Technical and Organizational Measures for Safeguarding Customer Data

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. For more information, go to www.broadcom.com. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.

Table of Contents

Overview 4
Measures for data encryption in transit and at rest 5
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of systems and services 6
Measures for ensuring availability and access to data storage environments 7
Measures for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures 8
Measures for user authentication and access control 8
Measures for ensuring security event logging 9
Measures for ensuring secure system configuration 9
Measures for internal IT security and governance 10
Measures for certification/assurance of processes and products 10
Measures for ensuring data minimization and limited data retention 11
Measures for ensuring data quality 11
Measures for ensuring accountability 12
Measures for detecting and responding to security incidents 12
Measures for increasing transparency of data transfers and associated privacy impacts 13
Measures for the handling, recording and reporting of government access requests to data . 13

Overview

This document describes the technical and organizational measures implemented by Broadcom Inc., including its wholly owned subsidiaries ("Broadcom"), to maintain the security of customer data held by Broadcom in the course of its business activities. The content contained herein represents the status quo as of the date of publication. Our security policies and procedures are subject to change without further notice, as the technology and/or threat landscape evolve.

Applicability of Information Security Standards

The applicability and scope of various standards (and corresponding controls) may differ with respect to the requirements of a specific business unit, service, product or specific engagement (e.g., control requirements for "on-premise" solutions may differ from requirements for hosted or cloud-based service offerings). Even though Broadcom's information security controls align with many leading industry standards, Broadcom adopts a standards-neutral approach in its commitment towards information security. Any controls or standards referenced herein reflect a minimum standard of policies and procedures and are intended to provide a general confirmation of implementation of such standards across applicable Broadcom products and solutions.

Policies, Procedures and Certifications

Policies and procedures that regulate the use of information, including its processing, receipt, transmission, storage, distribution, access and deletion ("Policies and Procedures"), are documented and implemented, and address how confidential information is managed and protected. Policies and Procedures are designed to comply with all applicable laws, rules and regulations in the countries in which Broadcom conducts business. The Policies and Procedures are approved by senior management and are reviewed and updated to remain compliant with applicable law and current industry practices.

Measures for data encryption in transit and at rest

Broadcom follows industry standard practices regarding encrypting data both in transit and at rest. Encryption use and applicable encryption standards are defined and documented, and encryption technology used adheres to all applicable legal requirements. Cryptographic key management procedures are documented and automated, and data encryption keys are themselves encrypted. Encryption levels are set at a strength that is commercially reasonable given the nature of the data transmitted and the transmission method(s).

Broadcom requires that any systems used to process personal data support encryption when in transit and implement industry-standard practices regarding encryption of personal data at rest. Encryption use and applicable encryption standards are documented. The encryption strength of confidential information in transmission is defined. Cryptographic key management procedures are documented and automated. Products or solutions are deployed to keep the data encryption keys encrypted.

For all forms of confidential information, including access credentials, any transmission over public networks requires use of an encrypted channel and secure protocols such as HTTPS/SSL, TLS, SFTP, etc. VPN transmissions are performed over an encrypted channel. Electronic transmission of data to and from off-site locations is performed over an encrypted channel. Mobile computing (where permitted) is performed exclusively over encrypted channels. Wireless Access Points allow only authorized users to connect.

Customer information is not stored on any unencrypted portable media. Backup storage devices are encrypted. Secure procedures are defined for transportation of media to and from off-site locations (e.g., inventory tracking, signed checklists), and use of portable media (e.g., removable hard drives, flash drives, removable disks or tapes) is restricted. Policies are defined and enforced for the safe and secure disposal and transmission of media containing confidential information, in accordance with U.S. Department of Defense 5220.22-M or like industry standard procedures and/or NIST standards, where applicable. Media and storage device destruction by a third party is accompanied by documented procedures (e.g., certificate of destruction) for destruction confirmation.

Broadcom contractually requires all third-party data sub-processors to implement technical, organizational and supplementary information security measures no less protective than the measures which Broadcom contractually commits to implement for its customers. To the extent technically feasible and commercially reasonable, such requirements specifically address the control of, and the access to any encryption keys used to protect the data of Broadcom and of its customers, with a view to minimizing the risk of such keys being exposed to any risk of undue access or interference.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of systems and services

Broadcom maintains a proactive security posture by continuously monitoring the threat landscape, analyzing emerging vulnerabilities, and evaluating the impact of real-world attacks. We use these insights to stress-test and refine our internal security controls. Our monitoring framework integrates robust policy governance with advanced malware detection, intrusion prevention, and real-time system health tracking. Furthermore, our comprehensive logging processes ensure that all security events are captured, providing the visibility necessary for rapid investigation and response.

