Information Security Controls for Broadcom

The content contained herein represents the status quo as of the time it was written. Our security policies and procedures are subject to change without further notice, as technology evolves.

I. 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 (for e.g.; controls requirements for "on-premise" solutions may differ from requirements for hosted, cloud-based, service offerings). Even though Broadcom's Information Security Controls document aligns with many leading industry standards, Broadcom adopts a standards neutral approach in its commitment towards information security. Therefore, controls and standards referenced herein this document 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.

II. 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, reviewed and updated to remain compliant with the law and current industry practices.

III. Offerings Including Cloud Services

ISO Certification. Broadcom maintains certification against ISO/IEC 27001:2013 for security controls for facilities used in complying with customer obligations under the applicable governing agreement. Broadcom will provide the customer with a copy of our ISO/IEC 27001:2013 certification and accompanying Statement of Applicability identifying the controls that were evaluated as part of the certification process.

Audit Standards. Cloud Offerings are secured leveraging the previously mentioned ISO/IEC 27001:2013 certification or 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 (SSAE) No. 18, Reporting on Controls at a Service Organization ("SSAE 18") published by the American Institute of CPAs (AICPA). For those audits under SSAE 18, the resulting Service Organization Controls (SOC) Report includes: the auditor's opinion on the fairness of the presentation of Supplier 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.

IV. Controls

Physical Access Control

Physical access to facilities where data is processed is restricted through use of access control procedures for authorized users (e.g., badge access, security guards, etc.). Visitor access must be logged in a physical access log and visitors are escorted through restricted areas in the facility.

Monitoring cameras (e.g., CCTVs) cover sensitive areas within the facility. The monitoring equipment (e.g., CCTV) feed is monitored by a qualified team. Alerting procedures are defined and notification is given to qualified personnel.

Security guards are trained with regards to their response to security events. Security guards perform periodic patrols of the facility and restricted areas.

All employment candidates, contractors and third parties are subject to background validation checks in accordance with relevant laws and regulations

Clean desk/ clear screen policy is defined and enforced. Work stations are secured with access to the screen locked during prolonged absences during the day. Documents containing confidential information are secured in a locked file cabinet or office with access granted to only those individuals with a business need for such information. Offices, desks and file cabinets are locked at the close of business.

Logical Access Control

Authorized user names and individual passwords for accessing data processing systems. 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 access adheres to the 'least privilege' principle commensurate with the user's job responsibilities, all access and security events are logged, and software is used that enables rapid analysis of user activities.

Access Control Policy. 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.

User access reviews are performed periodically (e.g. quarterly) for business-critical applications, to confirm access and privileges are appropriate.

Procedures are documented for the timely onboarding and off-boarding users who have joined, left, or changed roles within the organization.

Platform/ Operating System Level ID Administration. The process for management of privileged user accounts is defined. Organizational responsibility for creation of privileged accounts is separate from general users (based on organization size). A review/governance process is in place and privileged accounts are reviewed periodically (e.g., quarterly) to ensure access is restricted, appropriate and documented (requests, approval) prior to account creation.

Remote control of desktop is restricted to a specific role (e.g., helpdesk admin) and remote control is not permitted unless and until the end user gives permission.

Segregation of Environments. In cloud / production environments where there may be storage and/or processing of customer's data, environments are either physically or logically segregated such that no customer could ever gain access to another customer's data. Furthermore, the production environments are segregated from the non-production environments at all the times. Production Data / Customer information is never used in non-production environments.

Authentication and Authorization. Documented password policy covers all applicable systems, applications and databases. Password best practices are deployed to protect against unauthorized use of passwords.

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. Access to password files is restricted only to system administrators. If the authentication engine for application fails, the default action is always to deny access.

Availability Control

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

Physical Controls. 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 servers/ computer/ telecommunications room compared to the general area.

Backup and Offsite Storage. Components supporting the physical and environmental security plan are based on the nature of the facility (e.g., data center, office facility) and include:
- Climate control system
- Thermostat sensor
- Raised floor
- Smoke detector
- Heat detector
- Vibration alarm sensors
- Fluid or water sensors
- CCTV installation points
- Fire suppression system
- Wireless access points
- Entrance points of the facility
- Uninterruptible power supply (UPS)
- Battery
- Generator

Backup Process. Backup and offsite storage procedures are documented. Procedures encompass ability to fully restore applications and operating systems. Periodic testing of successful restoration from back-up media is demonstrated. The on-site staging area has documented and demonstrated environmental controls (e.g., humidity, temperature).

Media and Storage Device Destruction. Procedures are defined for instructing personnel on the proper methods for destroying media and storage devices on which confidential information is stored. Media and storage devices containing confidential information are wiped utilizing Department of Defense 5220.22-M or like industry standard procedures, which relate to the permanent and non-recoverable removal of data. Media and storage device destruction by a third party is accompanied by documented procedures (e.g. certificate of destruction) for destruction confirmation.

Offsite Storage. Physical security plan for the offsite facility is 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. Electronic transmission of data to the off-site location is performed over an encrypted channel. Back-up storage devices (e.g., flash drives, CD, DVD, USB devices, back-up tapes) are encrypted. Secure transportation procedures (e.g., inventory tracking, signed checklists) of media to and from off-site location are defined.

