snowflake 由神州云计算运营

China Service Security Addendum
中国区服务安全附录

Last Updated: Jun.1st, 2024

更新日期：**2024年6月1号**

This Security Addendum is incorporated into and made a part of the Base Agreement between DCC and Customer for the China Service (together with all expressly incorporated addenda, policies, exhibits, attachments, Order Forms, and other terms, the “**Agreement**”). All capitalized terms used but not defined in this Security Addendum have the meanings set forth in the Base Agreement. In the event of any conflict between this Security Addendum and any other terms of the Agreement, this Security Addendum will govern to the extent of that conflict with respect to the subject matter herein.

本安全附录构成 DCC 和客户之间关于中国区服务的基础协议（连同所有明确收录的附录、策略、附表、附件、订单和其他条款，统称“协议”）的一部分。对于本安全附录中使用但未定义的术语，其定义见基础协议。如果本安全附录与本协议的任何其他条款之间存在任何冲突，则与此处所涉主题相关的冲突应以本安全附录为准。

DCC utilizes infrastructure-as-a-service cloud providers as further described herein and in the DCC Consumption Table referenced in the applicable Order Form and the Documentation (each, a “**Cloud Provider**”) and provides the China Service to Customer using a VPC/VNET and storage hosted by the applicable Cloud Provider (the “**Cloud Environment**”).

DCC 使用本文以及适用订单和中国区服务文档中引用的 DCC 消耗表中描述的“基础设施即服务”云厂商（各称为“云厂商”），并使用由适用云厂商托管的 VPC/VNET 和存储（“云环境”）向客户提供中国区服务。

DCC maintains a comprehensive documented security program, under which DCC implements and maintains physical, administrative, and technical safeguards designed to protect the confidentiality, integrity, availability, and security of the China Service and Customer Data (the “**Security Program**”), including as set forth below. DCC regularly tests and evaluates its Security Program and may review and update its Security Program as well as this Security Addendum; provided, however, that such updates will be designed to enhance and not materially diminish the Security Program.

DCC 有一份全面的、有文档记录的安全计划，并根据该计划实施并维持物理、管理和技术保障措施，旨在保护中国区服务和客户数据的保密性、完整性、可用性和安全性（“安全计划”），包括以下规定。DCC 定期测试和评估其安全计划，并有可能更新其安全计划以及本安全附录，但此等更新旨在加强而非实质性削弱安全计划。

1. DCC’s Audits & Certifications

DCC 的审计与认证

1.1. The information security management system used to provide the China Service will be assessed by independent third-party auditors as described in the following audits/certifications (“Third-Party Audits”), on at least an annual basis (or on such other timeline as required under the audit/certification): MLPS 2.0 Level 3 (based upon GB/T 22239-2019).

用于提供中国区服务的信息安全管理系统将由独立的第三方审计方按照以下审计 / 认证（“第三方审计”）中的描述进行至少每年一次（或按照审计 / 认证要求的其他时间）的评估，：MLPS 2.0 Level 3（基于 GB/T 22239-2019）。

1.2. Third-Party Audits are made available to Customer as described in Section 9.2.1.

如第 9.2.1 节所述，向客户提供第三方审计。

1.3. To the extent DCC decides to discontinue a Third-Party Audit, DCC will adopt or maintain an equivalent, industry-recognized framework.

在 DCC 决定终止第三方审计的情况下，DCC 将采用或维持一个同等的、业界认可的框架。

1.4. Information related to DCC-identified controls for which Customer is responsible in connection with PCI-DSS is available upon written request by Customer. Customer is responsible for performing an independent assessment of its responsibilities under the foregoing.

对于 DCC 指明的、涉及 PCI-DSS 并由客户负责的控制措施，DCC可应客户的书面要求提供相关信息。客户有责任对其上述责任进行独立评估。

2. Hosting Location of Customer Data

客户数据的托管位置

2.1. Hosting Location. The hosting location of Customer Data is the production cloud Environment in the regions offered by DCC and selected by Customer on an Order Form or as Customer otherwise configures via the China Service (each, a “Region”).

