Keysight Technologies, Inc.
1400 Fountaingrove Parkway
Santa Rosa, California 95403
www.keysight.com

Last Updated: 03 July 2024

Keysight Technologies Information Security Policies Overview

This document outlines the standardized and documented indexes of the policies, procedures, and guidelines in place required to direct Keysight Technologies on how to protect its data, information, networks, hardware, software, users, and clients from potential security breaches through their use of the firm’s resources and services.

Keysight's Information Security Policies exist to ensure compliance with relevant laws and regulations, and to create a foundation for secure, consistent, and reliable IT operations.

Security policies guide Keysight businesses and IT partners in the inclusion of information security within their processes and programs. Adherence to these policies is the responsibility of every Keysight employee, contractor, and business partner.

It is extremely important that our existing and potential customers, as well as Keysight employees, understand that Keysight takes information security very seriously, and that protecting our customers' information is a responsibility we take to heart.

Keysight has structured Information Security Policies based on NIST SP 800-171. These policies are reviewed at least annually and applied enterprise wide.

KEYSIGHT

Table of Contents

KEYSIGHT

3.0 Data Classification and Handling Policy

Policy Statement

The proper classification and handling of information processed and stored by an information system is essential to the selection of security controls that must deployed to ensure the confidentiality, integrity, and availability of the system and its information. This policy provides direction for classifying data as Keysight-Restricted, Keysight Confidential, or Keysight-Private, and defines how data should be handled once it has been classified. This policy also provides direction for the identification, marking, and handling of Controlled Unclassified Information (CUI) and government-classified information.

Management must:

- Ensure that each business unit properly classifies, reclassifies as needed, and handles the information it owns in accordance with the information's security categorization.
- Implement effective security protocols to ensure that information is handled in accordance with Keysight's classification scheme.
- Limit access to Keysight Confidential and Keysight Private Information to those with a legitimate business purpose.

Applicability

This policy and supporting procedures are applicable to all Keysight business units. Owners of applications, databases, operating systems, infrastructures, and supporting IT functions are responsible for developing guidelines and procedures to support this policy.

Implementation

Implementation of this policy is defined by the following procedures:

- Security Categories
- Labeling and Marking
- Confidentiality and Encryption

3.1 Access Control Policy

Policy Statement

Access to Keysight Technologies systems must be limited to authorized users, and must follow the principles of Least Privilege, Non-Repudiation, and Segregation of Duties.

Management must ensure that:

- Privileges and application roles for new or modified accounts for active employees or contractors are properly approved by business management, and that a unique user ID is assigned to each user.
- Procedures have been implemented to ensure the timely disabling of terminated employee and contractor accounts.
- User access reviews are periodically conducted to validate proper segregation of duties and adherence to the principle of least privilege.
- The number of privileged accounts (e.g., DBA, sysadmin, etc.) is limited to what is functionally necessary, and that the accounts are appropriate to job responsibilities.
- All passwords comply with corporate policy unless not supported due to system limitations.
- Segregation of duties is employed to avoid assigning conflicting roles to an individual.

Applicability

This policy and supporting procedures are applicable to all Keysight business units. Owners of applications, databases, operating systems, infrastructures, and supporting IT functions are responsible for developing guidelines and procedures to support this policy.

Implementation

Implementation of this policy is defined by the following procedures:

- User Account Management
- Segregation of Duties (SOD)
- Privileged Accounts
- Remote Access
- Wireless Access
- Access Control for Mobile Device
- Publicly Available Information

3.2 Awareness and Training Policy

Policy Statement

Keysight employees on the Keysight Technologies Network must undergo security awareness training.

Management must ensure that:

- Users receive security awareness training as part of the initial onboarding process and annually thereafter.

Applicability

This policy and supporting procedures are applicable to all Keysight business units. Owners of applications, databases, operating systems, infrastructures, and supporting IT functions are responsible for developing guidelines and procedures to support this policy.

