Texas Instruments

January 9, 2024

TI cybersecurity statement

Texas Instruments (TI) works continuously to identify and eliminate potential cybersecurity threats to its customers, employees, IT infrastructure, proprietary technologies, and confidential information. To ensure the value of our security investments, TI generally does not disclose specific details regarding information security practices; however, the following information provides an overview of TI's cybersecurity risk management program.

Our cybersecurity risk management program is based on best practice management and governance frameworks, such as the International Organization for Standardization (ISO), the National Institute of Standards and Technology (NIST) and the Center for Internet Security (CIS) Controls. We leverage foundational cybersecurity principles in our program, such as security by design, defense-in-depth, least privilege, and resilience-focused backups to manage risk.

Our cybersecurity strategy, plans, policies and protocols are designed to reduce our risks and strengthen our security posture to protect our company, technology, and data. Our policies include defining the acceptable use of our information assets, defining access requirements for specific data or technologies, protecting personal information and privacy, and complying with regulations such as the EU General Data Protection Regulation and the China Cybersecurity Law.

TI’s cybersecurity risk management program is governed by:

- An Executive committee that oversees TI's information security programs
- A Board of Directors Audit Committee that is responsible for conducting annual reviews of internal and external audit results
- TI cross-business governance and compliance councils that focus specifically on confidential information protection and personal data protection, including that of third parties
- An advisory panel representing all IT divisions that assists in security initiative alignment

To protect TI assets and intellectual property, TI’s global IT Security Team, reporting to the Chief Information Security Officer (CISO), provides various services including threat and vulnerability management, security monitoring and incident response, policy development, risk compliance management, security strategy development and execution, contingency planning, security and phishing awareness training.

TI's security program focuses on the following policy and technology elements: system access procedures, periodic account access reviews, password complexity and change frequency requirements, client and server secure baselines, vulnerability management programs, disaster recovery planning, secure network design (including firewalls, demilitarized zones and internal trust zones), and multi-factor authentication.

In addition, all TI employees and contractors are responsible for protecting information that’s been entrusted to TI. To fulfill this responsibility, TI employees and contractors must adhere to TI's Acceptable Use Policy, properly handle confidential data, protect passwords, and learn to identify and report suspicious emails. IT security training is mandatory for all employees and contractors, with specific role-based training provided for key IT roles.

For TI, cybersecurity is of utmost importance. We are constantly striving to improve and fortify our cybersecurity risk management program by drawing from best practices frameworks, internal and external audit findings, and industry lessons learned.

Important note: This information is provided for illustrative purposes only, and should not be relied upon nor construed as a representation or warranty of any sort; this information is provided strictly on an “as-is” basis. Practices and policies in these areas change and evolve rapidly, and publishing the details of IT Security policies or approaches can be counterproductive to their effective practice. Accordingly, the above information is meant to convey a general sense of TI’s concerns and of some protective steps and measures undertaken, but does not reflect all applicable current practices and policies.