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 commercial 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:

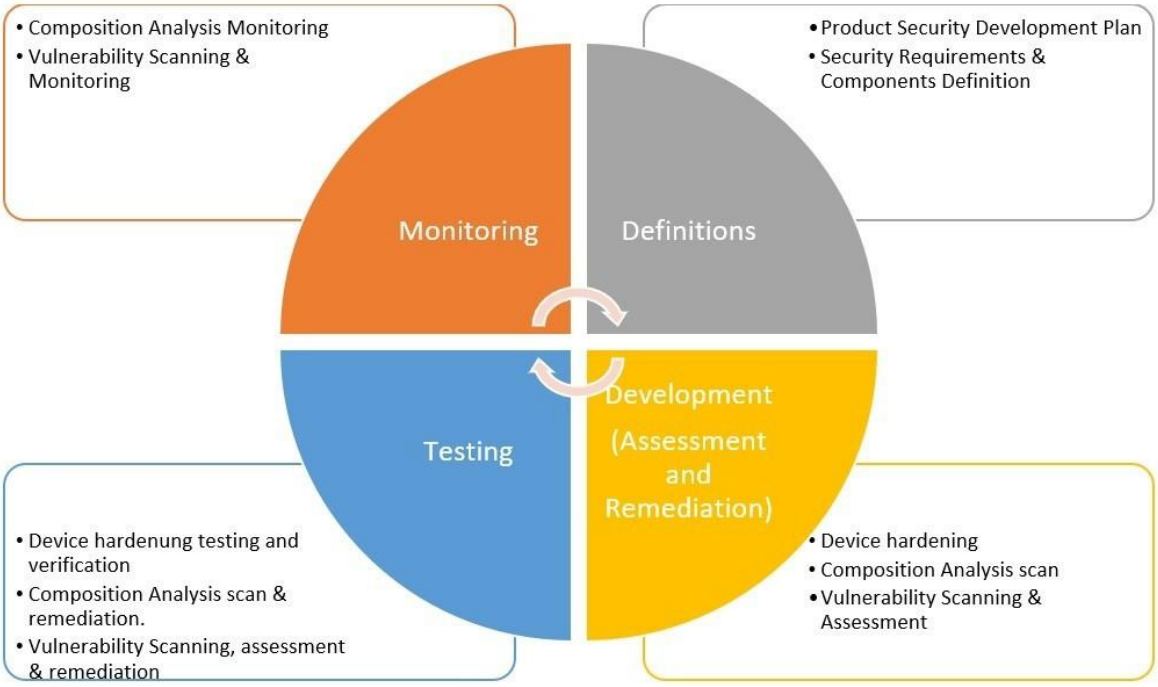
- Adoption of secure design principles and coding practices across product development. See Keysight Product & Solution Cyber Security information on www.keysight.com to learn more.
- Following the NIST SP800-218 – Secure Software Development Framework to mitigate the risk of software vulnerabilities.
- Establishment of the Keysight Product Lifecycle (KLC) which is used as the framework to structure a project for the development of a product or solution.

Keysight has developed a standard product lifecycle framework to ensure that Keysight develops products that repeatably meet the functionality, quality, and security needs of our customers. The KLC Process spans the entire life of all our products and services. It has fully integrated both scientific and comprehensive business practices that ensure robust solutions that exceed performance levels of competitive solutions. The KLC is adaptable to meet the varying needs of projects, and it is robust and flexible enough to enable its use for all product developments in Keusight.

The product lifecycle covers cross-functional efforts involving many departments, including Product Planning, Development and Marketing, Customer Support, Procurement, Manufacturing Engineering, Production, Quality, Finance, Learning Products & Organization Management.

Implementing product security

A typical product development lifecycle is divided into 4 different phases namely: definition, development, testing and monitoring



The Keysight Product Lifecycle (KLC) specifies that a Product Security Development Plan (PSDP) is required at the definition phase of the project. The PSDP provides a framework for the project manager and their team to ensure the adoption of secure product development methodologies throughout the development lifecycle as well as the implementation of required Security Features and Controls. The methodology is designed to complement Keysight's KLC processes and provide guidance to facilitate cybersecurity risk management. To effectively identify, protect, detect, response and recover, must be performed concurrently and continuously, as advocated in the National Institute of Standards and Technology (NIST) Cybersecurity framework.

Development, test, and production environments

Keysight's product development process require that the development environment, test environment, and the production environment are in separated networks with appropriate separation of duties and role-based access controls. These environments are secured by using secure systems with hardened configurations. These systems are also running the latest anti-malware programs with up-to-date intelligence feeds. Only software that is needed to carry out the tasks of developing the product are allowed into each environment.

