QUALCOMM SECURITY TERMS	QUALCOMM 安全条款
The vendor, seller, contractor, or service provider agreeing to these terms ("**Supplier**") has entered into an agreement with QUALCOMM Incorporated or one of its affiliates (each, as applicable, "**Qualcomm**") under which Supplier will Process Data (as respectively defined below) (the "**Agreement**").	凡同意这些条款的供货商、卖方、承包商或服务供应商（下称"**供应商**"）均已与 QUALCOMM Incorporated 或其关联方（如适用，均称为"**Qualcomm**"）签订相应的协议（下称"**协议**"），供应商将依据协议来处理数据（分别定义如下）。
I. Introduction	**I. 引言**
Supplier and Qualcomm agree that, unless expressly superseded in writing, these Security Terms (as may be modified from time to time) (these "**Security Terms**") govern the Processing of Data under the Agreement. These Security Terms are entered into solely in the English language, and if for any reason any other language version is prepared by any party, it shall be solely for convenience and shall have no force or effect and the English version shall govern and control in all respects.	供应商和 Qualcomm 同意，除非以书面形式明确取代，否则本安全条款（经不时修订）（下称本"**安全条款**"）适用于协议项下的数据处理。本安全条款只能以英文订立，如果任何一方由于任何原因编制任何其他语言版本，则这些语言版本应仅为方便起见，不具有任何效力，且在各方面应以英文版本为准。
II. Definitions	**II. 定义**
Capitalized terms in these Security Terms not otherwise defined herein shall have the meaning in the Agreement. For the purposes of these Security Terms:	本安全条款中未定义的术语应具有协议中规定的含义。在本安全条款中：
A. The term "**Data**" means any (i) non-public information of Qualcomm, any of its subsidiaries or affiliated companies, or any of its representatives, customers, distributors or other business partners Processed by Supplier in connection with services provided under the terms of	A. "**数据**"一词是指 (i) 供应商依据协议条款提供服务时处理的 Qualcomm、其任何子公司或关联公司、其任一代表、客户、经销商或其他业务伙伴的非公开信息；(ii) 以及个人信息。

the Agreement and (ii) and Personal Information.	
B. The term "**DP Terms**" means the Data Processing Terms located at https://sp.qualcomm.com/procurement/dataprocessingterms (as may be updated from time to time).	B. "**DP 条款**"一词是指以下网址所示的数据处理条款：https://sp.qualcomm.com/procurement/dataprocessingterms（经不时更新）。
C. The term "**Personal Information**" means any information relating to a particular natural person (or household, if required by Applicable Law) who (i) can be identified from such data, (ii) is potentially identifiable from such data either by itself or combination with any other information, or (iii) can be singled out in connection with such information, including through a unique identifier or through association with a device owned or used by that person.	C. "**个人信息**"一词是指具有以下特征的与特定自然人（或家人，如适用法律要求）相关的任何信息：(i) 可以根据此类数据来识别自然人的身份，(ii) 可以根据此类数据本身或将其与任何其他信息相结合来识别自然人的身份，或 (iii) 可以结合此类信息单独指定自然人，包括通过唯一标识符或者通过与该自然人拥有或使用的设备相关联。
D. The term "**Processing**" or "**Process**" means any operation or set of operations which is performed upon Personal Information, whether or not by automatic means, such as access, collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure, transfer (including cross border transfers), dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.	D. "**处理**"一词是指对个人信息执行的任何操作或一系列操作，无论是否通过自动方式，如访问、收集、记录、整理、存储、改写或修改、检索、咨询、使用、披露、传输（包括跨境传输）、传播或以其他方式提供、对齐或组合、拦截、删除或销毁。
E. The term "**Applicable Law**" means all transnational, national,	E. "**适用法律**"一词是指任何适用司法管辖区中与隐私、个人数