托管位置。客户数据的托管位置是 DCC 提供的、客户在订单中选择的或客户通过中国区服务另行配置的区域内的生产云环境（各称为“区域”）。

3. Encryption

加密

3.1. Encryption of Customer Data. DCC encrypts Customer Data at rest and in transit over untrusted networks.

客户数据加密。DCC 在客户数据存放时和通过不可信任网络传输时对其进行加密。

3.2. Encryption Key Management. DCC's encryption key management involves regular rotation of encryption keys and utilizes a key management service to safeguard top-level encryption keys.

加密密钥管理。DCC 的加密密钥管理包括定期轮换加密密钥，并利用密钥管理服务保护顶层加密密钥。

4. System & Network Security

系统和网络安全

4.1. Access Controls.

访问控制。

4.1.1. All DCC personnel access to the Cloud Environment is via a unique user ID, consistent with the principle of least privilege, requires a VPN, as well as multi-factor authentication and passwords meeting or exceeding PCI-DSS length and complexity requirements.

所有 DCC 人员须通过唯一的用户 ID 访问云环境（符合最小权限原则），使用 VPN 以及符合或超过 PCI-DSS 长度和复杂性要求的多因素身份认证和密码。

4.1.2. DCC personnel will not access Customer Data except (i) as reasonably necessary to provide China Service Offerings under the Agreement or (ii) to comply with the law or a binding order of a governmental body.

DCC 人员不得访问客户数据，除非（i）有为提供本协议项下的中国区服务产品的合理须要或者（ii）为遵守法律或政府机构具有约束力的命令所合理需要。

4.2. Endpoint Controls. For access to the Cloud Environment, DCC personnel use DCC-issued laptops which utilize security controls that include, but are not limited to, (i) disk encryption, (ii) endpoint detection and response (EDR) tools to monitor and alert for suspicious activities and Vulnerabilities (as defined below), and (iii) Vulnerability management in accordance with Section 4.7.3 (Vulnerability Management).

终端控制。在访问云环境时，DCC 人员须使用 DCC 配发的笔记本电脑，这些笔记本电脑采用的安全控制措施包括但不限于：（i）磁盘加密；（ii）端点检测和响应（EDR）工具，用于监控可疑活动和漏洞（定义见下文）并发出告警；（iii）根据第 4.7.3 节（漏洞管理）进行漏洞管理。

4.3. Separation of Environments. DCC logically separates production environments from development environments. The Cloud Environment is both logically and physically separate from DCC's corporate offices and networks.

环境分离。DCC 在逻辑上将生产环境与开发环境分隔。云环境在逻辑上和物理上都与 DCC 的公司办公室和网络分隔。

4.4. Firewalls / Security Groups. DCC will protect the Cloud Environment using industry standard firewall or security groups technology with deny-all default policies to prevent egress and ingress network traffic protocols other than those that are required for the operation of the China Service.

防火墙 / 安全组。DCC 将使用符合行业标准的防火墙或安全组技术保护云环境，并采用“一律拒绝”的默认策略，以阻止入站和出站网络流量协议（中国区服务运行所需的协议除外）。

4.5. Hardening. The Cloud Environment will be hardened using industry-standard practices to protect it from vulnerabilities, including by changing default passwords, removing unnecessary software, disabling or removing unnecessary services, and regular patching as described in this Security Addendum.

加固。云环境将使用行业标准实践进行加固，以防范漏洞，包括更改默认密码、删除不必要的软件、禁用或删除不必要的服务，以及按照本安全附录所述定期打补丁。

4.6. Monitoring & Logging.

监控与日志记录。

4.6.1. Infrastructure Logs. Monitoring tools or services, such as host-based intrusion detection tools, are utilized to log certain activities and changes within the Cloud Environment. These logs are further monitored, analyzed for anomalies, and are securely stored to prevent tampering for at least one year.