Implementation

Implementation of this policy is defined by the following procedures:

- Security Awareness Training

3.3 Audit and Accountability Policy

Policy Statement

Activity on the Keysight Technologies Information Systems must be monitored, recorded, and periodically reviewed to support after-the-fact investigations of security incidents.

Management must ensure that:

- Auditable events, including access to and modifications of sensitive or critical system resources, are logged, reviewed, retained, and protected.

Applicability

This policy and supporting procedures are applicable to all Keysight business units. Owners of applications, databases, operating systems, infrastructures, and supporting IT functions are responsible for developing guidelines and procedures to support this policy.

Implementation

Implementation of this policy is defined by the following procedures:

- Auditable Devices
- Content and Protection of Audit Records
- Audit Review, Analysis, and Reporting

3.4 Configuration Management Policy

Policy Statement

Keysight must ensure that only authorized configuration changes are implemented in Keysight systems. This includes establishing secure configuration baselines, maintaining a repository of current configuration information, and periodically verifying actual configuration information against baselines to identify potential unauthorized changes.

Management must ensure that:

- Baseline configurations are maintained for organizational information systems.
- Changes to the baseline configuration are properly reviewed and approved.
- Keysight systems are configured in accordance with the principle of least functionality.

Applicability

This policy and supporting procedures are applicable to all Keysight business units. Owners of applications, databases, operating systems, infrastructures, and supporting IT functions are responsible for developing guidelines and procedures to support this policy.

Implementation

Implementation of this policy is defined by the following procedures:

- Baseline Configuration
- Configuration Change Control
- Access Restrictions for Change
- Least Functionality
- Information System Component Inventory

3.5 Identification and Authentication Policy

Policy Statement

This policy restricts access to Keysight information systems to authorized users.

Management must ensure that:
The identity of users, processes, or devices, prior to granting them access to organizational information systems are authenticated.

Applicability

This policy and supporting procedures are applicable to all Keysight business units. Owners of applications, databases, operating systems, infrastructures, and supporting IT functions are responsible for developing guidelines and procedures to support this policy.

Implementation

Implementation of this policy is defined by the following procedures:

- Password Settings and Connection Requirements

KEYSIGHT

3.6 Incident Response Policy

Policy Statement

Keysight Technologies must maintain an incident response plan to react in a timely manner to security incidents to limit or mitigate potential adverse impacts to business. The plan must include the following elements:

- Detection, Assessment, and Triage
- Containment, Evidence Collection, Analysis and Investigation, and Mitigation
- Remediation, Recovery, and Post-Mortem analysis.

Management must:

- Implement a plan that documents specific steps to take in responding to security incidents in a timely manner. Security incidents can include theft, misuse of data, logical or physical intrusions, hostile probes, failure of security systems (e.g., anti-virus or firewalls), faults in information processing systems, and impacts of malicious software. The plan must address both external and internal threats.
- Define risk categories, procedures, escalation paths, and responsibilities to ensure a timely, effective, and orderly response to information security incidents. These procedures must include provisions for assessment, containment, recovery, and documentation of the security incident.
- Deploy a system for tracking and documenting security incidents and their resolution to communicate root causes, additional risk response requirements and process improvements to appropriate decision makers and to ensure that the cause, response requirements, and process improvement are included in the risk management processes.
- Ensure that all key stakeholders receive training appropriate to their assigned roles and responsibilities.
- Collect and retain evidence that in a manner that conforms to the rules of evidence defined by the relevant local jurisdiction(s), where follow-up legal action against a person or organization related to an information security incident may be required.
- Report incidents to appropriate internal and external stakeholders.

Applicability

This policy and supporting procedures are applicable to all Keysight business units. Owners of applications, databases, operating systems, infrastructures, and supporting IT functions are responsible for developing guidelines and procedures to support this policy.

Implementation

Implementation of this policy is defined by the following procedures:

- Incident Response Planning Procedure
- Incident Response Reporting Procedure

3.7 System Maintenance Policy

Policy Statement

Maintenance of Keysight Technologies information systems must be scheduled, monitored, and controlled by Keysight personnel.