federal, state and local laws (statutory, common or otherwise), treaty, convention, ordinances, codes, rules and regulations of any applicable jurisdiction related to privacy, personal data protection and information security that apply to Qualcomm or Supplier in the performance of its obligations or exercise of its rights under the Agreement.	据保护和信息安全相关并且适用于 Qualcomm 或供应商履行协议规定之义务或行使协议规定之权利的所有跨国、国家、联邦、州和地方法律（成文法、习惯法或其他法律）、条约、公约、条例、守则、规则和法规。
III. <u>Additional Terms</u>	**III. <u>附加条款</u>**
A. <u>DP Terms</u>. In the event that Supplier is Processing any Personal Information under the Agreement, the DP Terms are in addition to and, other than as set forth in Section III (D) (Precedence) below, do not replace any provisions in these Security Terms. If Supplier is Processing Personal Information under the Agreement and the Agreement does not otherwise incorporate the DP Terms, the DP Terms are incorporated by reference into and form an integral part of these Security Terms.	A. <u>DP 条款</u>。若供应商依据协议处理任何个人信息，则 DP 条款作为对本安全条款中任何规定的补充（除下文第 III (D) 条［优先级］所规定的情况之外），不能取而代之。若供应商依据协议来处理个人信息且协议并未另行纳入 DP 条款，则 DP 条款通过引用的方式并入本安全条款，并构成本安全条款不可或缺的一部分。
B. <u>Information Security Review Process.</u> Supplier will be subject to regular security reviews on behalf of Qualcomm and agrees to cooperate in such reviews, including, without limitation, providing all reasonable information requested by Qualcomm regarding Supplier's security policies and practices as part of such review. If any security vulnerabilities, breaches or potential thereof is discovered as part of any security review or otherwise (collectively, "**Findings**"), Supplier shall promptly resolve each	B. <u>信息安全审查流程</u>。供应商将代表 Qualcomm 接受定期安全审查，并同意在此类审查中予以合作，包括但不限于提供 Qualcomm 要求的所有关于供应商安全政策和实践的合理信息，以作为此类审查的一部分。如果在任何安全审查或其他过程中发现任何安全漏洞、泄露或者潜在漏洞或泄露（统称为"**审查结果**"），供应商应根据 Qualcomm 规定的时间表（或双方商定的替代时间表）及时解决每个此

such Finding in accordance with the timeline specified by Qualcomm (or an alternate timeline mutually agreed upon). Failure to promptly address any Finding will constitute a material breach by Supplier and will give Qualcomm the right to immediately terminate this Agreement for cause without the requirement of providing any notice or cure period that may be specified in the Agreement. In the event of a termination pursuant to this Section, Supplier shall provide a prorated refund of any unearned, prepaid payments made to Qualcomm. Notwithstanding the foregoing, this Section in no way limits the other remedies available to Qualcomm under the Agreement. Security reviews will be performed no more frequently than annually, unless the results of any such review results in Findings.	类审查结果。若未能及时解决任何审查结果，将构成供应商的重大违约，并且 Qualcomm 将有权立即因故终止本协议，无需提供协议中可能规定的任何通知或补救期。如果根据本条终止协议，供应商应按比例向 Qualcomm 提供任何未到期预付款的退款。尽管有前文规定，本条不以任何方式限制 Qualcomm 在协议项下享有的其他救济。安全审查的执行频率不会超过每年一次，除非任何此类审查的结果构成审查结果。
C. Qualcomm Training. The following Supplier personnel will be required to complete training on protecting the proprietary and confidential information of Qualcomm and its affiliates:	C. Qualcomm 培训。下列供应商人员需要完成关于保护 Qualcomm 及其关联方的专有和机密信息的培训：
1. Personnel providing services at a Qualcomm or Qualcomm-affiliate facility; or	1. 在 Qualcomm 或 Qualcomm 关联设施提供服务的人员；或
2. Personnel accessing any Data, including, without limitation, Personnel that have access to:	2. 访问任何数据的人员，包括但不限于有权访问以下内容的人员：
a) Qualcomm or	a) 包含数据的