基础设施日志。监控工具或服务（如基于主机的入侵检测工具）用于记录云环境中的特定活动和变更。DCC将对这些日志进行进一步监控和异常分析，并安全存储至少一年以防篡改。

4.6.2. User Logs. As further described in the Documentation, DCC also captures logs of certain activities and changes within the Account and makes those logs available to Customer for Customer's preservation and analysis.
用户日志。如中国区服务文档中进一步描述的，DCC 还会捕获账户中特定活动和更改的日志，并将这些日志提供给客户，供客户保存和分析。

4.6.3. Third-Party Log Analysis & Product Improvement. Security logs, including those described in this Section 4.6, will be provided to Snowflake China and its third-party service providers within China for security purposes, as well as for product development and improvement. The logs may include information such as username, user ID, as well as IP addresses for the connection being made to the Account.
第三方日志分析和产品改进。安全日志（包括本第 4.6 节所述日志）将提供给 Snowflake 中国及其在中国的第三方服务提供商，用于安全目的以及产品开发和 改进。日志可能包括用户名、用户 ID 以及与账户连接的 IP 地址等信息。

4.7. Vulnerability Detection & Management.

漏洞检测与管理。

4.7.1. Anti-Virus & Vulnerability Detection. The Cloud Environment leverages advanced threat detection tools with daily signature updates, which are used to monitor and alert for suspicious activities and actual or potential errors, flaws, malware, viruses, malicious computer code, and/or other vulnerabilities that may result in a Security Incident within the China Service (collectively, "Vulnerabilities"). DCC does not monitor Customer Data for Vulnerabilities.
反病毒和漏洞检测。云环境利用每日更新签名的高级威胁检测工具，监控可疑活动和实际或潜在的错误、缺陷、恶意软件、病毒、恶意计算机代码和 / 或其他可能导致中国区服务安全事件的漏洞（统称"漏洞"）并发出告警。DCC 不会监控客户数据的漏洞。

4.7.2. Penetration Testing & Vulnerability Detection. DCC regularly conducts penetration tests and engages one or more independent third parties to conduct penetration tests of the China Service at least annually. DCC also runs weekly Vulnerability scans for the Cloud Environment using updated Vulnerability databases.
渗透测试和漏洞检测。DCC 定期进行渗透测试，并至少每年聘请一家或多家独立第三方对中国区服务进行渗透测试。DCC 还使用更新的漏洞数据库每周对云环境进行漏洞扫描。

4.7.3. Vulnerability Management. Vulnerabilities meeting defined risk criteria trigger alerts and are prioritized for remediation based on their potential impact to the China Service. Upon becoming aware of such Vulnerabilities, DCC will use commercially reasonable efforts to address private and public (e.g., CN-CERT announced) critical and high Vulnerabilities within 30 days, and medium Vulnerabilities within 90 days, in each case measured by the availability of a third-party patch, if required. To assess whether a Vulnerability is 'critical,' 'high,' or 'medium,' DCC leverages the China National Vulnerability Database's (CNVD) Common Vulnerability Scoring System (CVSS), or where applicable, the U.S.-CERT rating.
漏洞管理。符合既定风险标准的漏洞会触发告警，并根据其对中国区服务的潜在影响确定修复的优先次序。一旦发现此等漏洞，DCC 将尽商业上合理的努力，在 30 天内应对私人和公共层面上的（如 CN-CERT 公布的）关键和高风险漏洞，在 90 天内应对中风险漏洞，在每种情况下，如有需要，则以第三方补丁的可用性来衡量。为了评估漏洞的等级为"关键"、"高"还是"中等"，DCC 使用中国国家漏洞库（CNVD）的通用漏洞评分系统（CVSS），或在适用的情况下，使用美国计算机应急响应小组（U.S.-CERT）的评分。

5. Administrative Controls

行政管控

5.1. Personnel Security. DCC requires criminal background screening on its personnel as part of its hiring process, to the extent permitted by applicable law.
人员安全。在适用法律允许的范围内，DCC 要求在招聘过程中对其人员进行犯罪背景筛查。

5.2. Personnel Training. DCC maintains a documented security awareness and training program for its personnel, including onboarding and on-going training.
人员培训。DCC 为其员工制定安全意识和培训计划，有文档记录在案，包括入职培训和持续培训。

5.3. Personnel Agreements. DCC personnel are required to sign confidentiality agreements. DCC personnel are also required to sign DCC's information security policy, which includes acknowledging responsibility for reporting security incidents involving Customer Data.

人事协议。DCC 人员必须签署保密协议。DCC 人员还须签署 DCC 的信息安全规定，其中包括知晓有责任报告涉及客户数据的安全事件。

5.4. Personnel Access Reviews and Separation. DCC reviews the access privileges of its personnel to the Cloud Environment at least quarterly and removes access on a timely basis for all separated personnel.