Handling and Storage. There are policies for the safe and secure disposal and transmission of media containing confidential information in accordance with DOD and/or NIST standards wherever applicable. Use of any portable media (e.g., laptops, removable hard drives, flash drives, removable disks, or tapes) is restricted in Broadcom environments. Customer information is not stored on any unencrypted portable media.

Organizational Control

Operational Procedures and Responsibilities. IT operational procedures ensure secure operation of its IT assets. Operational procedures are documented and successfully executed.

The operation procedures include the following components:
- Scheduling requirements
- Handling errors (e.g., transport of data, printing, copies)
- Generating and handling special output
- Maintenance and troubleshooting of systems
- Documented procedures to manage the SLAs/ KPIs and the reporting structure for escalations

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

End of Life and Faulty Equipment. Procedures exist for disposal/ reuse of retired or failed equipment including proper removal of confidential information.

Change Management. Changes to the system, network, 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.

Change Policy and Procedure. Change management policy includes application, operating system and network infrastructure, including firewall changes. 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 Fix Procedures. 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.

V. Communication and Connectivity

Robust controls are implemented over our communication network 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.

Network Identification Architecture. Network diagrams highlighting key internal network components, network boundary components and Demilitarized Zone (DMZ) environments are documented.

End user access to data is only accessible through application authorization. End users are logically or physically separated from back end data.

Confidential information is encrypted when in transit outside of Broadcom's network.

Firewall management processes are documented. All 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 any critical vulnerabilities identified are promptly remediated.

Network/Communications Security Policy. 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 the Broadcom internal networks.

Remote Access Administration. Unauthorized remote connections from devices are disabled as part of standard configuration. The data flow in the remote connection is encrypted and multi-factor authentication is utilized during the login process.

Third Party Remote Access. Dependent third-party service provider (i.e., subcontractor) remote access adheres to the same or similar controls, and any subcontractor remote access has valid business justification.

Mobile Computing. Mobile computing (where permitted) is performed exclusively over encrypted channels. Wireless Access Points only allows authorized users to connect.

E-mail and IM. Policies and procedures are established and adhered to for proper control of an electronic

mail and/ or instant messaging system.

Authorized E-mail Systems. Preventive and detective controls block malicious e-mails/ attachments. Policy prohibits auto-forwarding of emails. Emails are encrypted via Transport Layer Security (TLS).

Website. Established controls exist to help protect customer data gathered via a website application that is hosted, developed, or supported by Broadcom.

Website Configuration. Multi-tiered architecture is established where the web presentation, business logic and data tier are separated into separate servers and network zones. Website design forces removal of cached data as part of the process upon session termination. Multi-factor authentication or IP address restriction is required to login if customer data is accessible through the website. Periodic penetration testing is performed against the website.

Penetration test includes, but is not limited to, 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
- Failure to restrict URL access

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

VI. Encryption

Encryption Policy. Encryption use and applicable encryption standards are documented. The encryption strength of confidential information in transmission is defined.

Email / Messaging Encryption. Acceptable solutions for email encryption include commercial options such as PGP. Encryption technology used adheres to all legal requirements governing the use of such technology.

Encryption in Transit. Confidential information is encrypted while in transit over any public network or wireless network.

Encryption at Rest. Laptops containing confidential information is encrypted leveraging system level encryption.

Encryption Key Management. Cryptographic key management procedures are documented and automated. Products or solutions are deployed to keep the data encryption keys encrypted (e.g., software-based solution, Hardware Security Module (HSM)).

Encryption Uses. Confidential information transmission over the public internet always utilizes an encrypted channel. Encryption details are documented if transmission is automated. If manual encryption is required, approved and dedicated staff is responsible for encrypting/ decrypting the data. Confidential information is encrypted while in transit over any network using secure protocols like HTTPS, SSL, SFTP, etc. VPN transmissions are performed over an encrypted channel.

VII. Vulnerability Monitoring.

Broadcom continuously gathers and analyzes information regarding new and existing threats and vulnerabilities, actual attacks on the institution or others, and the effectiveness of the existing security controls. Monitoring controls include related policy and procedure, virus and malicious code, intrusion prevention and detection, and event and state monitoring. Related logging process provides an effective control to highlight and investigate security events.

Vulnerability Policy and Procedure. Penetration testing of the internal/ external networks and/ or applications are performed at least annually. The tests are usually performed externally by a reputable external organization. Customer environments are covered as part of the scope of the tests.

Automated vulnerability scans of confidential information are performed periodically to identify, mitigate and remediate any vulnerabilities. Assets include any servers, applications, endpoint desktops, laptops and network devices.

All issues identified from the penetration tests and vulnerability scans rated as critical, high or medium risks are remediated within appropriate timelines.
Anti-virus and Malicious Code. Servers, workstations and internet gateway devices are updated periodically with latest antivirus definitions that include zero-day anti-malware protection. Defined procedure highlights all anti-virus updates. Anti-virus tools are configured to run weekly scans, virus detection, real time file write activity and signature files updates. Laptops and remote users are covered under virus protection. Procedures to detect and remove any unauthorized or unsupported (e.g., freeware) applications are documented.