Qualcomm-affiliate systems containing Data (such as Qualcomm-owned, licensed or leased servers, which may include servers at a colocation site or in a cloud environment (e.g., AWS, Microsoft Azure, or the Google Cloud Platform); or	Qualcomm 系统或 Qualcomm 关联系统，如 Qualcomm 拥有、许可或租赁的服务器，可能包括托管站点或云环境中的服务器（如 AWS、微软 Azure 或谷歌云平台）；或
b) Data hosted by a third party, such as a cloud service (e.g., SaaS or IaaS).	b) 由第三方托管的数据，如云服务（如 SaaS 或 IaaS）。
The content of the training will be determined at Qualcomm's sole discretion and will be based on the access requirements necessary for Supplier to provide the services. Qualcomm may ask such personnel to certify in writing completion of the training. In addition, Qualcomm may require additional training at various intervals throughout the term of the Agreement. Failure to timely complete any such training will be considered a material breach of the Agreement and could result in delayed access to the facility and/or data center. Supplier will be responsible for any delay in the services caused by failure of its personnel to timely complete such training.	培训内容将由 Qualcomm 自行决定，并基于供应商提供服务所需的访问要求。Qualcomm 可以要求这些人员书面证明已经完成上述培训。此外，Qualcomm 可要求在整个协议期限内以不同的时间间隔进行额外的培训。若未能及时完成任何此类培训，将被视为严重违反协议，并可能导致对设施和/或数据中心的访问延迟。供应商将对因其人员未能及时完成此类培训而导致的服务延迟负责。
D. Precedence. The terms of the Agreement apply in full to these Security Terms. In the event of any conflict or inconsistency between any provision in these Security Terms and any provision in the Agreement, the provision in these Security Terms shall	D. 优先级。协议条款全部适用于本安全条款。如果本安全条款中的任何规定与协议中的任何规定存在冲突或不一致之处，则以本安全条款中的规定为准，除非协议中的规定明确引用和取代本安全条款中

take precedence, unless the provision in the Agreement expressly references and supersedes the conflicting or inconsistent provision in these Security Terms.

的冲突或不一致规定。

IV. Security Requirements

A. Safeguards. Supplier shall maintain Data and its information technology environment secure from unauthorized access by using best commercial efforts and state-of-the art organizational, physical, and technical safeguards. Such safeguards shall include:

1. Encryption of Data;
2. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;
3. The ability to restore the availability and access to Data in a timely manner in the event of a physical or technical incident;
4. A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of Processing; and
5. All additional controls and measures set out in Sections IV(C) and (D) below.

IV. 安全要求

A. 防护措施。供应商应采取最佳商业措施和最先进的组织、物理及技术防护措施，以保护数据及其信息技术环境免遭未经授权的访问。此类防护措施应包括：

1. 数据加密；
2. 能够始终确保处理系统和服务的保密性、完整性、可用性与恢复性；
3. 在发生物理或技术事件时，能够及时恢复数据的可用性与可访问性；
4. 制定流程，以定期测试、评估及评价技术与组织措施在确保安全处理数据方面的有效性；及
5. 下文第 IV 条 (C) 与 (D) 部分列出的所有额外控制与相关措施。

B. Changes in Security Policy. Supplier shall refrain from implementing changes that materially lower the level of security protection provided as of the effective date of the Agreement. Supplier shall comply with the minimum security standards set forth in these Security Terms and provide sixty (60) days prior written notice to Qualcomm of any significant changes to Supplier's information security policy. If Supplier conducts SSAE 16 or similar or successor audits (such as audits against ISO 27001-2), Supplier shall, at Supplier's expense, provide Qualcomm prompt notice of any non-conformance and promptly remediate and/or mitigate any non-conformance findings. When requested, Supplier shall provide to Qualcomm a sanitized version of any remediation or mitigation plan.	B. 安全政策变更。自协议生效日起，供应商应避免实施那些会大幅降低所提供之安全保护水准的变更。供应商应遵守本安全条款中列明的最低安全标准，并提前六十 (60) 天以书面形式通知 Qualcomm 有关供应商信息安全政策出现的任何重大变更。若供应商执行 SSAE 16、类似审计或后续审计（如依据 ISO 27001-2 开展的审计），则供应商应立即向 Qualcomm 发出任何不合规事项通知并及时补救和/或缓解任何不合规情况，费用由供应商自行承担。一经请求，供应商应向 Qualcomm 提供任何安全版本的补救或缓解计划。
C. Passwords. With respect to Supplier's information technology infrastructure, servers, databases, or networks that Process Data, Supplier shall adhere to each of the following password parameters:	C. 密码。凡涉及供应商信息技术基础设施、服务器、数据库或数据处理网络，供应商均应遵守以下每一项密码参数：
1. Be at least eight characters in length;	1. 长度不得低于八个字符；
2. Include a combination of letters and numbers;	2. 包含字母与数字的组合；
3. Include at least one special character, such as ! & @ * ?;	3. 至少包含一个特殊字符，如 ! & @ * ?；
4. Never be shared or used in connection with another system; and	4. 不得与其他系统共享或结合使用；及