人员访问权限检查和离职。DCC 至少每季度检查一次其人员对云环境的访问权限，并及时删除所有离职人员的访问权限。

5.5. DCC Risk Management and Threat Assessment. DCC’s risk management process is modeled on MLPS and ISO 27001 principles. DCC’s security committee meets regularly to review reports and material changes in the threat environment, and to identify potential control deficiencies to make recommendations for new or improved controls and threat mitigation strategies.

DCC 风险管理和威胁评估。DCC 的风险管理流程以 MLPS 和 ISO 27001 原则为模型。DCC 的安全委员会定期召开会议，回顾威胁环境的报告和重大变化，并确定潜在的控制缺陷，以便就新的或改进的控制和威胁缓解战略提出建议。

5.6. External Threat Intelligence Monitoring. DCC reviews external threat intelligence, including CN-CERT vulnerability announcements and other trusted sources of vulnerability reports. CN-CERT announced vulnerabilities rated as ‘critical’ or ‘high’ are prioritized for remediation in accordance with Section 4.7.3 (Vulnerability Management).

外部威胁情报监控。DCC 检查外部威胁情报，包括 CN-CERT 漏洞公告和其他可信的漏洞报告来源。根据第 4.7.3 节（漏洞管理），CN-CERT 公布的被评为“关键”或“高”等级的漏洞将被优先修复。

5.7. Change Management. DCC maintains a documented change management program for the China Service.

变更管理。DCC 为中国区服务维护一份记录在案的变更管理计划。

5.8. Vendor Risk Management. DCC maintains a vendor risk management program for vendors that process Customer Data designed to ensure each vendor maintains security measures consistent with DCC’s obligations in this Security Addendum.

供应商风险管理。DCC 为处理客户数据的供应商制定供应商风险管理计划，以确保每个供应商采取的安全措施与 DCC 在本安全附录中的义务相一致。

6. Physical & Environmental Controls

物理和环境控制

6.1. Cloud Environment Data Centers. To ensure the Cloud Provider has appropriate physical and environmental controls for its data centers hosting the Cloud Environment, DCC regularly reviews those controls as audited under the Cloud Provider’s third-party audits and certifications, to the extent summarized in reports provided by the Cloud Provider. Each Cloud Provider will have MLPS and ISO 27001 certifications, or industry recognized equivalent frameworks. Such controls will include, but are not limited to, the following:

云环境数据中心。为确保云厂商对其托管云环境的数据中心进行恰当的物理和环境控制，DCC 按照云厂商提供的报告中总结的内容，定期检查云厂商的第三方审计和认证中所审核的控制措施。每家云厂商应拥有 MLPS 和 ISO 27001 认证或行业认可的同等框架。此类控制措施将包括但不限于以下内容：

6.1.1. Physical access to the facilities are controlled at building ingress points;

在建筑物入口处对设施的物理访问进行管控；

6.1.2. Visitors are required to present ID and are signed in;

来访者必须出示证件并签到；

6.1.3. Physical access to servers is managed by access control devices;

对服务器的物理访问由访问控制设备管理；

6.1.4. Physical access privileges are reviewed regularly;

定期检查物理访问权限；

6.1.5. Facilities utilize monitor and alarm response procedures;

设施采用监控和告警响应程序；

6.1.6. Use of CCTV;

使用闭路电视；

6.1.7. Fire detection and protection systems;

火灾探测和保护系统；

6.1.8. Power back-up and redundancy systems; and

备用电源和冗余系统；以及

6.1.9. Climate control systems.

气候控制系统。

6.2. DCC Corporate Offices. While Customer Data is not hosted at DCC's corporate offices, DCC's technical, administrative, and physical controls for its corporate offices will include, but are not limited to, the following:
DCC 公司办事处。尽管客户数据不托管在 DCC 公司办事处，但 DCC 对其公司办事处的技术、管理和物理控制将包括但不限于以下内容：