Management must ensure that:

- All maintenance and repair activities on Keysight information systems are scheduled.
- All maintenance activities are approved and monitored, whether performed on-site or remotely.
- Equipment and systems that are taken off-site for maintenance or repair are sanitized (all non-public information is removed from storage media and memory caches) prior to removal from Keysight facilities.

Applicability

This policy and supporting procedures are applicable to all Keysight business units. Owners of applications, databases, operating systems, infrastructures, and supporting IT functions are responsible for developing guidelines and procedures to support this policy.

Implementation

Implementation of this policy is defined by the following procedures:

- Maintenance Control
- Maintenance Tools
- Off-Site Maintenance
- Maintenance Personnel

3.8 Media Protection Policy

Policy Statement

Keysight personnel must protect and control CUI, Keysight Confidential Information, and Keysight Private Information on removable media from unauthorized use or disclosure to comply with federal and local laws, executive orders, directives, and other governmental regulations as well as industry standards, guidance, and best practices.

Management must:

Implement procedures and technologies to ensure that media containing CUI, Keysight Confidential Information, and Keysight Private Information is protected from unauthorized use or disclosure throughout its lifecycle.

Applicability

This policy and supporting procedures are applicable to all Keysight business units. Owners of applications, databases, operating systems, infrastructures, and supporting IT functions are responsible for developing guidelines and procedures to support this policy.

Implementation

Implementation of this policy is defined by the following procedures:

- Media Protection

3.9 Personnel Security Policy

Policy Statement

Keysight Technologies must ensure that access to systems is granted only to authorized processes, user accounts, or programs, and is limited to the information and resources necessary to perform required functions and regular job responsibilities.

Management must:

- Limit access to information systems to those individuals with a legitimate business purpose.
- Implement procedures and technologies that would prevent or detect the unauthorized use or disclosure of CUI.

Applicability

This policy and supporting procedures are applicable to all Keysight business units. Owners of applications, databases, operating systems, infrastructures, and supporting IT functions are responsible for developing guidelines and procedures to support this policy.

Implementation

Implementation of this policy is defined by the following procedures:

- User Review
- User Terminations
- CUI User Intra-Company Transfers

KEYSIGHT

3.10 Physical Protection Policy

Policy Statement

Keysight Technologies must physically secure installations and buildings containing Keysight information systems.

Management must:

- Restrict physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
- Protect and monitor the physical facility and support infrastructure for those information systems that store or process Keysight information.

Applicability

This policy and supporting procedures are applicable to all Keysight business units. Owners of applications, databases, operating systems, infrastructures, and supporting IT functions are responsible for developing guidelines and procedures to support this policy.

Implementation

Implementation of this policy is defined by the following procedures:

- Data Center Security

3.11 Risk Assessment Policy

Policy Statement

Keysight Technologies will perform a risk assessment on the information technology environment to identify potential security issues and to use as the foundation of Keysight's risk mitigation strategy.

Management must:

- Assess risk, including the likelihood and impact of unauthorized access, use, disclosure, disruption, modification, or destruction of Keysight Technologies information systems.
- Disseminate risk assessment results to business units and system owners to use as the foundation of Keysight's risk mitigation strategy.
- Update the risk assessment annually or whenever there are significant changes to the information system or environment of operation, including the identification of new threats and vulnerabilities or other conditions that may impact the security of the system.

Applicability

This policy and supporting procedures are applicable to all Keysight business units. Owners of applications, databases, operating systems, infrastructures, and supporting IT functions are responsible for developing guidelines and procedures to support this policy.

Implementation

Implementation of this policy is defined by the following procedures:

- Risk Assessment

3.12 Security Assessment Policy

Policy Statement

Keysight Technologies will perform security assessments of information systems that process, store, or transmit CUI, financial data, and intellectual property.

Management must:

- Assess the security controls of information systems that process, transmit, or store CUI, financial data, and intellectual property.

Applicability

This policy and supporting procedures are applicable to all Keysight business units. Owners of applications, databases, operating systems, infrastructures, and supporting IT functions are responsible for developing guidelines and procedures to support this policy.