Product vulnerability management

Keysight's Product Security team has developed an in-house, web-based Vulnerability Management Tool (VMT) to help product developers perform vulnerability assessments of Keysight developed products. It utilizes backend vulnerability scanning engines that are commonly used in the industry. The VMT also integrates with our Keysight issue tracking system. The tool allows teams to identify, track and mitigate vulnerabilities that they find in their products. The results are also made available to business managers and used to validate conformance during the KLC checkpoint sign-off.

Threat modelling is carried out by individual product development team to identify areas within a product that could be exposed to attack and define methods of protecting them from possible threats. The VMT assesses the level of security risk inherent in the product and provides recommendations for the most appropriate mitigation of identified vulnerabilities. Factors that are considered include whether the product is used in environments containing sensitive information, implementation of security controls in the product, and the potential impact of a security breach resulting from the exploitation of any known or unknown product vulnerabilities.

Software composition analysis

Keysight uses and industry recognized commercial software product to perform software (SW) composition analysis on the SW that we ship to our customers. This allows the development team to assess the security risks of known vulnerabilities in third party SW components used in the product and mitigate as appropriate. This process also supplies us with the ability to monitor and track open-source usage within our product development.

Secure hardening

Most operating systems (OS) come with default configurations that are not secured for our product's application environment. Guided by industry standards, Keysight has developed secure hardening requirements which improve the security profile of a product through various methodologies like closing of unused ports and services (disabling of debug services or vulnerable OS services), or improved authentication schemes used to access the product, implement firewall schemes, etc. The basic security controls implemented include access controls, principles of least privilege, default secure settings, hardened server settings and secure communications. The approach taken in designing hardening controls is similar to common best practices found in the industry, like the Center of Internet Security (CIS) hardening guides and the Defense Information Systems Agency's Security Technical Implementation Guide (DISA STIG).

Cryptography

Sensitive data, including credentials, API keys, cryptographic keys, and all other sensitive data must be encrypted and stored in a secure location outside of the source code repositories. Keysight uses a 'secrets' vault to securely store this information.

Software supply chain security

The processes defined in the KLC help provide software supply chain security by ensuring that Keysight produces robust software that is free from trapdoors, backdoors, viruses, or other undocumented behaviors. Keysight IT security policies require endpoint protection, including antivirus, centrally controlled identity and access management, etc. to protect Keysight intellectual property and the software that we deploy to our customers. The KLC and IT security policies are designed to ensure that our product development activities align with NIST SP800-218 Secure Software Development Framework recommendations. Our focus on secure design, development, and vulnerability management help to reduce the risk that a vulnerability may accidentally be introduced during product development. These practices provide a high level of assurance that our software is safe to use.

Product security awareness training

To emphasize the importance of designing for security, the PDSP recommends that appropriate development team members take two in-house developed courses focused on the fundamentals of secure design and development:

- Secure Design Principles
- Secure Development/Coding Practices

These trainings are developed based on Open Web Application Security Project's (OWASP) 10 secure design principles and 14 secure coding practices respectively. They are technology agnostic and are adapted to be applicable for use in a wide variety of application spaces used in Keysight products and solutions. They provide guiding principles that emphasize how secure design principles, security tactics and patterns are to be incorporated as early as possible in the product development lifecycle.

Vulnerability discovery

After a Keysight product is shipped, it is recommended that the product development team carry out the following up activities:

- VMT scanning of shipping products should be performed regularly (e.g., every 6 weeks).
- Important OS security patches or releases should be applied.
- Review composition analysis notifications of newly found vulnerabilities and evaluate mitigation options.
- Review of any updated version of our Secure Hardening Standard or security requirements and consider the need for updates.
- Monitor industry cybersecurity incidents that may affect the product.

Cybersecurity incident monitoring and response

Keysight also maintains a product security response process that is utilized when new vulnerabilities or exploits are discovered that can impact our products and solutions. We also maintain a Product Security page providing:

- Information regarding security advisories for Keysight products.
- Information to help customers use our products securely.
- Information to assist Aerospace Defense customers using Keysight products in secure environments.

Security incident/vulnerability reporting

Customers can contact Keysight to report a Keysight product or solution that has been impacted by a cyber security issue by sending an email with the details of the issue to productsecurity@keysight.com, or by visiting Keysight's Report a Product Cybersecurity Issue page.

Keysight recognizes the importance of documenting memory types and sanitization procedures for many of our products. Documents of Volatility (aka Letters of Volatility) can be found on the Keysight Instrument Security page.

Borderless Information Security Program

Keysight Technologies information security program applies a risk-based approach that has foundations in industry standards and best practices. Our information security teams facilitate a comprehensive Information Security Management System (ISMS) to maintain the confidentiality, integrity, and availability of information and systems in our environment. Information security is an important priority, and we continuously invest in our People, Processes, and Techniques to strengthen our security posture to protect both Keysight's data and our customer's data.