Robust controls are implemented over Broadcom communication networks to safeguard data, tightly control access to network devices through management approval and subsequent audits, disable remote communications if no business need exists, log and monitor remote access, secure remote access devices, and use strong authentication and encryption to secure communications. Defined Access Control Lists (ACLs) to restrict traffic on routers and/ or firewalls are reviewed and approved by network administrators. IP addresses in the ACLs are specific and anonymous connections are not allowed. Only authorized devices connect to Broadcom internal networks.

Firewall management processes are documented. Changes to the firewall are performed via change management processes. Firewall access is restricted to a small set of super users/administrators with appropriate approvals.

Periodic network vulnerability scans are performed, and critical vulnerabilities identified are promptly remediated. Penetration testing of the external perimeter is performed at least annually and may include testing the following attributes: Cross Site Scripting (XSS), injection flaws, malicious file execution, insecure direct object reference, Cross Site Request Forgery (CSRF), information leakage and improper error handling, broken authentication and session management, insecure cryptographic storage, insecure communications and failure to restrict URL access. Follow-up is performed to eliminate or mitigate any risks rated as critical, high or medium.

Personnel authorized to access customer data are subject to an obligation of strict confidentiality as a condition of employment or contract. Employees and any third parties who may access confidential information are required to take training at least annually relating to the security, privacy and protection of such information. Methods of training and awareness include: in-person and online educational programs; exercises; and management communications.

Measures for ensuring availability and access to data storage environments

Protection against fire and measures in case of power outages are implemented in the data processing centers including backup.

Components supporting the physical and environmental security plan are based upon the nature of the facility (e.g., data center or office facility) and may include, where applicable, climate-control systems and sensors, raised floors, smoke and heat detectors, vibration alarm sensors, fluid or water sensors, CCTV installation points, fire-suppression systems, wireless access points, uninterruptible power supplies (UPS), batteries and generators.

Backup, redundancy/failover and offsite storage procedures are documented and include Business Continuity and Disaster Recovery procedures. Procedures encompass the ability to fully restore or utilize redundant platform resources for applications and operating systems. Periodic testing of successful restoration from backup media and redundant failover solutions are demonstrated.

Monitoring tools/ solutions are in place to monitor uptime of web-hosted resources. Restrictions are placed on web server resources to limit denial of service (DoS) attacks.

Effective controls are in place to protect against physical penetration by malicious or unauthorized people. Physical controls covering the entire facility are documented. Additional access restrictions are enforced for server/computer/telecommunications rooms compared to the general area.

Physical access to facilities where data is processed is restricted through the use of access control procedures for authorized users (e.g., badge access). Visitor access must be logged and visitors are escorted through restricted areas in the facility. Physical security plans for offsite facilities are documented. Access control is enforced at entry points and in storage rooms. Access to the off-site facility is restricted and there is an approval process to obtain access.

Monitoring cameras (e.g., CCTV) cover sensitive areas within the facility.

Clean desk/clear screen policy is defined. Workstations are secured, with access to the screen locked during prolonged absences.

Measures for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures

Cloud offerings are subject to third-party audits at least once per year during the term of the applicable governing agreement under Statement on Standards for Attestation Engagements No. 18 (“SSAE 18”, Reporting on Controls at a Service Organization published by the American Institute of CPAs (AICPA). For audits under SSAE 18 the resulting Service Organization Controls (SOC) Report includes the auditor's opinion on the fairness of the presentation of Broadcom's description of controls that have been placed in operation, the suitability of the design of the controls to achieve the specified control objectives, and the auditor's opinion on whether the specific controls were operating effectively during the period under review. Additionally, the specific audit conducted depends on the applicable cloud offering and may include ISO 27001, ISO 27017, ISO 27018, SOC2, SOC3, HIPAA, PCI, IRAP, and any other industry assessments and certifications which will be periodically renewed as appropriate. Broadcom certifications are available at the Trust Center.

Measures for user authentication and access control

Authentication and authorization controls are appropriately robust for the specific levels of risk to the information, data, application and platform. Access rights are monitored to ensure that access adheres to the “least privilege” principle commensurate with the user’s job responsibilities. Access and security events are logged and software is used for anomaly detection in user activities. Access-control policy and corresponding procedures are documented. The access procedures define the request, approval, access provisioning, and de-provisioning, and monitoring processes. The access processes restrict user access (local or remote) based on user job function (role/ profile based, appropriate access) for applications, databases and systems to ensure segregation of duties. Multi-factor authentication or IP address restriction is required to login if customer data is accessible through a public network.