5. Must be changed at least every one hundred eighty (180) days. Alternatively, passwords exceeding twenty-four (24) characters and meeting all complexity requirements above may be changed less frequently (eighteen (18) months or less).

5. 须至少每一百八十 (180) 天更改一次。或者，若密码超过二十四 (24) 个字符且符合以上所有复杂性要求，则可较长时间更改一次（不得超过十八 (18) 个月）。

If a secure multifactor option is used (excluding SMS text one-time password multifactor), password requirements may be reduced by extending password expiration to 12 months.

如果使用安全的多因素密码（不包括短信一次性多因素密码），密码过期时间可延长至 12 个月，从而降低密码要求。

D. Technical Security Controls. With respect to information technology infrastructure, servers, databases, or networks that Process, store, or transmit Data, Supplier shall use the following technical security controls where applicable (and keep them current by incorporating and using all updates commercially available):

D. 技术安全控制措施。凡涉及信息技术基础设施、服务器、数据库或者处理、存储或传输数据的网络，供应商均应在适用情况下采用以下技术安全控制措施（并通过合并及使用所有市售更新以使其保持最新状态）：

1. *Network Protection.*

1. *网络防护。*

a) Network based firewalls;

a) 基于网络的防火墙；

b) Network intrusion detection/protection systems.

b) 网络入侵检测/防护系统。

2. *Client Protection.*

2. *客户端保护。*

a) An anti-virus program using commercially available software that is updated at least daily on systems that are commonly susceptible to virus and

a) 采用使用市售软件的防病毒程序，且至少应每日针对易受病毒和恶意软件攻击的系统进行更新；

malware attacks;

b) Host-based firewall/intrusion prevention software that blocks activity not directly related to or useful for business purposes;

c) A vendor supported operating system with all current critical patches and security fixes installed.

3. *System and Software Protection.*

a) All system and applications must utilize secure authentication and authorization mechanisms;

b) All Supplier-developed applications must be designed and implemented using secure coding standards and design principles (e.g. OWASP);

c) Operating systems should be hardened appropriately according to industry best practices (e.g. NIST 800 series, NSA guidelines, CIS benchmark, etc.).

4. *Encryption.*

Supplier shall utilize only industry accepted encryption algorithms with a minimum key length of 256 bits.

5. *Data Protection.*

b) 采用基于主机的防火墙/入侵预防软件，以阻止无直接关联或无益于商业用途的活动；

c) 采用受供货商支持且安装有当前所有高危补丁和安全修补程序的操作系统。

3. *系统与软件防护。*

a) 所有系统与应用程序均须采用安全认证与授权机制；

b) 供应商开发的所有应用程序在设计与应用过程中，均须符合安全的编码规范及设计原则（如 OWASP）；

c) 操作系统应根据行业最佳实践（如 NIST 800 系列标准、NSA 指导方针、CIS 基准等）进行相应强化。

4. *加密。*

供应商应仅采用行业公认的加密算法，最小密钥长度应为 256 位。

5. *数据保护。*

a) Data Access: Supplier shall ensure that only authorized individuals (based on role) shall, on behalf of Supplier, have access to Data.

b) Data Storage: Supplier shall not Process Data on or transfer such to any portable storage medium unless that storage medium is encrypted in accordance with encryption requirements set forth in this Addendum.

