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, CIS Controls Compliance, and Data Privacy and Enterprise Risk Management programs 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
  - TISAX ENX Association
- 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

Keysight Product & Solution Security

Keysight's Product and Solution Security Program is focused on the cybersecurity of 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
- 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
- Comprehensive Security Governance
- Risk Management
- Vulnerability Management
- Compliance Assurance
- Identity and Access Management
- Incident Management and Response
- Security Awareness and Education
- IT Contingency Planning (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 Defense Counterintelligence and Security Agency (DCSA) 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 DCSA 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.

DoD security clearance

All requests for information regarding Facility Clearances (FCLs) and Personnel Clearances (PCLs) will be reviewed and processed on an individual and as needed basis."

Government property control plan overview

The Keysight Government Property Control Plan can be found on Keysight's Quality & Security Resources webpage.

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 prevention conflict mineral sourcing, trade compliance policies, and industry-leading cybersecurity controls for our supply chain.

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. Keysight has a companywide Keysight Counterfeit Materials Management Program (CMMP) and Keysight Counterfeit Electronic Components Prevention Policy, which outlines the requirements and processes to actively avoid and mitigate the potential impact of counterfeit components. These counterfeit prevention controls include, implement procurement protocol to source the authentic electronics component, maintain appropriate detection processes to assure electronics component is authentic, deploy training programs for employee's awareness about the risk of counterfeit, and establish disposition and reporting process for all cases of suspected counterfeit components found across Keysight's supply

chain, conduct audit to verify out adherence to the policy, and continued creating the counterfeit awareness across the organization. In addition, we also defined the supplier requirements such as, supplier shall obtain a written consent and approval from Keysight prior the procure of electronic components from the non-authorized sources, and prior the use of the electronic components on our products. Suppliers shall adhere to the requirements and ensure their supplied parts, components, materials, and products that are incorporated into Keysight products are authentic, safe, and connected across the supply chain.

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 Labor Policy. Consistent with this mission, we established the Keysight Conflict Minerals Statement, 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 Section 1502 of the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank Act") and requires that all suppliers adhere to these requirements as outlined in our Supplier Code of Conduct. We expect suppliers to supply materials that are "DRC Conflict Free" and do not contain minerals that directly or indirectly finance or benefit armed groups in the Democratic Republic of the Congo or an adjoining country.

Keysight is a participant of the Responsible Mineral Initiative (RMI), and our sourcing of minerals is in accordance with the Organization for Economic Co-Operation and Development (OECD) Guidance. We utilize RMI tools and resources that support mineral sourcing, including the Responsible Minerals Assurance Process (RMAP) validation audit of smelters and refiners, and the Conflict Mineral Reporting Template (CMRT). We engage a third-party consultant to collect CMRT responses from our suppliers and work closely with our suppliers to meet responsible sourcing goals. We publish the SEC annual disclosure reports and a due diligence plan concerning conflict minerals, which is accessible on our company website.

Our conflict minerals due diligence process includes the five steps as defined by the OECD Guidance:

1. Establishing strong company management systems
2. Identifying and assessing risks in our supply chain
3. Designing and implementing a strategy to respond to identified risks
4. Utilizing independent third-party audits
5. Publicly reporting on our supply chain due diligence

In addition, we also participate in the Cobalt Initiative and work closely with our suppliers to meet responsible sourcing goals. The Extended Minerals Reporting Template (EMRT) is used to collect the cobalt sourcing information within our supply chain. Refer to Keysight Statement on Responsible Cobalt Sourcing for more details.

Additional information is available at Keysight Conflict Minerals Report.

Customs-Trade Partnership Against Terrorism (C-TPAT)

Keysight is committed to participating in and supporting the Customs – Trade Partnership Against Terrorism (C-TPAT) program. As a strong advocate of the C-TPAT program, Keysight 's goals are to enhance and maintain effective security processes throughout the global supply chain, and to ensure the timely delivery of all incoming cargo. Keysight urges each of our US suppliers to join C-TPAT. In addition, US Customs expects non-US suppliers to implement appropriate security measures to secure their goods throughout their international supply chains. Accordingly, Keysight expects each of our suppliers of goods or services to notify their plants, offices, and subsidiaries of the C-TPAT program and of Keysight's participation.

