Texas Instruments Incorporated

TI Business Partner Information Security Requirements

Business Partners' access to or use of TI Information Assets (which include both Business Information and Information Resources) must be in accordance with TI's policies, procedures, processes, industry best practices, and applicable law. This document is a reference for Business Partners summarizing TI's policies, procedures, and processes applicable to Business Partners' use of TI Information Assets.

Business Partners must:

- Use TI Information Assets for TI business purposes only;
- Use TI Information Assets safely;
- Avoid loss or damage to TI, its operations, and its financial and reputational interests when using TI Information Assets; and
- Seek clarification from TI if a policy, procedure, or process is unclear or does not appear to expressly cover a particular use of TI Information Assets.

Business Partners must meet requirements in the following areas:

- Business Partner IT security and privacy controls;
- Appropriate use of TI Information Assets; and
- Information Asset requirements.

DEFINITIONS

"Business Information" includes all information owned, used or produced by TI or its subsidiaries. This information is an asset regardless of how it is created, distributed, or stored.

"Business Partner" means contractors, service providers, and other third parties that have a business relationship with TI.

"Confidential Information" is information or data that: 1) is not generally known or readily ascertainable from public sources; 2) derives value from the fact that it is not generally known; and 3) is the subject of reasonable efforts to maintain its secrecy. Confidential Information includes information that TI has a duty to keep confidential or that TI chooses to keep confidential because it maintains its value by not being generally available to the public.

"Computer Security Incident" is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. Examples include:

- Attempts (either failed or successful) to gain unauthorized access to a system or its data;
- Unwanted disruption or denial of service;
- The unauthorized use of a system for the processing or storage of data; or
- Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.

“Data Privacy Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed.

“Information Assets” means Business Information and Information Resources (any physical or logical thing that creates, processes, transmits, or stores TI Business Information). Examples of Information Assets include mobile phones, computers, manufacturing tools, and workstations, and the Business Information they contain (for example, product designs, sales and marketing data, or HR records).

“Information Resource” means any physical or logical thing that creates, processes, transmits, or stores TI Business Information. Examples include but are not limited to: hardware, software, servers, applications (to include middleware), workstations, personal computers, storage, and network routers, switches, or other networking devices. NOTE: Includes hosted services (cloud, etc.)

“Logical Access Controls” are tools and protocols used for identification, authentication, authorization, and auditing in computer information systems. Logical access is often needed for remote access of hardware and is often contrasted with the term "physical access", which refers to interactions (such as a lock and key) with hardware in the physical environment, where equipment is stored and used.

“Logical Account” is a user profile that provides identification, authorization, authentication, and auditing for Information Resources (otherwise known as a login account containing an assigned ID and password used to access online information or computer systems). Examples of Logical Accounts include: user accounts, computer accounts, process accounts, etc.

“Personal Data” means any information relating to an identified or identifiable natural person (the “Individual”). A person’s identity is “identifiable” if it can be derived from Personal Data (e.g., email, telephone number, home address, identification number, function, or other distinguishing characteristics).

“Sanitize” means a process to render access to target data on storage media infeasible for a given level of effort, providing a reasonable assurance that the target data may not be retrieved and reconstructed. Clear, purge, and destroy are actions that can be taken to sanitize media; see: NIST-800-88 Guidelines for Media Sanitization Appendix A.

Business Partner IT security and privacy controls program:

Business Partners must implement an IT security and privacy controls program that:

- Is appropriate for the mission and business requirements of the Business Partner and similar to other companies in the Business Partner’s industry;
- Demonstrates due diligence with regard to information security and risk management; and
- Supports TI Information Asset policies, procedures, and processes.

Business Partners IT security and privacy control program should address the following areas:

Access Control	Personnel Security
Application Development and Security Practices	Physical and Environmental Protection
Assessment, Authorization, and Monitoring	Planning
Audit and Accountability	Privacy Authorization
Awareness and Training	Program Management
Configuration Management	Risk Assessment
Contingency Planning	Security Assessment and Authorization
Identification and Authentication	System and Communications Protection
Incident Response	System and Information Integrity
Maintenance	System and Services Acquisition
Media Protection	Third Party Assessment

Derived from NIST 800-53 revision 5 Section 2.2 Control Structure and Organization

Additionally, Business Partners' IT security and privacy control program must assure that TI Personal Data will be:

- Processed fairly, lawfully, and transparently;
- Collected and processed only for specific legitimate purposes;
- Limited to the relevant data needed;
- Maintained to be accurate as necessary;
- Processed in a manner that ensures appropriate security, including protection against Data Privacy Breach using reasonable technical and organizational measures;
- Transferred to another country or a third party only when appropriate safeguards are in place; and
- Retained only for as long as necessary for the purposes for which TI Personal Data is processed.

Business Partners who engage third parties to process TI Business Information must have at a minimum the same or similar security and privacy requirements included in their third party agreements as set forth in TI's policies and must regularly perform third-party security assessments.

Appropriate use of TI Information Assets:

Business Partners will not create the appearance or reality of misuse of TI Information Assets, including by:

- Violating the rights of others;
- Using TI Information Assets for non-TI work;
- Attempting to circumvent any security measures or controls; or
- Creating, displaying, procuring, or transmitting inappropriate materials.

Business Partners will not search for or request access to TI Information Assets not necessary or relevant to TI's business purpose; access to TI Information Assets is only allowed if necessary to achieve TI business and approved by TI.

Business Partners must treat TI Business Information as Confidential Information until it has been classified by TI.

Business Partners processing TI Confidential Information must:

- Implement controls to prevent accidental or intentional misuse or loss of TI Confidential Information;
- Encrypt TI Confidential Information in transit and appropriately protect it at all other times;
- Consult with TI to properly classify TI Business Information created by the Business; and
- Protect authentication information, such as passwords, as the highest level of TI Confidential Information.