6.2.1. Physical access to the corporate office is controlled at office ingress points;
在办公室入口处对公司办公室的物理访问进行管控；

6.2.2. Badge access is required for all personnel and badge privileges are reviewed regularly;
要求所有人员佩戴胸卡进入，并定期检查胸卡权限；

6.2.3. Visitors are required to sign in;
来访者必须签到；

6.2.4. Use of CCTV at building ingress points;
在大楼入口处安装闭路电视；

6.2.5. Tagging and inventory of DCC-issued laptops and network assets;
对 DCC 配发的笔记本电脑和网络资产进行标记和清点；

6.2.6. Fire detection and sprinkler systems; and
火灾探测和自动喷水灭火系统；以及

6.2.7. Climate control systems.
气候控制系统。

7. Incident Detection & Response
事件检测与响应

7.1. Security Incident Reporting. If DCC becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data (a "Security Incident"), DCC will notify Customer without undue delay, and in any case, where feasible, within 72 hours after becoming aware. To facilitate timely notification, Customer must register and maintain an up-to-date email within the China Service for this type of notification. Where no such email is registered, Customer acknowledges that the means of notification will be at DCC's reasonable discretion (which may include using the Customer-designated email address associated with the OrgAdmin or AccountAdmin roles of the affected Accounts, and DCC's ability to timely notify will be negatively impacted.
安全事件报告。如果 DCC 发现安全漏洞，导致意外或非法破坏、丢失、篡改、未经授权披露或访问客户数据（"安全事件"），DCC 将立即通知客户，不得无故延误；在任何情况下，如果可行，应在发现后 72 小时内通知客户。为便于及时通知，客户必须在中国区服务中注册并维护一个用于接收此类通知的电子邮箱。如果未注册此等电子邮箱，客户知晓通知方式将由 DCC 合理决定（可能包括使用由客户制定的受影响账户的组织管理员或账户管理员的电子邮箱地址），且DCC 及时通知的能力将受到负面影响。

7.2. Investigation. In the event of a Security Incident as described above, DCC will promptly take reasonable steps to contain, investigate, and mitigate any Security Incident. DCC will preserve any logs determined to be relevant to a Security Incident for at least one year.
调查。如果发生上述安全事件，DCC 将立即采取合理措施，控制、调查和缓解任何安全事件。DCC 将保存任何由其确定与安全事件相关的日志至少一年。

7.3. Communication and Cooperation. DCC will provide Customer timely information about the Security Incident to the extent known to DCC, including the nature and consequences of the Security Incident, the measures taken and/or proposed by DCC to mitigate or contain the Security Incident, the status of DCC's investigation, a contact point from which additional information may be obtained, and the categories and approximate number of data records concerned. Notwithstanding the foregoing, Customer acknowledges that because DCC personnel may not have visibility to the content of Customer Data, it is unlikely that DCC can provide information as to the particular nature of the Customer Data, or where applicable, the identities, number, or categories of affected data subjects. Communications by or on behalf of DCC with Customer in connection with a Security Incident will not be construed as an acknowledgment by DCC of any fault or liability with respect to the Security Incident.
沟通与合作。DCC 将及时向客户提供 DCC 已知的有关安全事件的信息，包括安全事件的性质和后果、DCC 为缓解或控制安全事件而采取和 / 或建议采取的措施、DCC 的调查状况、可提供更多信息的联络方以及相关数据记录的类别和大致数量。尽管有前述规定，客户知晓，由于 DCC 人员可能无法看到客户数据的内容，因此 DCC 不可能提供有关客户数据的具体性质的信息，或在适用的情况下

，受影响数据主体的身份、数量或类别的信息。由 DCC 或代表 DCC 就安全事件与客户进行的沟通不应被解释为 DCC 承认与安全事件有关的任何过失或责任。

8. Deletion of Customer Data.

删除客户数据。

8.1. By Customer. The China Service provides Customer controls for the deletion of Customer Data, as further described in the Documentation.

由客户删除。中国区服务提供由客户控制的删除客户数据的措施，详见中国区服务文档。

8.2. By DCC. Subject to applicable provisions of the Agreement, upon the later of (i) expiration or termination of the Agreement and (ii) expiration of the Retrieval Period, DCC will promptly delete any remaining Customer Data.