User access reviews are performed periodically for business-critical applications, to confirm that permissions and privileges are appropriate. Procedures are documented for the timely onboarding and off-boarding of users who have joined, left or changed roles within the organization.

The process for the management of privileged user accounts is defined. Organizational responsibility for the creation of privileged accounts is separate from general users. A process is in place to review privileged accounts periodically to ensure that access is restricted, appropriate and documented.

Remote control of desktops is restricted to specific roles (e.g., help desk admin) and remote control is permitted only after the end-user gives permission and persists only until the end of the support session. Unauthorized remote connections from devices are disabled as part of standard configuration. The data flow in the remote connection is encrypted.

Documented password policy covers all applicable systems, applications and databases. Password best practices are deployed to protect against unauthorized use of passwords. The password policy includes the following components: password is communicated separately from user ID, password expiration, password is not shared, initial password generated is random, forced initial password change, minimum password length, password complexity, password history, password lockout for failed password attempts. Passwords are saved only as one-way hash/encrypted files.

Measures for ensuring security event logging

Security events are logged, monitored and addressed through timely and documented action. Network components, workstations, applications and monitoring tools are enabled to monitor and detect anomalies in user activity. Organizational responsibilities for responding to events are defined. Critical system configuration changes are logged and monitored. The log permission restricts alteration by administrators. Retention schedules for various logs are defined and enforced. Logs contain appropriate information to perform forensic analysis.

Measures for ensuring secure system configuration

Information systems are deployed with appropriate default security configurations and reviewed periodically for compliance with security policies and standards.

Standard security configuration is documented. Security hardening procedures include security patches, vulnerability management, avoidance of default passwords, registry settings, and file directory rights and permissions.

Security patch process and procedures, including patch prioritization, are documented.

Documented operating system versions are implemented. Minimum Security Baselines (MSB) are established for various operating systems and versions.

Servers, workstations, laptops, mobile devices, and internet gateway devices are updated periodically with the latest antivirus definitions. Anti-virus tools are configured to run periodic scans, virus detection, real-time file-write activity and signature files updates. Procedures to detect and remove any unauthorized or unsupported applications are documented.

Measures for internal IT security and governance

Policies and procedures regulating the use of information, including its processing, receipt, transmission, storage, distribution, access and deletion ("Policies and Procedures") are documented and implemented, and address how confidential information is managed and protected. Policies and Procedures are designed to comply with all applicable laws, rules and regulations in the countries in which Broadcom conducts business. The Policies and Procedures are approved by senior management, reviewed and updated regularly to remain compliant with the law and current industry practices.

Problem Remediation Management Process/Procedures are documented. The problem management lifecycle includes the following discrete steps: Identification; Assignment of severity to each problem; Communication; Resolution; Training (if required); Testing/validation; Reporting.

Changes to systems, networks, applications, data files structures, other system components, and physical/ environmental changes are monitored and controlled through a formal change control process. Changes are tested, reviewed, approved and monitored during post-implementation to ensure that expected changes are operating as intended.

The change management policy covers all changes to applications, operating systems and network infrastructures, including firewalls. Emergency change management procedures are specified, including factors leading to emergency change. The change management policy/procedure includes the following attributes: Clearly identified roles and responsibilities, including separation of duties; Impact or risk analysis of the change request; Testing prior to implementation of change; Security implications review; Authorization and approval; Post-installation validation; Back-out or recovery plans; Management sign-offs; Post-change review and notification.

Emergency change procedures have stated roles and responsibilities for request and approval. The procedures include a post-change implementation validation. The procedures include post-emergency change documentation update.

Measures for certification/assurance of processes and products

Broadcom maintains certification against ISO/IEC 27001:2022 for security controls for facilities used in complying with customer-facing obligations under the applicable governing agreement. Broadcom will provide the customer with a copy of the applicable ISO/IEC 27001:2022 certification and accompanying Statement of Applicability identifying the controls that were evaluated as part of the certification process.

Broadcom maintains a Secure Software Development Life Cycle ("SSDLC") policy for its commercial software offerings. Software Development Life Cycle (SDLC) methodology is documented and includes version control and release management procedures. SDLC methodology also includes validation of security requirements (e.g., Information Security [IS] sign-offs, periodic IS reviews, static/dynamic scanning). System documentation is managed by appropriate access controls. Code certification is performed to include security review when code is developed by third parties. Software vulnerability assessments are conducted internally or using external experts. Any vulnerability gaps identified are remediated in a timely manner. Developer access to production environments is restricted by policy and in implementation.