Alert events include the following attributes:
- Unique identifier
- Date
- Time
- Priority level identifier
- Source IP address
- Destination IP address
- Event description
- Notification sent to security team
- Event status

Security Event Monitoring. Security events are logged (log files), monitored (appropriate individuals) and addressed (timely action documented and performed). Network components, workstations, applications and any monitoring tools are enabled to monitor user activity. Organizational responsibilities for responding to events are defined. Configuration checking tools are utilized (or other logs are utilized), that record critical system configuration changes. The log permission restricts alteration by administrators. Retention schedule for various logs are defined and adhered.

VIII. Incident Response

An Incident Response plan and associated procedures are documented in the event of an information security incident. The incident response plan clearly articulates the responsibilities of personnel and identifies relevant parties for notification. Incident response personnel are trained, and execution of the incident response plan is tested at least annually.

Incident Response Process. Information security incident management procedures are documented. The incident management procedures include the following attributes:

- Organizational structure is defined
- Response team is identified
- Response team availability is documented
- Timelines for incident detection and disclosure are documented
-

Incident process lifecycle is defined including the following discrete steps:

- Identification
- Assignment of severity to each incident
- Communication
- Resolution
- Training
- Testing (check frequency)
- Reporting
- Incidents must be classified and prioritized
- Incident response procedures include notification to the relationship (delivery) manager or another contact listed in the contract

Escalation/Notification. The Incident response process is executed as soon as Broadcom is aware of the incident (irrespective of time of day).

Employee Education and Awareness. Employees and any third parties who may access to confidential information are required to take training at least annually relating to the protection of that data. Methods of training and awareness include:

- Online educational programs
- Messaging from management to employees
- Internal and external data privacy websites
- Webline and helpline resources for reporting issues
- Internal portals

IX. Internal System Development

There is an established software development lifecycle for defining, acquiring, developing, enhancing, modifying, testing and implementing internal information systems.

Development Lifecycle. 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 identified vulnerability gaps are evaluated and appropriately addressed in a timely manner. Developer access to production environment

is restricted by policy and in implementation.

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

Secure Configuration Availability. Standard security configuration for internal information systems is documented. Security hardening and procedures include: security patches, vulnerability management, default passwords, registry settings, and file directory rights and permissions.

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

Vulnerability Analysis. Penetration testing of the external perimeter of internal information systems is performed at least annually. For most recent testing results/ report, follow-up is performed to eliminate or mitigate any issues rated as critical, high and medium risk. Tools/processes are in place to perform vulnerability monitoring, penetration testing, antivirus definitions, firewalls, application gateway (proxy) and guard testing.

Operating System. Documented operating system versions are implemented. Minimum Security Baselines (MSB) are established for various operating systems and versions. Multiple simultaneous logins to the environment are not allowed for any single administrator.

X. Security applicable to products and solutions

Secure Code Development. All product teams are required to follow our product securability policies and procedures, which provide security standards, strategies and tactics for each phase of the product development lifecycle. These procedures include guidelines and requirements on what, when and how security activities should take place. Specifically, they include activities for all phases of the Secure Software Development Lifecycle, such as Training, Coding Guidelines, Architectural Risk Analysis, Code Analysis, Penetration Testing, as well as Vulnerability Response. In addition, we have processes to build privacy into our products and services from the initial design phase and we are continuously evolving our practices around Privacy by Design (PbD) and Privacy by Default to meet GDPR and other global privacy requirements.

Encryption. We follow industry standard practices with regard to encrypting data in transit and at rest. Our systems use encryption to protect transmitted records and files containing data that will travel across public networks, with encryption at a strength that is commercially reasonable given the nature of the data transmitted and the transmission method(s). We require that our systems used to process sensitive data, including personally identifiable information (PII), passwords, account information, *etc.*, support encryption when in transit on the network and implement industry-standard practices regarding encryption of sensitive data stored at rest.

Security Standards and Safeguards. Our solutions are required to 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, and industry requirements and regulations.

Secure Code Release. Prior to release of products to our customers, antivirus/antimalware scanning is performed in accordance with industry standards and based on the risk profile additional testing may be performed. Identified vulnerabilities are tracked in a central defect tracking system together with an associated risk rating. Identified Vulnerabilities are ranked using a risk rating (typically using the Common Vulnerability Scoring System (CVSS)) consistent with the NIST Framework to determine their severity and response.

Product Security Incident Response. We follow a set of comprehensive *incident response and vulnerability handling policies* (consistent with ISO 29147 and ISO 30111) 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 Customer Support website. Additionally, we may disseminate security notices and advisories to public mailing lists (mentioned above), and to various vulnerability-related organizations such as CERT and Mitre CVE.

XI. Revision History

Revision	Date	Update Description	Author
1.2	1/6/2020	Aligned document with current Broadcom security standards.	Michael Mattia

Approved By: **Date:**

Sean Oldham, Chief Information Security Officer (CISO)	DocuSigned by: Sean Oldham EB655E4DE1B6432...	Jan-08-2020