由 DCC 删除。根据本协议的适用条款，在（i）本协议到期或终止和（ii）检索期到期（以较晚者为准）时，DCC 将及时删除任何剩余的客户数据。

9. Customer Rights & Shared Security Responsibilities

客户权利和共同安全责任

9.1. Customer Penetration Testing. Customer may provide a written request for a penetration test of its Accounts ("Pen Test") by submitting such request via a support ticket. Following receipt by DCC of such request, DCC and Customer will mutually agree in advance on details of such Pen Test, including the start date, scope and duration, as well as reasonable conditions designed to mitigate potential risks to confidentiality, security, or other potential disruption of the China Service, DCC's, or DCC's third-party service providers or partners respective businesses. Pen Tests and any information arising therefrom are deemed DCC's or its third-party service providers' or partners' Confidential Information. If Customer discovers any actual or potential Vulnerability in connection with a Pen Test, Customer must immediately disclose it to DCC and will not disclose it to any third-party.

客户渗透测试。客户可通过提交支持工单提出书面请求，要求对其账户进行渗透测试（"渗透测试"）。DCC 收到该请求后，DCC 和客户将事先共同商定此等渗透测试的细节，包括开始日期、范围和持续时间，以及为缓解潜在风险而设定的合理条件，此等风险涉及中国区服务、DCC 或 DCC 的第三方服务提供商或合作伙伴各自业务的保密性、安全性或其它可能的影响。渗透测试和由此产生的任何信息都被视为 DCC 或其第三方服务提供商或合作伙伴的机密信息。如果客户在渗透测试中发现任何实际或潜在的漏洞，客户必须立即向 DCC 披露，且不得向任何第三方披露。

9.2. Customer Audit Rights.

客户审计权。

9.2.1. Upon written request of Customer and approval by DCC, DCC will provide Customer, and/or its appropriately qualified third-party representative (collectively, the "Auditor"), access to reasonably requested (i) documentation evidencing DCC's compliance with its obligations under this Security Addendum in the form of, as applicable, documentation evidencing DCC's satisfaction of the MLPS 2.0 Level 3 (based upon GB/T 22239-2019 standards), and (ii) data flow diagrams for the China Service (collectively with Third-Party Audits, "Audit Reports"). If additional charges or costs are incurred due to the Customer's request, the Parties will negotiate the payment of these charges or costs separately.

根据客户的书面请求并经 DCC 批准，DCC 将应客户和 / 或其具有恰当资格的第三方代表（统称为"审计方"）的合理要求提供：（i）证明 DCC 遵守本安全附录所规定义务的文件，其形式为（如适用）证明 DCC 符合 MLPS 2.0 Level 3（基于 GB/T 22239-2019 标准）的文件；（ii）中国区服务的数据流图表（与第三方审计统称为"审计报告"）。如果因客户要求而产生额外费用或成本，双方将另行协商支付此等费用或成本。

9.2.2. Customer may also send a written request for an audit of DCC's applicable controls, including inspection of its facilities. Following receipt by DCC of such request, DCC and Customer will mutually agree in advance on the details of the audit, including the reasonable start date, scope, and duration of and security and confidentiality controls applicable to any such audit. DCC may charge a fee (rates will be reasonable, taking into account the resources expended by DCC) for any such audit. Audit Reports, any audit, and any information arising therefrom will be considered DCC's Confidential Information.

客户也可以发送书面申请，要求对 DCC 的适用控制措施进行审计，包括检查其设施。在 DCC 收到此等请求后，DCC 和客户将事先共同商定审计的细节，包括合理的开始日期、范围、持续时间，以及适用于任何此等审计的安全和保密控制措施。DCC 可就任何此等审计收取费用（费率应合理，并考虑到 DCC 所花费的资源）。审计报告、任何审计以及由此产生的任何信息将被视为 DCC 的机密信息。

9.2.3. Where the Auditor is a third-party (or Customer is using a third party to conduct an approved Pen Test under Section 9.1), such third party may be required to execute a separate confidentiality agreement with DCC prior to any audit, Pen Test, or review of Audit Reports, and DCC may object in writing to such third party if in DCC's reasonable opinion the third party is not suitably qualified or is a direct competitor of DCC, or of DCC's third-party service providers or partners. Any such objection by DCC will require Customer to appoint another third party or conduct such audit, Pen Test, or review itself. Any expenses incurred by an Auditor in connection with any review of Audit Reports, or an audit or Pen Test, will be borne exclusively by the Auditor.

