TECHNICAL AND ORGANISATIONAL MEASURES FOR DATA SECURITY

Effective Date: April 1, 2025

1. Purpose

This document provides an overview of technical and organizational measures that Qualcomm employs as part of its information security practices applicable to Qualcomm-managed information technology systems (Qualcomm's "Technical and Organizational Measures"). Qualcomm reserves the right to update this document, provided such updates do not substantially degrade the Technical and Organizational Measures.

2. Information Security and Risk Management Program

2.1 Program Scope

Qualcomm maintains an information security and risk management program that includes policies, procedures, and controls that address the management of data ("Information Security and Risk Management Program"). The Information Security and Risk Management Program is designed with measures intended to protect the confidentiality, integrity, and availability of data through a multi-tiered technical, procedural, and people-related control approach in accordance with industry standards.

2.2 Governance

Qualcomm maintains an information security department with staff designated to maintain Qualcomm's Information Security and Risk Management Program.

2.3 Information Security Policies and Standards

As part of the Information Security and Risk Management Program, Qualcomm maintains internal information security policies and standards that are designed to align to industry standards (e.g., ISO 27000-series), with customizations to accommodate Qualcomm's unique security requirements. Exceptions to the policies and standards follow our exception management process.

2.4 Assessments

The Information Security and Risk Management Program is subject to periodic information security assessments that focus on various objectives, such as evaluating the effectiveness of the Information Security and Risk Management Program or portions thereof. For example, assessments may be designed to recognize and assess the impact of risks and to implement identified risk reduction or mitigation strategies to address new and evolving security technologies, changes to industry-standard practices, and evolving security threats.

3. Physical and Environmental Security

3.1 Physical Security

Qualcomm facilities utilize reasonable and appropriate physical controls designed to restrict access to data, including, as Qualcomm deems appropriate, access control protocols, physical barriers such as locked facilities and areas, employee access badges, visitor logs, visitor access badges, card readers, surveillance cameras, and intrusion detection alarms. Qualcomm maintains policies for visitors to Qualcomm facilities, which can include, among other items, sign-in points for visitors. Certain portions of Qualcomm facilities may have further restricted areas that are secured with access controls at entry points (e.g., multi-factor personal identification number (PIN) or badge reader). Qualcomm prioritizes protection of facilities, buildings, and areas based upon their criticality and as such, scales physical security controls accordingly. Further, Qualcomm maintains procedures for review of physical access lists for restricted areas.

3.2 Environmental Security

Qualcomm employs commercially reasonable and appropriate measures designed to protect its facilities from failure of environmental variables such as power, telecommunication, water supply, heating, and ventilation as applicable.

4. Technical Security Measures

4.1 Access Administration

Qualcomm deploys technical authentication and authorization measures on its Qualcomm-managed information technology systems. Such measures may include:

- User authentication requirements to gain access to production and non-production environments.
- Personnel being assigned unique user accounts.
- Use of secure remote access connections, complex passwords, account lock-out, and a phish resistant two-factor authentication connection.

Per a defined policy, access privileges should be configured based on job responsibilities, using the principles of least privilege, and revoked on termination of employment or end of the applicable contract. Access entitlements are reviewed by appropriate management on a defined basis.

4.2 Encryption

Qualcomm uses industry-standard encryption to protect data in transit to and from the public networks. Data is transferred across encrypted network connections and protocols (i.e., HTTPS and/or VPN). Full disk encryption is implemented on Qualcomm-managed end user laptops.

4.3 Logging and Monitoring

Qualcomm utilizes a centralized security information and event management (SIEM) solution to collect and correlate events configured to be logged in an effort to detect anomalies and respond as appropriate. The types of logs that may be captured include Qualcomm-managed network, operating system, application, authentication, and security event logs. Relevant teams within Qualcomm define security monitoring and data flow alert criteria, and Qualcomm's security team has protocols to respond to flagged system alerts.

4.4 Network Security

Qualcomm employs network security measures designed to harden its internet perimeter and help secure infrastructure, including use of firewalls, intrusion detection and prevention systems, and other protection technologies applied where appropriate. Updates to such applied measures are done in accordance with Qualcomm policy.

4.5 Intrusion Detection Systems

Qualcomm uses an intrusion detection system to monitor Qualcomm-managed networks and systems for malicious activity. Intrusion detection activities are collected using the SIEM solution.

4.6 Malware Prevention

Qualcomm runs antivirus and anti-malware (i.e., endpoint detection and response (EDR) software) on Qualcomm-owned and managed endpoints (including employee laptops, desktops, and servers) and provides updates to such software at regular intervals. Additionally, Qualcomm maintains tooling to scan its corporate email instance and traffic thereon for malware.