c) Data Transmission: All transmission or exchange of Data by Supplier shall use secure protocol standards in accordance with encryption requirements set forth in this Addendum.

a) 数据访问：供应商应确保仅经授权的个人（基于角色）才可作为供应商代表来访问数据。

b) 数据存储：供应商不得在任何便携式存储介质上处理数据或向其转移数据，除非该存储介质已按照本附录列明的加密要求进行加密。

c) 数据传输：供应商进行的所有数据传输或交换均应采用符合本附录所列加密要求的安全协议标准。

V. Incidents

Except as otherwise set forth in the Agreement or the Data Processing Terms, upon discovery or awareness of any actual or suspected (i) unauthorized access to or disclosure of the Data Processed by Supplier; (ii) unauthorized access to equipment, applications, processes, or systems owned, managed or subcontracted by Supplier on which Data is Processed, or (iii) critical vulnerabilities in any equipment, applications, processes, or systems owned, managed or subcontracted by Supplier potentially affecting the security of Data (each a "Incident"), Supplier will promptly and without undue delay:

1. take steps to mitigate and/or remediate any Incident to protect Data from further risk or harm, initiate an investigation, and notify Qualcomm of the

V. 事件

除非协议或数据处理条款另有规定，否则一旦发现或获知任何实际或可疑的 (i) 未经授权访问或披露供应商处理的数据；(ii) 未经授权访问供应商拥有、管理或分包的、用于处理数据的设备、应用程序、流程或系统，或 (iii) 供应商拥有、管理或分包的任何设备、应用程序、流程或系统中存在潜在影响数据安全的严重漏洞（均称为“事件”），供应商将立即（不得无故延迟）：

1. 采取相应的措施来缓解和/或补救任何事件，以保护数据免受进一步风险或损害，启动调查，并将问题或潜在问题通知

issue or potential issue;	Qualcomm；
2. institute appropriate controls to maintain and preserve all electronic evidence relating to the Incident in accordance with industry best practices;	2. 根据行业最佳实践，采取恰当的控制措施以维护和保存涉及事件的所有电子证据；
3. gather facts and report to Qualcomm the nature of the Incident (including, where possible, the categories of data breached and categories of data loss methods, and to the extent that Personal Information is involved, the categories and approximate number of data subjects concerned and the approximate number of Personal Information records concerned);	3. 收集事实，并向 Qualcomm 报告事件的性质（如有可能，包括泄露数据的类别和数据丢失方式的类别，以及在涉及个人信息的情况下，相关数据主体的类别和大致数量以及相关个人信息记录的大致数量）；
4. provide the name and contact details of the data protection officer or other contact point where more information can be promptly obtained, the likely consequences of the Incident, and the measures taken or proposed to be taken to address the Incident, including (where appropriate) measures to mitigate its possible adverse effects; and	4. 提供数据保护专员的姓名和联系方式或其他可迅速获得更多信息的联络点、事件的可能后果，以及为解决事件已采取或拟采取的措施，包括（适当时）为减轻事件可能造成的不利影响而采取的措施；及
5. take steps to prevent any similar Incident from occurring in the future.	5. 采取相应措施以防止将来发生类似事件。

For the avoidance of doubt, an unsuccessful Incident like pings on firewalls, port scans and malware that is highly unlikely to result in unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system shall not be taken as a reportable Incident for Supplier to report to Qualcomm.

为避免疑问，那些极不可能导致信息的未授权访问、使用、泄露、修改或破坏或干扰信息系统中的系统操作的不成功事件（如防火墙上的 ping、端口扫描和恶意软件），不应被视为供应商应向 Qualcomm 报告的可报告事件。

At no additional cost, Supplier will fully cooperate with Qualcomm in investigating the Incident, including, but not limited to, the provision of system, application, and access logs, conducting forensics reviews of relevant systems, imaging relevant media, and making personnel available for interview. Supplier will also consult and cooperate with any investigations, disputes, inquiries, claims, litigation, or regulatory actions arising from the Incident and provide any information reasonably requested by Qualcomm.

