Keysight Security

Keysight's Commitment to Security in a Connected World

Technology is driving breakthroughs that help connect and secure the world, all while more efficiently managing business operations. However, faster communications, connected devices and integrated networks also open the door to vulnerabilities that can result in new, unintended security and privacy implications. Keysight is uniquely positioned to recognize the opportunities and challenges that these technologies offer to build a better planet.

Keysight solutions, which are developed with focus on product security, provide the tools needed to find and fix vulnerabilities in emerging technologies before they impact operations. This helps maintain end user safety, security and privacy.

From an operational perspective, Keysight is committed to conducting business with integrity. Ethical governance is at the core of our operations. We have programs, policies and procedures designed to:

- Respect the privacy and personal data protection of our stakeholders
- Support company site and employee safety and security
- Manage security risk impacts to business continuity
- Meet compliance requirements worldwide

Keysight's Approach to Security Management

Keysight's security approach includes the following risk mitigation controls:

- Security Programs – Product, Borderless Information, Government, Physical and Site, and Supply Chain security programs, along with Data Privacy and Enterprise Risk Management programs together provide end-to-end management of the company's security commitments.
- Supporting Information Management Systems – Security policies, regulatory, and compliance are documented across supporting information management systems, as noted below, providing a strong governance structure that ensures Keysight meets all applicable laws, certification requirements and accreditations including:
  - ISO 27001:2013 Certification for Information Security Management System (ISMS)
  - UK Cyber Essentials PLUS Certification
  - PCI-DSS Certification
  - Enterprise-wide information security policies based on the NIST SP800-171 framework
- Business Management System; ISO9001:2015, AS9100D:2016, ISO/IEC17025
- Environmental Occupational Health & Safety Management System; ISO14001:2015

KEYSIGHT TECHNOLOGIES

Keysight Product & Solution Security

Keysight's Product and Solution Security Program is focused on the cybersecurity of all our company's products and solutions through:

- Processes and tools that support vulnerability management;
- Standards for secure product and solution definition, development, manufacturing and support; and
- Adoption of secure design principles and coding practices across product development

See Keysight Product & Solution Cyber Security information on www.keysight.com to learn more.

Information Security Program

Keysight's Borderless Information Security Program applies a risk-based approach that has foundations in industry standards and best practices. Our information- and cyber- security operations and procedures include a comprehensive ISMS framework inclusive of all legal, physical and technical controls involved in the organization's information risk management processes. This ensures Keysight maintains the confidentiality, integrity, and availability of information and systems in our environment. We continuously invest in our people, processes, and tools to strengthen our security posture to protect both Keysight and stakeholder data.

A dedicated Information Security and Compliance (ISC) organization owns and operates Keysight's ISMS and reports directly to the company's Chief Information Security Officer (CISO). The program includes functions such as:

- Information Security Policy Management
- Risk Management
- Vulnerability Management
- Compliance Assurance
- Identity and Access Management
- Incident Management
- Security Awareness and Education
- IT Disaster Recovery

See Keysight's Borderless Information Security Program to learn more.

Government Security Controls

Keysight's Government Security Program ensures the company is compliant with U.S. Government and Department of Defense (DoD) directives, regulations and public laws pertaining to the protection and safeguarding of U.S. national defense information under the National Industrial Security Program (NISP). As part of that program, Keysight has strategically-located secure facilities to accommodate the direct needs of the DoD and Intelligence Community elements and has an appropriate level of employees with security clearance at all levels to work in this environment. For non-U.S. regions, Keysight also maintains the appropriate levels of data protection and physical security on an as-needed basis.

Government Property Control Plan Overview

The Keysight property control management system is comprised of processes, procedures, records, and methodologies for effective and efficient control of Government property, including:

- Reports of discrepancies
- Loss of Government property
- Physical inventory results
- Audit and self-assessments
- Corrective actions
- Other property-related reports

Supply Chain Security

Suppliers play an important role in our success, and as such we require them to conduct business as Keysight does – with uncompromising integrity and according to high standards of business ethics. This includes the areas of safety and security where we employ several programs that include counterfeit parts and components, conflict mineral sourcing, and trade compliance policies.