Keysight is ISO27001, UK Cyber Essential Plus, and PCI-DSS certified. Keysight Information Security Policies are based on NIST SP 800-171 and apply to the entire Enterprise.

Keysight has a borderless, enterprise-wide approach to information security and has a dedicated Information Security and Compliance organization (ISC) that owns and operates the information security management system. The ISC organization reports directly to Keysight's Chief Information Security Officer (CISO) and includes functions such as:

1. Information Security Policy Management
2. Risk Management
3. Vulnerability Management
4. Compliance Assurance
5. Identify and Access Management
6. Incident Management
7. Security Awareness and Education
8. IT Disaster Recovery

Keysight's Borderless Information Security Program focuses on the following domains:

Risk management and compliance

Keysight uses robust programs and processes to make informed decisions about remediating, mitigating, or accepting risks to assist the organization in securely achieving its objectives.

Keysight adheres to mandated laws and regulations, customer compliance requirements, and our organizations' policies, procedures, and processes.

Risk management

Keysight's risk management program is used to assess, document, monitor, and report risk. Risk exposure, avoidance, mitigation, and acceptance are analyzed, documented, and reviewed.

Information security review

The ISR process assesses the risk to Keysight systems and information by analyzing the likelihood and impact of harmful events. It delivers recommendations for reducing the risk involved in activities and processes so that they can be executed more safely and confidently.

Compliance assurance

Keysight has operations worldwide and is subject to a variety of regulatory requirements, including SOX, DFARS, GDPR, HIPAA, and PCI-DSS, ensuring that we implement a strategic plan to ensure compliance.

Independent assessments

Approved third party companies are used for ensuring regulatory compliance, control performance validation, penetration testing, and impartial risk assessments.

Vulnerability management

The vulnerability management team provides insight on current trends and events within the information security community. This visibility is used to proactively protect our environment. The vulnerability management team follows patching and remediation procedures according to best practice timelines.

Customer compliance

Keysight receives and responds to our customers' security and compliance inquiries. Where applicable this input is taken into consideration for future policies or controls.

Third party risk

Third party partners with access to Keysight's network and information or that supply Keysight with managed services present additional risk that needs to be evaluated and controlled. Keysight has processes and procedures in place to constantly review and evaluate third party risk.

Supply chain risk management

Keysight monitors its suppliers' information security via the supply chain risk management program which includes supplier audits and independent monitoring of suppliers' information security posture.

Third party access

Third party access to Keysight's networks is catalogued and reviewed. Third parties' access is granted on the principle of least privilege, and regularly reviewed.

Supplier audits

Keysight's Internal Audit organization performs independent audits to help to identify potential control weaknesses, compliance concerns or operational inefficiencies in suppliers' operation and Keysight IT's oversight and governance processes.

Organizational governance, training and awareness

Organizational governance activities ensure that critical management information reaching the stakeholders is complete, accurate and timely to enable appropriate management decision making, and provide the control mechanisms to ensure that strategies, directions, and instructions from management are carried out systematically and effectively.

Information security and compliance

Organizational meetings are held to discuss and inform management, stakeholders, and employees of strategies and direction. These meetings include areas from all functions in the organization to provide alignment and awareness.

Performance metrics

Metrics on the performance, availability, and health of Keysight's IT environment are reviewed every month by top management and representatives from all operational areas of IT and other stakeholders.

Change management process

Controls are in place to ensure that changes in production environments are deployed in a controlled fashion, and are documented, tested, and approved prior to deployment.

Security awareness education

Continuous training programs are required to be completed by employees worldwide. These programs cover security, Standards of Business Conduct, and compliance. Additionally, there are enterprise-wide phishing simulation tests and function/role-based trainings as required.

Training

Keysight encourages and supports employee's continual development and education through investing in external training and certifications relevant to their scope of work.

Information security policy management

Keysight has structured Information Security Policies that are reviewed at least annually and updated as needed. The policies are based off NIST SP 800-171.

Security tools optimization

Security tools are critical for Keysight to predict, protect, and respond to potential risks and threats to the data and systems in our environment. Advanced persistent threats and zero-day vulnerabilities require constant monitoring by automated technologies combined with human oversight.

Network

Keysight uses firewalls, intrusion detection systems, intrusion prevention systems, and web content filtering protections for traffic traversing ingress/egress points with non-Keysight networks. Keysight uses separated zones to limit access to network resources. Internet facing systems are placed in a DMZ and the applications are further protected behind a web application firewall. Additionally, Keysight uses 802.1x to validate devices that are trying to connect to Keysight's network.