Cyber supply chain risk management

At Keysight, we are committed to assuring that the instruments manufactured, refurbished, serviced, calibrated, and demoed by Keysight are free of malware and other computer-based threats. We expect our supplier to comply with all applicable Data Protection Laws and only access Keysight's data and systems to fulfill its obligations under the Agreement or as explicitly directed by Keysight. Additionally, Suppliers shall establish an Information and System Security program that adheres to Keysight's Supplier Cybersecurity Control Guidelines.

When requested by Keysight, Suppliers shall demonstrate compliance with this requirement by completing the cybersecurity questionnaire to provide us a better understanding of your cybersecurity control level and risks to Keysight.

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 Global Security Policy and Security Systems Standards and Guidelines. Additionally, all individuals are required to use their own Keysight-issued access devices or credentials.

Keysight facilities controls also include the following:

- Surveillance - Keysight continuously evaluates the CCTV/surveillance/security camera technology available on the market and makes updates as necessary or as deemed appropriate.
- Security Guards - Keysight utilizes guard services in conjunction with electric security and is based on industry standards.
- Badge Access - Keysight continuously evaluates the security systems to ensure the safety of employees, Intellectual Property, and physical property are secured appropriately.
- Site Access Permissions - Site permissions are evaluated regularly to ensure the safety of employees, Intellectual Property, and physical property are secured appropriately.
- Access Logs - Access logs and records are considered confidential and proprietary, and are reviewed on an as-needed basis under strict controls.
- Data Center Controls - Controls are set up based on industry standards are considered confidential and proprietary.
- Asset Management - Movement of company assets and equipment are monitored and tracked in accordance with policies and procedures.
- Secure Data Storage - Controls are setup based on industry standards are considered confidential and proprietary.

Personnel security

Keysight's Standards of Business Conduct (SBC) requires that business be conducted with honesty and integrity, and the highest ethical standards. The SBC establishes clear ethical guidelines for how we do business and establishes accountability at all levels of the organization. All employees complete SBC training as part of onboarding and then take an annual refresher course. All employees must comply with the SBC.

Keysight's personnel security policies apply to all Keysight workers, regular employees and contractors, who have access to Keysight's internal information systems. All workers are required to acknowledge and follow our policies. Before being granted system access, each worker must pass a background check, accept terms of confidentiality, and participate in SBC and security training. Access to Keysight systems is revoked in a timely manner when a worker is terminated, or the tenure ends.

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.

Keysight Technologies and its employees have experienced impacts due to wildfires. In response, Keysight has developed and implemented a Wildfire Management Plan establishing a team responsible for providing situation updates, facilitating outreach for potentially impacted employees, coordinating assistance for potentially impacted employees, and developing and distributing employee communications. Situation updates are used by the local crisis management team to determine site responses up to and including site evacuations.

Travel health and security

Individuals who travel domestically/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 we are committed to the responsible collection, storage, use, transmission, 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 customer 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 the European Union's General Data Protection Regulation (2016/679/EU) ("GDPR")
- Keysight's Standards of Business Conduct
- 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 to 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. In addition, Keysight has established a Supplier Privacy Statement which provides a clear and prominent explanation of how Keysight collects, uses, shares, and protects supplier 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

Crisis Management Keysight's Business Continuity and Response to Crisis Events

Additional Resources

- Keysight Quality and Security
- Keysight Borderless Information Security Program
- Keysight Information Security Policies Overview
- Keysight Security and ISO Certifications
- Report a Product Cybersecurity Issue
- Report an Enterprise Cybersecurity Issue
- Keysight Computer Virus Control Policy
- Keysight Computer Virus Control Program
- Keysight Supply Chain Security
- Keysight Supplier Privacy Statement
- Keysight Customer Privacy Statement
- Keysight Crisis Management and Business Continuity Program

For additional questions, please contact Keysight.