4.7 Change Control

Qualcomm maintains a change management policy and procedures to evaluate and set out implementation steps for production changes to Qualcomm-managed application, software, database, and hardware services.

4.8 Configuration Management

Qualcomm maintains security baseline and hardening standards, drawing from a variety of industry-standard hardening guides, including those from the Center for Internet Security (CIS), AWS and Azure Well-Architected Frameworks, and the National Institute of Standards and Technology (NIST). Qualcomm regularly reviews, enhances, and refines such standards, incorporating insights from cybersecurity experts and research firms.

4.9 Software Development

Qualcomm develops and maintains processes that provide secure coding principles to be used and applied to development activities both within Qualcomm and for products and services supplied by Qualcomm to others.

4.10 Vulnerability Management

Qualcomm conducts security vulnerability evaluations on a schedule determined by the potential level of risk corresponding to the applicable information asset. Qualcomm carries out external and internal vulnerability scans on Qualcomm-managed networks and infrastructure on a regular periodic basis and discovered vulnerabilities are managed according to Qualcomm's defined policy for vulnerability management. Security-relevant patches, including software, hardware, or firmware updates, are administrated in accordance with Qualcomm's then-current vulnerability management and security patch management standard operating procedures.

5. Organizational Security Measures

5.1 Personnel Security

Subject to applicable legal and regulatory requirements, Qualcomm conducts pre-hire verification checks proportional to the business requirements, the classification of the information to be accessed, and the perceived security risks associated with a position as applicable, for employees (including temporary and contract employees) in accordance with Qualcomm's then-current applicable standard operating procedure and subject to applicable laws.

5.2 Confidentiality

Processes are maintained that inform and obtain agreement from Qualcomm personnel (including temporary and contract employees) to maintain the confidentiality of Qualcomm-owned or managed information and to comply with Qualcomm's internal information and acceptable use requirements.

5.3 Security Awareness Training

Qualcomm personnel (including temporary and contract employees) are required to complete cybersecurity training upon hire and annually thereafter throughout their employment or applicable contract with Qualcomm.

5.4 Vendor Risk Management

Qualcomm maintains a vendor risk management program designed to assess the security posture of its vendors that store, process, develop, or transmit Qualcomm-owned and or managed data.

6. Service Continuity Measures

6.1 Operational Resilience

Qualcomm maintains operational resilience (i.e., business continuity and disaster recovery) plans that align with ISO 22301 and address the availability of critical business processes and systems as determined by Qualcomm. The plans include components such as site risk assessments, business impact analysis, business continuity, and disaster recovery plans. An emergency operations (crisis response) structure is maintained to respond to events that may impact operations throughout the company.

6.2 Backup

Qualcomm maintains a backup schedule for in-scope systems, which includes for certain systems backup on a daily basis to a secondary site. Backups are maintained based on Qualcomm's retention policies for such data.

7. Incident Response Management

Qualcomm has an information security incident response program that evaluates and responds to information security incidents within or impacting Qualcomm. The incident response program is maintained and managed by a dedicated incident response team that operates pursuant to incident management policies and associated processes.

8. Penetration Tests

Qualcomm, or a third-party organization on its behalf, performs periodic security application and or penetration testing on Qualcomm-managed systems and/or applications, or portions thereof, to identify risks and appropriate and commercially reasonable remediation options to help enhance security of the applications.

9. Cloud Security Measures

9.1 Identity and Access Management for Cloud Infrastructure

Qualcomm employs multi-factor authentication (MFA) implementation for all users. Programmatic access requires consistent key rotation, and the principle of least privilege is applied.

9.2 Logging and Monitoring for Cloud Infrastructure

Administrative events are configured to be logged and monitored leveraging the cloud provider recommended mechanisms and are audited by internal security tools as well as a cloud security posture management solution.

9.3 Network Security for Cloud Infrastructure

Qualcomm employs network security measures designed to limit inbound access where appropriate. Virtual private clouds (VPCs) are leveraged to isolate cloud resources.

9.4 Data Encryption in Cloud Infrastructure

Qualcomm's current guidance is that Qualcomm-managed data in transit be encrypted using TLS 1.2+ and Qualcomm-managed data at rest be encrypted using AES256 encryption algorithms.

10. Certifications

Qualcomm's information security management system is certified against the ISO/IEC 27001:2022 standard (Information security, cybersecurity, and privacy protection — Information security management systems). The certificate can be made available upon request.