Systems

Up to date antivirus and malware detection tools are maintained on all endpoints. Scans are configured to be performed on access as well as full system scans. Full disk encryption is used as appropriate. System hardening is performed on workstations, servers, network equipment, and mobile devices. This hardening is performed by restricting administrative rights, disabling unneeded and potentially insecure services, removing default passwords, disabling auto-run, and applying Keysight's security configuration.

Security information and event management

Keysight utilizes a SIEM to process logs and events. The SIEM correlates input from across the Keysight network and creates alerts when suspicious behavior is detected.

Email protections

Phishing remains one of the more popular ways that bad actors try to gain access to protected networks. Keysight has deployed tools and services for enhanced email security to protect against phishing attacks and to reduce spam, bulk, and other unwanted emails. The email protections include SPF, DMARC, and DKIM. Email communication is encrypted.

Privileged account management

Keysight has PAM tools that enable the securing, control, managing, and monitoring of privileged access to its critical assets.

Data protection and assessment management

To protect Keysight's data and assets, Keysight keeps an up-to- date inventory of assets and employs many layers of controls to ensure the confidentiality, integrity, and availability of its information.

Identity and access management

Identities are securely managed with robust account provisioning and deprovisioning processes. Access controls include multi- factor authentication, the application of the principle of least privilege, and periodic privileged account reviews. Third parties are vetted, and their access is periodically reviewed.

Cloud security

Keysight has a cloud security policy which references a robust cloud security architecture, with processes and procedures that define secure methods for operating in shared security responsibility models.

Mobile device management

All Keysight mobile devices on the company network that access Keysight systems or information have their configurations controlled and use encryption.

Encryption

Encryption is used where required and includes information in motion and at rest. Encryption methods use the current best practices with regards to the encryption protocols, algorithms, and strength used.

Database activity monitoring

A database activity monitoring tool is used to independently monitor and audit database activity. This ensures that Keysight can identify and report fraudulent or other undesirable database activity.

Asset management

Inventory of assets are kept in our enterprise databases. This inventory includes details of the asset including the configuration, software installed and running, and the owner.

Media disposal

Keysight uses advanced techniques for data destruction and has policies that require all media to be sanitized before it is disposed of, re-purposed, or when no longer in use.

IT disaster recovery

Disaster recovery plans and processes are documented, tested, and reviewed. The disaster recovery site is geographically separated from the enterprise data center.

Backup

Backups are in place and configured with a backup frequency that is applicable to the information being backed up. Keysight tests backups on a periodic basis to ensure they can be correctly restored.

Security operations

Keysight has processes in place for detection, prompt action, and responses to potential attacks, breaches, or disruptions to reduce the impact on the confidentiality, integrity, and availability of the environment. Keysight focuses on the people and process that allow us to respond appropriately.

Security operations center

Keysight operates an in-house dedicated 24x7 Security Operations Center with human and machine monitoring for potential IT security events.

IT operations

Keysight has IT support operations teams which monitor the health of the IT environment 24x7. This includes real-time network monitoring.

Event correlation

A SIEM (Security Information and Event Management) is used for monitoring and performing correlations across the entire Keysight network to identify, report, and alert on security events and anom.

Incident response team

This dedicated team leads the investigation into security related events. The security related events come from many different sources including the SOC (Security Operations Center), IT Operations, Employees, Management, and Customers.

Incident response plan

Keysight has a documented security incident response plan that defines roles and responsibilities. This plan includes processes and procedures for responding to incidents, including the necessary communication channels and sequences.

Incident management

Keysight has IT support teams to address non-security related incidents and events, to ensure a robust environment, and to maintain availability and integrity of the systems and data.

Communications

Processes are in place to notify impacted stakeholders during and after a reportable event.

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

See Keysight's Quality & Security Resources webpage for the Keysight Government Property Control Plan.

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 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 mineral, 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 rep
6. Sorting 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 a better understanding of 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 all facility entry points. 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 Keysight-issued access device or credentials.

Keysight facilities controls also include the following:

- Surveillance – Keysight continuously evaluates 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 controls also include the following:

- Security Policies – 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.
- System Access – 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.
- Visitors – Visitors to Keysight locations are required to sign-in and must present a Government ID to prove identity. All visitors are screened against global watch lists, and a Non-Disclosure Agreement must be acknowledged at the time of sign-in. A Temporary Visitor Badge is issued to visitors with a unique color of the badge and lanyard for easy identification. A Keysight host must always escort the visitor while in non-public areas of the Keysight facility. Visitor logs are electronically maintained in accordance with Keysight Records Retention policy.

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 employees have experienced impacts due to wildfires. In response, Keysight has 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 Privacy
- Keysight Information Security Policies Overview
- Keysight Security and ISO Certifications
- ISO 27001 Certificate
- UK Cyber Essential PLUS
- PCI-DSS Certificate
- 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.