在不增加额外成本的前提下，供应商应全力配合 Qualcomm 调查事件，包括但不限于提供系统、应用程序和访问记录、对相关系统开展取证审查、制作相关媒体影像及安排面谈人员。供应商须商议并配合事件引起的调查、争议、问询、索赔、诉讼或监管行为，并应 Qualcomm 的合理要求提供任何信息。

VI. Audit Rights

VI. 审计权利

Not more than once per calendar year during the term of the Agreement and with at least thirty (30) days prior written notice by Qualcomm to Supplier, Qualcomm may, at Qualcomm's sole expense, audit Supplier to verify compliance with the terms and conditions of these Security Terms, and Applicable Law. Supplier shall cooperate with any legitimate inspection carried out by (i) Qualcomm or any person or party appointed by Qualcomm for this purpose (such person or party not being a competitor of Supplier), or (ii) any competent supervisory authority under Applicable Law, or (iii) both (i) and (ii). Such audit shall be:

在协议期间，每个日历年不超过一次审计且 Qualcomm 至少提前三十 (30) 天向供应商发出书面通知。Qualcomm 可自付费用对供应商开展审计调查，以核实其是否遵守本安全条款所列的条款和条件以及适用法律。供应商应配合以下各方进行的任何合法检查：(i) Qualcomm 或者 Qualcomm 为此目的指定的任何个人或一方（此类个人或一方不是供应商的竞争对手），或 (ii) 适用法律规定的任何有资格的监督机构，或 (iii) (i) 和 (ii) 两者。此类审计应：

1. Completed within two (2) weeks;
2. Performed in a manner that does not unreasonably disrupt Supplier's operations;
3. Performed during Supplier's

1. 在两 (2) 周内完成；
2. 以合理方式进行，不会无端中断供应商的经营活动；
3. 在供应商的正常营业时间进

normal business hours; and

4. Performed on Supplier's premises or through a self-access documentation portal.

Qualcomm shall disclose the results of its audit to Supplier within one (1) week after its completion. Supplier shall promptly respond to audit findings and, at Supplier's expense, remediate and/or mitigate any critical and high-risk findings to the satisfaction of Qualcomm.

VII. Data Deletion or Return

A. Qualcomm's Request. Within seven (7) days of Qualcomm's request, Supplier (and any third parties to whom Supplier has transferred or made available Data) shall, at Qualcomm's option:

1. Electronically erase, destroy, and render unreadable all Data (or any portion of the Data specifically requested by Qualcomm) held in an intangible form;

2. Physically destroy all Data (or any portion of the Data specifically requested by Qualcomm) that is held in a tangible form through shredding all physical media containing such Data; and/or

3. Provide Qualcomm with all physical media containing Data (or any portion of the Data specifically requested by Qualcomm).

Supplier shall certify in writing to

行；及

4. 在供应商的场所或通过可自行访问的文档门户网站进行。

Qualcomm 应在审计工作结束后的一 (1) 周内向供应商披露审计结果。供应商应立即对审计结果做出回应，并自付费用按照 Qualcomm 的要求及时补救和/或缓解任何重大和高危后果。