SSDLC procedures include guidelines and requirements on what, when and how security activities should take place. Specifically, they include activities for Training, Coding Guidelines, Architectural Risk Analysis, Code Analysis, Penetration Testing, as well as Vulnerability Response. In addition, Broadcom has processes to build privacy protections into products

and services from the initial design phase and continuously improves its Privacy by Design (PbD) and Privacy by Default practices.

Broadcom solutions adhere to technical security standards and safeguards that are appropriate for their intended use and benefit. Security standards are determined after a comprehensive review is conducted that assesses the type of data that will be handled by the solution, how and where the solution is implemented, relevant industry requirements and applicable laws and regulations. Prior to release of products to customers, security scanning is performed in accordance with industry standards and based on the risk profile, additional testing may be performed. Identified vulnerabilities are tracked together with an associated risk rating. Identified Vulnerabilities are ranked using a risk rating (typically using the Common Vulnerability Scoring System [CVSS]) to determine their severity and the appropriate response.

Measures for ensuring data minimization and limited data retention

Where Broadcom acts as a Data Controller, it only collects personal data necessary for and proportionate to the purposes of the processing, pursuant to the terms of Broadcom's Privacy Policy.

Broadcom's products and services are developed and operated following the principles of Privacy by Design and will only collect and process the data necessary for and proportionate to the fulfillment of their intended functionalities. In many cases, customers can configure their products and services by exercising discrete choices on the use of specific functionalities and thereby control the data collected and processed by the specific product or service. More detailed information about the core and optional features of the various products and services, and about the data they involve, may be found in the Transparency Notices.

Broadcom embeds the principle of limited data retention into the design and operation of the services and systems it develops and maintains and adheres to a defined record retention policy. Retention timelines for data in various systems, products and services will depend on the nature, scope and purpose of the system, product or service considered and of the data held therein; on the applicable contractual commitments; on the applicable legal and regulatory requirements; on the existence of a valid business need or legal obligation to retain the data.

Measures for ensuring data quality

Where Broadcom acts as a Data Controller, it takes technically feasible and commercially reasonable steps to ensure that the personal data it processes is accurate and relevant in accordance with Broadcom's Privacy Policy.

Where Broadcom acts as a Data Processor, it offers technical and organizational means for the relevant Data Controller to self-service the accuracy (e.g. rectification or erasure) of personal data processed by Broadcom on its behalf.

Measures for ensuring accountability

Broadcom operates a global privacy program under the responsibility of the Global Privacy Officer. The program includes the creation and maintenance of records of data processing operations, the fulfillment of data subject rights, the handling of inquiries and complaints, the enforcement of privacy by design and privacy by default principles, the provision of transparency information about Broadcom's data processing practices and of the data processing practices involved in the use of specific Broadcom products and services, the response to privacy events and incidents, and privacy training. More detailed information can be found here.

Measures for detecting and responding to security incidents

Broadcom follows comprehensive incident response and vulnerability handling policies, and works closely with leading vulnerability research entities to actively monitor a large number of sources for vulnerability information, including vendor sites, public mailing lists, and security-related websites. To address validated vulnerability issues, we post security notices, patches, and remediation information on the Broadcom Support website. Additionally, we may disseminate security notices and advisories, including to various vulnerability-tracking organizations.

An Incident Response plan and associated procedures are documented and executed in the event of an information security incident. The incident response plan articulates the responsibilities of personnel and identifies relevant parties to notify. Incident response personnel are trained and the execution of the incident response plan is tested regularly.

Measures for increasing transparency of data transfers and associated privacy impacts

Broadcom follows a documented third-party vendor onboarding process to assess, manage and monitor its third-party vendors. Broadcom enters into contracts with sub-processors which incorporate data protection obligations substantially similar to those in this Information Security Practices document and the Data Processing Addendum. The terms of each sub-processor agreement ensures that Broadcom can meet its obligations to customers, including implementing required technical and organizational measures to protect Customer data, to assist with data subject requests and to protect personal data in compliance with applicable data privacy and protection laws and regulations.

Measures for the handling, recording and reporting of government access requests to data

Broadcom has a process to govern the handling of government data access requests whereby requests addressed to Broadcom are acknowledged, assessed for validity and merit, challenged if questionable, disclosed to the extent feasible and permitted by applicable law to the persons concerned and if validated fulfilled only to the minimum extent necessary for compliance with applicable laws, in line with applicable due process.

Revision History

Last updated: June 1, 2026