Creating a More Connected and Secure World

Peace of Mind: Internally Secure

As you leverage Keysight solutions to improve the connectivity and security of your technical pursuits, we also bring the peace of mind that comes from knowing your valuable data is safe and secure within our internal systems. The following information will help you understand our dedication to security, the methods we use, and our commitment to protecting your data.

Organized for Security

Keysight has created an effective security program, designed to foster high confidence in our storage, processing, and transmission of customer data. Our security program adheres to NIST standards, follows best industry practices, and is regularly assessed by third parties.

People: The Foundation of Security

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 security training. Access to Keysight systems is revoked in a timely manner when a worker is terminated or the tenure ends.

Security and Awareness Training

In addition to initial training in privacy and security, all workers must complete annual refresher training. Workers must also acknowledge annually that they've read, understand, and will adhere to Keysight's information security policies. Workers who have roles with elevated access due to the nature of their responsibilities receive additional job-specific security training.

The Information Security Team

Keysight has established an Information Security Team with clearly defined roles for operating and managing the various aspects of our security program.

The head of that team is the Chief Information Security Officer (CISO), with top-level responsibility for the implementation and management of our security policies and procedures. The CISO is supported by the other members of the Information Security Team, who collectively possess a wealth of skills and experience in all facets of the security program.

The Information Security Team's responsibilities include security engineering and operations; incident response; architecture; and risk and compliance.

Keysight's Information Security Team actively follows community developments and discussions to keep abreast of emerging threats and maintain a high level of state-of-the-art knowledge. This, in turn, allows us to prepare strong defenses and react quickly should a security event occur.

Policies and Standards

Keysight maintains security policies and procedures that specify a wide range of operating rules for the Keysight environment. These documents provide assurance to our customers that our workers behave ethically and that our services operate securely. Our policies and procedures are reviewed regularly, updated when necessary, and made available to all workers.

Audit and Compliance

Keysight's information security program addresses all applicable security requirements and validates adherence through audits, security testing, and compliance analysis.

Audits

Keysight assesses its overall security environment for compliance with internal and external requirements, and engages certified third-party assessors to perform external audits at least annually. Audit results are presented to executive management, and all issues are resolved or mitigated. Keysight also has a dedicated internal audit organization that continually tests and monitors the environment.

Security Testing

Independent third parties are routinely engaged to conduct application and infrastructure assessments. Results of these assessments are shared with Keysight management. The Information Security Team reviews and prioritizes the findings and tracks the ensuing remediation.

Compliance Analysis

Keysight employs dedicated security compliance professionals who review projects, systems, and applications to ensure compliance with applicable legal and regulatory requirements.

Designed for Security

Keysight assesses the security risk of IT and business projects through the Information Security Review (ISR) process. to determine if there are potential security risks. This analysis results in assigning projects specific risk levels. Based on the analysis and assigned risk, a set of requirements is generated that must be met before the project or change can be implemented within the production environment.

Keeping Customer Data Safe

The primary objective of Keysight's security program is to prevent data compromise. To accomplish this, our security professionals take comprehensive measures to identify and mitigate risks, employ best practices, and continuously develop ways to improve.

Encrypting Data in Transit and at Rest

Keysight employs strong encryption any time data is transmitted over a public network, supporting the most current compatible protocols and encryption methods.

Sensitive data stored in our production environment is encrypted using current industry and government standards. Encryption keys are stored in a secure server with restricted access, are provided at process commencement, and are kept in memory only during use.

Keysight employs data centers that are either Keysight-owned, or maintained by top service providers. These data centers provide strong physical protection for the servers, infrastructure, and operating environment. Entry into the data centers to physically access Keysight systems is restricted to authorized personnel.

Data Availability

Keysight uses a combination of storage technologies to ensure customer data is segregated, protected from hardware failure, and is consistently available.

Securing the Network

Customer data is hosted either within Keysight's highly controlled production network, or by cloud-based, security-certified vendors. Administrative access to these production systems is limited to approved personnel with related job responsibilities.

Access to Keysight's production environment from the Internet is tightly restricted. Relatively few production servers are accessible from the internet, and then only through the fortress of the DMZ. Only those network protocols required to provide services to our users are open at Keysight's

perimeter, where we implement protections against external attacks. This protection includes Intrusion Detection Systems and Intrusion Prevention Systems (IDS/IPS) that are implemented using a combination of host-based and network-based controls. Changes to our production network must be approved through our rigorous change management process, and can be implemented only by authorized personnel.