See Keysight Responsible Sourcing information on www.keysight.com to learn more.

Counterfeit Parts Prevention Program

Keysight is committed to preventing the introduction of counterfeit electronic components into our products. We have a company-wide Counterfeit Electronic Parts Avoidance and Response System in place, “Keysight Counterfeit Materials Management Program,” which includes policies and processes to actively avoid and mitigate the potential impact of counterfeit parts.

To help prevent counterfeit components and parts, we:

- Use only electronic components that are manufactured by or for original component manufacturers
- Inform our suppliers of this policy and hold suppliers accountable for compliance
- Maintain appropriate processes and provide ongoing training to Keysight employees to assure electronic component authenticity
- Investigate all incidents of suspected counterfeit electronic components reported to Keysight’s supply chain management
- Maintain appropriate processes to isolate, quarantine and remove counterfeit electronic components from Keysight’s supply chain, and make appropriate disclosures to the proper authorities

See the Counterfeit Parts Prevention Program Overview document to learn more.

Conflict Minerals

As part of doing business with uncompromising integrity, Keysight is committed to promoting human rights within the company's sphere of influence, as set forth in Keysight's Standards of Business Conduct and Human Rights and Labour Policy. Consistent with this mission, Keysight also remains committed to the responsible sourcing of conflict minerals and will continue to comply with governmental rules and regulations relating to conflict minerals.

Keysight is committed to complying with the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank Act") and has implemented policies and practices to ensure compliance. Keysight also requires that all Keysight-identified supply-chain partners be in compliance with the conflict minerals requirements of the Dodd-Frank Act and the SEC. See the Conflict Minerals Report, Conflict Minerals Statement, or Statement on Responsible Cobalt Sourcing documents to learn more.

Customs-Trade Partnership Against Terrorism (C-TPAT)

The C-TPAT program is a joint industry/U.S. government initiative to strengthen and improve the security of companies' supply chains with respect to terrorism. Keysight is committed to participating in and supporting the C-TPAT program and requires all suppliers in connection with providing Goods and Services to KEYSIGHT, to be a C-TPAT member or a member in an approved Authorized Economic Operator (AEO) program with a Mutual Recognition Arrangement (MRA) with the United States (or an approved MRA), or have security measures in place that meet or exceed CTPAT's Minimum Security Criteria (MSC).

In addition, Keysight assesses our key U.S. importers and suppliers on their supply chain security control annually.

Physical and Site Security

Keysight utilizes a security management system to ensure appropriate facility controls, security programs, crisis management procedures and assessments are in place to protect customer assets, the company and employees worldwide.

Facility Controls

Keysight facilities provide a clear demarcation between public spaces and controlled access areas as well as adequate controls and operational access to entry points into all facilities. Electronic access control installations must meet the requirements of the Keysight Security Systems Standards and Guidelines. Additionally, all individuals are required to use their own Keysight-issued access devices or credentials.

Site/Regional Security Policy

Keysight Site/Region Security and Workplace Solutions (WPS) Management teams are accountable for the implementation and execution of all elements of this policy, as well as communicating specific business accountabilities to business managers.

Crisis Management, Communications and Disaster Recovery Planning

In any crisis it is expected that Keysight and its employees act in a manner that maintains the company's long-term integrity, reaffirms corporate values, and reinforces a positive public perception.

The priority of disaster recovery planning efforts corresponds with the urgency of critical business functions. As such, following a disaster, Keysight's building systems and business functions may not necessarily be resumed in a "business as usual" manner all at once. The realities of an event may dictate that certain systems resume at a degraded level, or that business functions are performed in a modified manner.