VII. 数据删除或返还

A. Qualcomm 的要求。在 Qualcomm 提出要求后的七 (7) 天内，供应商（以及供应商已向其传输或提供数据的任何第三方）应根据 Qualcomm 的选择：

1. 以电子方式擦除、销毁以无形形式持有的所有数据（或 Qualcomm 特别要求的数据的任何部分），并使其不可读；

2. 通过粉碎包含数据的所有物理介质，物理销毁以有形形式保存的所有此类数据（或 Qualcomm 特别要求的数据的任何部分）；和/或

3. 向 Qualcomm 提供所有包含数据（或 Qualcomm 特别要求的数据的任何部分）的物理介质。

供应商应以书面形式向 Qualcomm 证明

Qualcomm that these actions have been completed. If, as part of the services, Supplier is Processing Data that is Personal Information, Supplier (and any third parties to who Supplier has transferred or made available Personal Information) must be able to delete / destroy data (as described above) on an individual name-level basis.	上述行为已经完成。如果作为服务的一部分，供应商正在处理属于个人信息的数据，则供应商（以及供应商已向其传输或提供个人信息的任何第三方）必须能够基于个人姓名删除/销毁（如上所述的）数据。
B. Termination or Expiration. Without limiting the foregoing, within thirty (30) days after termination or expiration of the Agreement or the termination or completion of the particular services involving the Processing of Data under the Agreement, Supplier (and any third parties to whom Supplier has transferred or made available Data) shall, at Qualcomm's option:	B. 终止或到期。在不限制前述内容的情况下，在协议终止或到期后三十 (30) 天内，或涉及协议项下数据处理的特定服务终止或完成后三十 (30) 天内，供应商（以及供应商已向其传输或提供数据的任何第三方）应根据 Qualcomm 的选择：
1. Electronically erase, destroy, and render unreadable all Data held in an intangible form;	1. 以电子方式擦除、销毁以无形形式保存的所有数据，并使其不可读；
2. Physically destroy all Data that is held in a tangible form through shredding all physical media containing such Data; and/or	2. 通过粉碎包含数据的所有物理介质，物理销毁以有形形式保存的所有此类数据；和/或
3. Provide Qualcomm with all physical media containing Data. Supplier shall certify in writing to Qualcomm that these actions have been completed.	3. 向 Qualcomm 提供所有包含数据的物理介质。供应商应以书面形式向 Qualcomm 证明上述行为已经完成。
C. Retention Required by Law. In the event that Supplier is required by Applicable Law to retain all or any any portion of the Data, the above Data deletion or return requirements will not apply to any such Data	C. 法律要求的保留。若适用法律要求供应商保留所有数据或数据的任何部分，则上述数据删除与返还要求将不适用于任何需由供应商保留的此类数据，直至供应商需依

required to be maintained by Supplier until the expiration of the period for which Supplier is legally required to retain such Data. During such retention, these Security Terms will remain in effect with respect to any such retained Data.

法保留此类数据的期限到期为止。在此类保留期间，本安全条款对任何此类保留数据始终有效。

VIII. Term & Termination

Notwithstanding anything in the Agreement to the contrary, these Security Terms will take effect on the effective date of the Agreement and will remain in effect until the later of: (i) the completion of the Data deletion or return requirements set forth in Section VII above and (ii) termination of the Agreement.

VIII. 期限和终止

即使协议中有任何相反规定，本安全条款将自协议生效之日起生效，有效期将持续至 (i) 上文第 VII 条列明的数据删除或返还要求完成时，和 (ii) 协议终止，以较晚者为准。

IX. Updates to the Security Terms

Qualcomm may change these Security Terms where such change is required by Applicable Law, court order, or guidance issued by a governmental regulator agency. Any change to these Security Terms in accordance with this Section IX shall become effective on the date that is thirty (30) days' after Qualcomm notifies Supplier of such change (or such earlier period as required by the Applicable Law, court order, or guidance issued by a governmental regulator or agency).

IX. 安全条款更新

如果适用法律、法院命令或政府监管机构发布的指南要求变更本安全条款，Qualcomm 可以变更本安全条款。根据本第 IX 条对本安全条款进行的任何变更应在 Qualcomm 通知供应商此类变更三十 (30) 天（或适用法律、法院命令或政府监管部门或机构发布的指南要求的更早期限）后生效。

X. Manufacturing Security Requirements

In addition to the requirements in these Security Terms, if Supplier configures, or installs equipment and/or provides service and/or maintenance to stand-alone or networked application or hardware solutions within Qualcomm's manufacturing plants, Supplier must comply with the Qualcomm Manufacturing

X. 生产安全要求

除本安全条款中的要求之外，如果供应商在 Qualcomm 的生产工厂内为独立或联网的应用程序或硬件解决方案配置或安装设备，并且/或者提供服务和/或维护，则供应商必须遵守以下网址所示的 Qualcomm 生产安全要求：https://sp.qualcomm.com/procurement/securityterms（经不时更新）。

	Security Requirements located at https://sp.qualcomm.com/procurement/securityterms (as may be updated from time to time).	