Subcontractor shall follow a documented secure development lifecycle, including secure coding practices, code review, and security testing prior to delivery, and shall not knowingly introduce any malicious code or undisclosed means of access into any Deliverable.

11. INFORMATION SECURITY INCIDENT MANAGEMENT

11.1. **Incident Management Program.** Subcontractor shall maintain an information security incident management program to identify, report, and act on all Security Breaches affecting Confidential Information. As used in this section, a “**Security Breach**” is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, access to, or other unauthorized processing of Confidential Information that Subcontractor transmits, stores, or otherwise processes. Subcontractor shall promptly and thoroughly investigate and document each and every Security Breach, including the facts relating to the Security Breach, its effects, and the remedial actions taken. Subcontractor shall maintain a cross-functional incident response team, exercise its incident response procedures (such as through tabletop exercises) at least annually, and implement plans to address any gaps identified in such exercises.

11.2. **Security Breach Notification.** Subcontractor shall notify ClickHouse, without undue delay, after having become aware of a Security Breach. Subcontractor shall assist ClickHouse as reasonably requested by ClickHouse in order to comply with ClickHouse’s own obligations under the relevant data privacy laws to notify if the Confidential Information includes any information relating to an identified or identifiable natural person.

11.2.1 Subcontractor shall notify ClickHouse, without undue delay, and in any event within forty-eight hours, after becoming aware of a Security Breach and in accordance with the Data Processing Addendum. Such notice shall be provided to ClickHouse at security@clickhouse.com and legal@clickhouse.com and shall include, to the extent known, the nature of the Security Breach, the categories and approximate volume of Confidential Information and data subjects affected, the likely consequences, and the measures taken or proposed to address it, and Subcontractor shall supplement such information as it becomes available. Subcontractor shall assist ClickHouse as reasonably requested by ClickHouse in order to comply with ClickHouse’s own obligations under applicable data privacy laws and ClickHouse’s agreements with its customers, including any obligation to notify customers, regulators, or affected individuals. Subcontractor shall not notify any ClickHouse customer or make any public statement regarding a Security Breach involving Customer Data without ClickHouse’s prior written consent, unless required by law.

12. BUSINESS CONTINUITY MANAGEMENT

12.1. Subcontractor shall establish, implement, and maintain processes, procedures, and controls to ensure the required level of continuity for information security during an adverse situation. Subcontractor shall review, update, and exercise the operability of such processes, procedures, and controls by conducting scenario-based recovery exercises at least annually.

13. THIRD PARTIES

13.1. Subcontractor shall ensure that any agent, including without limitation any third-party Subcontractor, to whom Subcontractor provides Confidential Information agrees in writing to maintain safeguards no less protective than those set forth in this Subcontractor Security Addendum to protect such Confidential Information. Subcontractor shall not permit any agent or subcontractor to access Customer Data without ClickHouse’s prior written consent. Prior to subcontracting services, Subcontractor shall establish appropriate contract requirements and conduct an assessment of controls as appropriate to confirm compliance with the objectives of this Subcontractor Security Addendum. Any issues identified by Subcontractor with respect to any agent shall be mitigated in timeframes commensurate with the risk associated with (i) the data, (ii) ClickHouse’s business or operational needs including business continuity, or (iii) granting the agent connectivity to Subcontractor’s network or systems. Subcontractor shall exercise ongoing oversight over each of its Subcontractors to ensure compliance is maintained with the objectives of this Subcontractor Security Addendum. Subcontractor shall remain fully responsible to ClickHouse for the acts and omissions of its agents and subcontractors as if they were Subcontractor’s own.

14. CLICKHOUSE RIGHTS

14.1. **Penetration Testing.** If Subcontractor Systems are used to (a) access ClickHouse Systems or Customer Data or (b) process or store Customer Data, then ClickHouse, or its appropriately qualified third-party representative, may conduct penetration tests (“**Penetration Tests**”) of the Subcontractor Systems upon reasonable notice to Subcontractor. If any such Penetration Test reveals “critical”, “high”, or “medium” vulnerabilities, then unless Subcontractor remediates those vulnerabilities in the timeframes set forth in Section 10.6 to ClickHouse’s satisfaction, ClickHouse may terminate the Agreement for material breach upon notice to Subcontractor without any cure period.

14.2. **Audit Rights.** At no additional cost to ClickHouse, Subcontractor shall provide ClickHouse, or its qualified third-party representative, access to Subcontractor Personnel, and to reasonably requested documentation, logs, and data evidencing Subcontractor’s compliance with its obligations under this Subcontractor Security Addendum and other access as reasonably necessary to allow ClickHouse to review Subcontractor’s security and privacy controls and supporting practices and procedures.

14.2.1 If the audit specified above reveals that Subcontractor does not meet any of the requirements of this Subcontractor Security Addendum or the Agreement, or where ClickHouse identifies a vulnerability or security risk, then Subcontractor will reasonably cooperate with ClickHouse in the resolution of such vulnerability or risk and will provide evidence of such remediation efforts to ClickHouse within the timeframe specified by ClickHouse. If ClickHouse determines, in its reasonable discretion, that Subcontractor does not or cannot sufficiently remediate such security risk or a violation of this Subcontractor Security Addendum, ClickHouse may terminate the Agreement upon notice to Subcontractor.

15. ADDITIONAL REQUIREMENTS

15.1. The parties acknowledge and agree that they will comply with additional requirements as are set forth in the applicable Statement(s) of Work, including commitments required to be flowed down by ClickHouse to Subcontractor as a result of ClickHouse’s commitments to a particular Customer.