Business Partners are responsible for all activity associated with Logical Accounts assigned to their users. Business Partners' users will not share Logical Accounts.

Business Partners are required to promptly notify TI in the event:

- TI Business Information is misused or lost, including as a result of a Computer Security Incident; or
- TI Information Assets may have been affected by a Computer Security Incident involving the Business Partner.

Business Partners with access to TI Information Assets are required to complete periodic TI IT Security training.

Business Partners should have no expectation of privacy while using TI Information Assets.

Abuse of TI Information Assets may result in the loss or restriction of Business Partner's privileges to access TI Information Assets.

Information Asset requirements:

Logical Access Controls

Business Partners must take action (including notifying TI as applicable) to revoke their users' access to TI Information Assets when that access is no longer necessary for TI business purposes. Business Partners must take action within 24 hours for users who have separated from the Business Partner including by resignation, termination, retirement, etc.

Where technically feasible, TI authentication should be used to restrict access to TI Information Assets (which includes Business Partner provided services), for example through the use of single sign-on. When TI authentication cannot be used, Business Partners are responsible for providing secure authentication processes including:

- Passwords that meet TI's requirements for maximum age, minimum length, complexity and strength, history, and lockout;
- Changing default passwords;
- Password reset procedures that are secure and resistant to social engineering; and
- Protecting TI Confidential Information accessible from the internet by multi-factor authentication.

Business Partners with access to TI Information Assets must require multi-factor authentication when remotely accessing the Business Partner's network. Business Partners that use cloud-based email or other critical cloud-based infrastructure solutions must require administrators of the cloud solutions to use accounts secured with multi-factor authentication.

Physical Access Controls

Business Partners must implement physical access controls to prevent unauthorized access to their Information Resources that process TI Business Information.

Endpoint Protection

Business Partners are expected to have an endpoint protection program that meets current security best practices, including:

- Running an operating system (OS) that is supported by the OS vendor and is current on critical security patches;
- Using an up to date anti-malware solution with real-time protections enabled;
- Implementing strong password or other equivalent authentication protections;
- Implementing full disk encryption for laptops and mobile devices; and
- Other specific controls as communicated by TI.

Business Partners must scan all removable media, storage media, laptop computers, and other Information Assets for malware and remediate before directly connecting to any TI Information Assets.

Business Partner webservers which are processing TI Business Information must be configured securely, similar to the controls described in NIST 800-44.

Network Access Controls

Business Partner Information Resources that are connecting to TI's network may be assessed in real time for compliance with endpoint security requirements (as stated in Endpoint Protection); non-compliant Information Resources may be denied access.

Data Protection

Encryption methods must meet industry standards, such as NIST Cryptographic Standards and Guidelines, and include a key management plan.

Business Partners storing TI Business Information will consult with TI to establish backup requirements that assure the availability, confidentiality, and integrity of the Business Information including:

- Which TI Business Information must be backed up;
- Encryption of backups;
- Frequency of backups and number of backup versions to retain; and
- Maximum time to restore (Recovery Time Objective) and restore point (Recovery Point Objective) of requested data.

Business Partners are required to Sanitize TI Business Information on their Information Resources when notified by TI that the TI Business Information is no longer required for TI business purposes or before an Information Resource is recycled, disposed of, or given to a third party.

Software Licensing
All software used to process TI Business Information must be properly licensed.

Recording Devices
Business Partners must receive specific approval from TI before use of a recording device on TI premises; notice and consent are required.

Business Partner Information Resources on TI premises will not automatically enable webcams or other recording devices.

Application Security
Business Partners providing applications, including Software as a Service (SaaS), to TI must:

- Regularly scan the application (including the supporting infrastructure) for vulnerabilities, promptly remediate vulnerabilities found, and retain evidence of scans and remediation;
- Promptly install security patches;
- Validate all user supplied input against expected responses;
- Design error messages such that they do not reveal information that might be helpful to someone trying to reverse engineer or break the application (for example, authentication failures must not specifically reveal why the authentication failed); and
- Not store users' credentials, permissions, authentication information, or other sensitive information in clear text such as browser cookies, html tags, logs, or scripts.

Network Security
Business Partner will not configure their network, without express written authorization from TI, in any way that bridges TI's network with any third party network.

Business Partners are prohibited from modifying the TI network in any way without the express written authorization from TI (for example, by configuring commercially purchased switches, routers, hotspots, or configuring information resources to route or switch traffic for other systems).

Business Partners must not access TI Confidential Information over non-TI networks through insecure protocols such as FTP or TELNET.

Audit Logs
Business Partner's Information Assets that are processing TI Business Information must enable audit logging to support forensic analysis, assure audit logs are active at all times, protect audit logs from accidental or intentional loss or alteration, retain logs for at least 6 months, and make such logs available to TI upon request.

Instant Messaging
Business Partners must not use any instant messaging service (e.g. SMS text messaging, iMessage, WhatsApp) to transfer TI Confidential Information unless that service has been approved by TI.

Email
Business Partners with access to a TI email account may not automatically redirect email from that account to a non-TI account.

Business Partners sending mass emails on TI's behalf must:

- Include a procedure to unsubscribe from mass emails;

- Clearly indicate in the body of the email that it was sent by the Business Partner and not by TI; and
- Provide a legitimate, correct, and valid sender and return email address.

Business Partners must not send email with a TI domain sender or return address from non-TI managed infrastructure without explicit TI approval.

Training and Awareness

Business Partners are required to assure that their users and subcontractors who come into contact with TI Information Assets are aware of these security requirements and have received appropriate security training.