Classifying and Handling Data

To maximize protection for the data we store and process, Keysight classifies data into various levels, each requiring specific labeling and handling. This includes both internal classifications and standard external classifications such as CDI (Covered Defense Information). Further, Keysight controls data flow to ensure that customer information can reside only within properly classified systems.

Access Authorization

To protect data from compromise, Keysight follows the principle of least privilege, allowing workers to access only data that is necessary for their job functions. To ensure these access limitations, all workers who access Keysight systems are given unique user IDs; and user accesses are reviewed periodically to validate continuing needs.

Upon hire, workers may be granted access to a limited number of internal systems such as employee-support utilities; however, requests for further accesses follow a documented process requiring business justification and management approval.

Authentication

For all systems, passwords are required to be complex and must embody several features, including minimum length, upper and lower case, special characters, etc. For systems with higher levels of classified data, Keysight further decreases the risk of unauthorized access by employing multi-factor authentication for administrative access to such systems.

System Monitoring, Logging, and Alerting

Keysight's Security Team utilizes a SIEM (Security Information and Event Manager) to collect and store security events for analysis. Access to the SIEM is restricted to members of the Security Team. Logs are protected from modification and retained for at least one year. Analysis of security events is performed through a combination of automation and human review to detect potential issues and alert responsible personnel.

Monitoring Endpoints

Keysight employ various monitoring tools to detect malware, unsafe configurations, or suspicious user behavior. Keysight's Security Team and IT Operations monitor alerts and coordinate issue resolution in a timely manner.

Managing Mobile Devices

To ensure Keysight's security standards are met, mobile devices used for company business are centrally managed via the appropriate mobile device management systems. These systems include the capabilities to track usage, encrypt data, enforce multifactor authentication, and, if necessary, remotely wipe mobile devices.

Response to Security Incidents

Keysight policies and procedures include directions for responding to possible security incidents. Keysight's dedicated Cybersecurity Incident Response Team manages all security incidents. Keysight defines and classifies the types of events that must be managed via the incident response process. Incident response procedures are tested at least annually and updated as required.

Disposing of Data and Media

Keysight follows industry standards and employs advanced techniques for data destruction, and has implemented policies requiring media to be properly sanitized before it is disposed of, re-purposed, or is no longer in use.

Securing Workstations

Keysight workstations are configured to comply with Keysight security standards. These standards require proper configuration, current system updates, monitoring software, and integration with Keysight endpoint management. Keysight's default configuration ensures that workstations have full-disk encryption, strong passwords, lock when idle, and run current monitoring software to report potential malware.

Controlling System Operations and Continuous Deployment

We employ various methods to protect against malicious programs and unauthorized access.

Detecting and Preventing Malicious Code

While Keysight employs rigorous change control methods for our systems, we also protect our production environment against the introduction of malicious code through various means

including inbound file checking, web application firewalls, advanced malware protection, and other state-of-the-art safeguards.

Controlling Change

To reduce the risk of data compromise, Keysight rigorously controls changes. Requirements are in place to ensure that changes are documented, tested, and approved prior to deployment.

Hardening Servers

Before deployment to production, new servers are hardened by disabling unneeded and potentially insecure services, removing default passwords, and applying Keysight's security configuration.

Ensuring Configuration Integrity

Keysight ensures that production servers have the proper configuration by frequently running a system that checks versions of key files. If this system detects unauthorized versions, it will overwrite those files with the correct version from a validated and protected storage area.

Disaster Recovery and Business Continuity

Keysight employs both local uninterruptible power systems and a geographically separate hosting location to ensure continuity of operations for critical systems. Keysight also employs data backup strategies for critical production applications to ensure the integrity of information should an outage occur. Keysight tests backups on a periodic basis to ensure they can be correctly restored.

Third-Party Suppliers

Keysight employs third-party sub-services to ensure that business runs efficiently. Where use of these services has the potential to impact security, Keysight takes measures to ensure that security is properly maintained. Keysight establishes agreements that require service organizations to follow the confidentiality commitments Keysight has made to its users. Keysight monitors the effective operation of the organization's safeguards by reviewing its service organization controls before implementation and at least annually thereafter.

Conclusion

Keysight takes security seriously, because all people and teams using our services expect their data to be secure and confidential. Safeguarding this data is a critical responsibility, and we work hard to accomplish this and to maintain the trust of our customers.