Keysight has established communication protocols for relaying pertinent information to internal company contacts in any case of a critical or high interest environmental, health and/or safety (EHS) event, or other select events with potential for business interruption. These protocols allow for efficient and timely reporting to internal contacts and preparation of external communications as necessary. They also serve as a mechanism for recording and communicating past lessons learned.

Travel Health and Security

Individuals who travel internationally for Keysight, whether experienced or novice, are provided information about the destination they are visiting. Depending on the individual employee's circumstances and current country conditions, the planning required prior to departure may vary considerably.

Keysight travelers are required to use a company-authorized travel agent when arranging business travel to ensure their itinerary can be located rapidly in case of an emergency. In addition, Keysight Security regularly provides all company-authorized travel agents important safety and security information that will assist them in arranging travel details while keeping employee safety and security in mind.

Data Privacy

One of Keysight’s most valuable assets is the goodwill it maintains with employees, customers and third parties with whom we do business, and thus are committed to the responsible collection, storage, use, transfer and disposal of their personal data. We follow applicable privacy and data protection laws wherever we do business, and respect individuals’ rights to privacy when it comes to their personal data. Our Global Data Privacy Policy applies to all Keysight legal entities worldwide owned directly or indirectly by the company, and our Customer Privacy Statement is posted publicly for transparency on how the company handles personal data.

Keysight Global Data Privacy Policy

The Keysight Global Data Privacy Policy details enterprise-wide requirements for processing personal data with a commitment to comply with:

- The laws and regulations of each country where Keysight conducts business, including specifically the European Union’s General Data Protection Regulation (2016/679/EU) (“GDPR”);
- Keysight’s Standards of Business Conduct; and
- Keysight’s policies and procedures designed to meet data privacy legal and regulatory standards

This policy defines how Keysight processes personal data in accordance with the following principles:

- Lawfulness/Fairness/Transparency
- Purpose Limitation
- Data Minimization
- Accuracy
- Storage Limitation
- Integrity and Confidentiality
- Accountability

Employees who handle personal data as part of their work are expected to be familiar with these principles and abide by them and this policy whenever processing personal data. In addition, Keysight maintains appropriate technical and organizational measures to protect personal data from unauthorized use or disclosure, and take swift, deliberate action to investigate and remedy any potential data breach.

Customer Privacy Statement

Customer success is at the heart of everything we do at Keysight. One of the ways we help honor our customer relationships is by ensuring that we respect and protect their personal data privacy, and that we are transparent in how we do so. As such, our publicly available Customer Privacy Statement provides a clear and prominent explanation of how Keysight collects, uses, shares and protects customer personal data.

See the Keysight Customer Privacy Statement to learn more.

Supplier Privacy Statement

Through business with Keysight, suppliers may receive personal data belonging to Keysight employees or other third parties. Suppliers shall comply with the terms of any data privacy agreement or addendum with Keysight. With this, Keysight has established a Supplier Privacy Statement which provides a clear and prominent explanation of how Keysight collects, uses, shares and protects their personal data.

See the Keysight Supplier Privacy Statement to learn more.

Enterprise Risk Management

Keysight continuously monitors ongoing risks associated with maintaining business continuity, developing mitigation plans, and implementing to such plans as needed. Specific plans have been developed by organization and are periodically tested through table-top or simulated environments for effectiveness, as well as to address other unplanned crises that could result in business interruption.

The Keysight Business Continuity Program addresses specific threats including:

- Pandemic
- Loss of a critical site
- Loss of a critical data center
- To ensure continued delivery of Keysight products and services

Keysight Security Resources

- Keysight's Borderless Information Security Program
- Computer Virus Control Policy
- Computer Virus Control Program
- Supplier Code of Conduct
- Supplier Privacy Statement
- Keysight Technologies Customer Privacy Statement
- Keysight Business Continuity Program

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at:
www.keysight.com/find/contactus