TI Corporate Citizenship

Topic Brief

Information protection

Texas Instruments

Information protection

Why it matters

The security of our technologies and our business is of utmost importance. We strive to protect our intellectual property, competitiveness and reputation from cybersecurity threats.

We leverage industry frameworks and security standards, and collaborate with expert resources and industry partners to exchange information about cybersecurity threats, best practices and trends.

Our approach

We work continuously to identify and eliminate potential threats to our information technology (IT) infrastructure and our proprietary technologies that are key to business growth and profitability.

Reducing risks

As computer-based threats and vulnerabilities continue to grow in number and sophistication, so have concerns about information protection from our global partners, suppliers and customers.

Our risk management process is based on best-practice management and governance frameworks, such as the International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technologies (COBIT) and more.

Using guidance from these organizations, as well as information gleaned from our own assessments, we have developed security plans, policies and protocols to reduce our risks and strengthen our security posture. Our policies range from defining the acceptable use of employee's information assets, to technical requirements for specific technologies and how we protect personal information and privacy.

Our Global Information Security team identifies and responds to threats and works with our business units and support teams to improve security. We also:

- Restrict access to data traveling to and from our computers, servers, networks and other IT systems
- Monitor IT systems and alerts of inappropriate activity
- Deliver cybersecurity awareness and confidential information protection training to all TIers and specialized security training to our IT Services team
- Conduct risk and compliance assessments on third parties that request access to our IT resources and information
- Deploy industry standard account protections, including password complexity, routine password changes and two-factor authentication

Assessing security effectiveness

We regularly review and test our controls to ensure protections are functioning as they should. We do this by conducting external penetration tests, internal vulnerability assessments and audits at the site and business level. We also evaluate our practices against industry standards and vet with external experts. We address any deficiencies that are identified.

Accountability

Our chief information officer oversees information protection. We also have several governance and compliance structures in place to ensure issues are elevated and addressed:

- Senior leaders from major business units and support entities provide regular updates on cybersecurity threats, assist in prioritizing security actions and help build awareness and support within their organizations
- Our Confidential Information Protection Council focuses on ensuring that confidential information and trade secrets are appropriately classified and protected
- Our Privacy Committee, comprised of cross-organizational representatives, helps ensure appropriate protection of personally identifiable information of TIers, customers and business partners

If employees identify potential threats, or have questions or concerns about IT security, we have internal channels in place to assist them. Customers and suppliers also can contact us directly if needed through their account managers and other channels.