Published: May 03, 2023

QUALCOMM SECURITY TERMS

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**").

I. Introduction

Supplier and Qualcomm agree that, unless expressly superseded in writing, these Security Terms (as may be modified from time to time) (these "**Security Terms**") govern the Processing of Data under the Agreement.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.

II. Definitions

Capitalized terms in these Security Terms not otherwise defined herein shall have the meaning in the Agreement. For the purposes of these Security Terms:

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 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).

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.

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.

E. The term "**Applicable Law**" means all transnational, national, 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.

III. Additional Terms

A. DP Terms. 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.

B. Information Security Review Process. 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 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.

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:

1. Personnel providing services at a Qualcomm or Qualcomm-affiliate facility; or

2. Personnel accessing any Data, including, without limitation, Personnel that have access to:

    a) Qualcomm or 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

    b) Data hosted by a third party, such as a cloud service (e.g., SaaS or 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.

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

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.

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.

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:

1. Be at least eight characters in length;
2. Include a combination of letters and numbers;
3. Include at least one special character, such as ! & @ * ?;
4. Never be shared or used in connection with another system; and
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).

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.

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):

1. Network Protection.

a) Network based firewalls;

b) Network intrusion detection/protection systems.

2. Client Protection.

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

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.

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 issue or potential issue;

2. institute appropriate controls to maintain and preserve all electronic evidence relating to the Incident in accordance with industry best practices;

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);

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

5. take steps to prevent any similar Incident from occurring in the future.

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.

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.

VI. Audit Rights

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:

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

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:

1. Electronically erase, destroy, and render unreadable all Data held in an intangible form;
2. Physically destroy all Data 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. Supplier

shall certify in writing to Qualcomm that these actions have been completed.

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 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.

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.

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).

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