如果审计方是第三方（或者客户使用第三方进行第9.1节规定的经批准的渗透测试），则可能要求此等第三方在进行任何审计、渗透测试或审核审计报告之前与DCC签订单独的保密协议；如果DCC合理地认为此等第三方不具备恰当的资格，或者是DCC或DCC的第三方服务提供商或合作伙伴的直接竞争对手，则DCC可以书面形式反对使用此等第三方。如DCC提出的任何此等异议，客户须指定另一家第三方或自行进行此等审计、渗透测试或审核。审计方在审核审计报告、审计或渗透测试中产生的任何费用将完全由审计方承担。

9.3. Sensitive Customer Data. Use of the China Service to meet regulatory requirements or other heightened standards ("Heightened Standards") may require that Customer implement additional security controls. Customer must implement all appropriate Customer-configurable security controls, including MFA for all User interactive logins (e.g., individuals authenticating to the China Service) to protect Customer Data subject to such Heightened Standards. Additionally, to the extent the Documentation or the Agreement (as amended) sets forth specific requirements related to Heightened Standards (e.g., additional agreements required by DCC and/or requirements to use designated editions and/or Regions of the China Service), Customer must satisfy such requirements before providing DCC any Customer Data subject to such Heightened Standards.

敏感客户数据。如果客户为满足监管要求或其他更严格标准（“更严格标准”）而使用中国区服务，则客户或须实施额外的安全控制。客户必须实施所有客户可配置的恰当安全控制，包括在所有用户界面登录（例如，验证登录中国区服务的个人的身份）中启用MFA，以保护受此等更严格标准约束的客户数据。此外，如果中国区服务文档或本协议（经修订）规定了与更严格标准相关的具体要求（例如，DCC要求的额外协议和/或须使用中国区服务的指定版本和/或区域），客户必须在向DCC提供受此等最严格标准约束的任何客户数据之前满足此等要求。

9.4. Shared Security Responsibilities. Without diminishing DCC's commitments in this Security Addendum, Customer agrees:

共同安全责任。在不减损DCC在本安全附录中的承诺的前提下，客户同意：

9.4.1. DCC has no contractual obligation to assess the content, accuracy or legality of Customer Data, including to identify information subject to any specific legal, regulatory or other requirement, and Customer is responsible for making appropriate use of the China Service to ensure a level of security appropriate to the particular content of Customer Data, including, where appropriate, pseudonymization of Customer Data, and configuration of the China Service to back-up Customer Data;

DCC没有合同义务评估客户数据的内容、准确性或合法性，包括识别受任何特定法律、法规或其他要求约束的信息；客户有责任恰当使用中国区服务，以确保达到适用于客户数据具体内容的安全级别，包括在恰当情况下对客户数据进行假名化，以及配置大陆区中国服务以备份客户数据；

9.4.2. Customer is responsible for managing and protecting its User roles and credentials, including (i) ensuring that all Users keep credentials confidential and not share such information with unauthorized parties, (ii) promptly reporting to DCC any suspicious activities related to Customer's Account (e.g., a user credential has been compromised) by submitting a support ticket and designating it as a Severity Level 1 in accordance with the Support Policy, (iii) appropriately configuring User and role-based access controls, including scope and duration of User access, taking into account the nature of its Customer Data, and (iv) maintaining appropriate password uniqueness, length, complexity, and expiration.

客户负责管理和保护其用户角色和登录凭证，包括：(i)确保所有用户保密登录凭证，不与未经授权方共享此等信息；(ii)通过提交支持工单，及时向DCC报告与客户账户有关的任何可疑活动（例如，用户登录凭证已被泄露），并根据支持策略将支持工单指定为严重等级1；(iii)考虑到客户数据的性质，恰当配置用户和基于角色的访问控制，包括用户访问的范围和期限；(iv)恰当维护密码的唯一性、长度、复杂性和有效期。

9.4.3. To promptly update its Client Software whenever an official update is announced.

在宣布官方更新时及时更新其客户端软件。