Implementation

Implementation of this policy is defined by the following procedures:

- Security Assessments

3.13 System Communications Protection Policy

Policy Statement

Keysight Technologies will ensure that electronic communications resources are used for legitimate business purposes; that those resources are used in compliance with applicable laws, industry standards and other Keysight policies; and that communications are protected from unauthorized use or disclosure.

Management must:

- Monitor, control, and protect information transmitted or received by information systems at the external boundaries and key internal boundaries to prevent disruption or unauthorized use of Keysight's electronic communications resources, services, and activities.
- Employ architectural designs, software development techniques, and systems engineering principles that promote efficient and effective information security within Keysight information systems.

Applicability

This policy and supporting procedures are applicable to all Keysight business units. Owners of applications, databases, operating systems, infrastructures, and supporting IT functions are responsible for developing guidelines and procedures to support this policy.

Implementation

Implementation of this policy is defined by the following procedures:

- System and Communication Protection
- Prohibition of Unofficial External Web Services

3.14 System and Information Integrity

Policy Statement

Keysight Technologies will implement procedures and technologies to ensure the processing integrity of its information systems.

Management must:

- Ensure information systems and infrastructure are configured, operated, and maintained to safeguard data from unauthorized use or disclosure.
- Provide a mechanism for identifying, reporting, and correcting system processing failures in a timely manner.

Applicability

This policy and supporting procedures are applicable to all Keysight business units. Owners of applications, databases, operating systems, infrastructures, and supporting IT functions are responsible for developing guidelines and procedures to support this policy.

Implementation

Implementation of this policy is defined by the following procedures:

- Vulnerability Assessments and Remediation
- Network Device Patching
- Anti-Malware Protection
- Open Virtual Appliance Patching
- Service Provider Management
- Handling of Unclaimed Systems on a Network
- Appendix A - Vulnerability Remediation Timeframes

3.15 Security Operations Policy

Policy Statement

This policy provides direction to ensure that Keysight information systems and associated data are secure.

Management must ensure that:
Keysight information systems and infrastructure are configured, operated, and maintained in a manner that safeguards data and provides a secure business environment.

Applicability

This policy and supporting procedures are applicable to all Keysight business units. Owners of applications, databases, operating systems, infrastructures, and supporting IT functions are responsible for developing guidelines and procedures to support this policy.

Implementation

Implementation of this policy is defined by the following procedures:

- Network Security
- Network Security Management Controls
- Application Security
- Cloud Resources Security
- Server Security
- Content Filtering
- Encryption
- Penetration Testing
- Appendix A Network Device Risk Classification Matrix
- Appendix B IDS Needs Assessment Matrix
- Appendix C High-Risk Outbound Tools
- Appendix D Cloud Vendor Security Procedures
- Appendix E Security Assessment Checklist
- Appendix F System Security Criticality
- Definitions
- Security Criticality Criteria

3.16 Acceptable Use Policy

Policy Statement

Keysight employees and non-Keysight workers on the Keysight Technologies network will adhere to acceptable behaviors while using Keysight-provided information systems.

Management must ensure that:

- Users understand their responsibilities when accessing Keysight owned, leased, or operated information systems.
- Users understand that Keysight information systems are to be used primarily for business purposes with occasional personal use.
- All information system use complies with applicable Keysight policies.
- Information system use conforms to legal and Keysight Standards of Business Conduct (SBC) requirements.

Applicability

This policy and supporting procedures are applicable to all Keysight business units. Owners of applications, databases, operating systems, infrastructures, and supporting IT functions are responsible for developing guidelines and procedures to support this policy.

Implementation

Implementation of this policy is defined by the following procedures:

- Acceptable Use of Information Systems
- Acceptable Use of Email
- Acceptable Use of Instant Messaging
- Acceptable Use of Voice Systems

KEYSIGHT

Revision History

Date	Version	Author	Comment
5 January 2022	1.0	Kyleigh Stennis	Published
24 May 2023	2.0	Scott Harrington	Published
03 July 2024	3.0	Anna Wolny	Index Updated for 3.13 & 3.14