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

www.keysight.com

Effective: 1 December 2023 Last Review: 25 May 2026

Supplier Cybersecurity Control Guidelines

Keysight solutions, which are developed with a 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. We are committed to assuring that instrument manufactured, refurbished, serviced, calibrated, and demonstrated by Keysight are free of malware and other computer-based threats.

In support of this commitment, Keysight expects its suppliers to maintain security industry's best practices, such as the following to protect both Keysight and its customers from cybersecurity threats:

1. Cybersecurity Policy

1.1. Maintain information security policies to protect data and systems from potential loss, misuse, or alteration of confidential or sensitive information.

2. Access Control

2.1. Only allow authorized personnel to access Keysight data and/or systems.

2.2. Implementation of controls to ensure the timely disabling of access from the supplier personnel who no longer require access to Keysight data and/or systems.

3. Asset Management

3.1. Only allow authorized personnel access to Keysight owned devices, including but not limited to servers, equipment, laptops, and smartphones with comprehensive technical security controls.

3.2. Only access and use Keysight owned devices/data for Keysight related activities, any personal use of the Keysight devices/data is strictly prohibited by policy.

4. Physical Protection

4.1. Protect and monitor the physical facility and support infrastructure for those information systems that store or process Keysight data and/or systems.

4.2. Restrict physical access to authorized personnel in the areas where Keysight owned devices are located.

5. System and Communications Protection

5.1. Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems to prevent unauthorized access or use of Keysight information.

6. Security Operations

6.1. Implementation of network access controls that separates supplier's internal network from the internet (e.g., firewall etc.) and configure alerts to report on any suspicious network activity.

6.2. Installation of anti-virus and malware protection software with up-to-date definitions and signatures to detect malicious activities to limit their effectiveness.

7. Incident Response

7.1. 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 should include the elements of detections, containment, and remediation.

7.2. Any security incident that impacts Keysight, Supplier shall notify Keysight within 48 hours of discovery by sending an email to sc.compliance@keysight.com and cybersecurity@keysight.com, and copy their Keysight Buyer.

7.3. Cooperate with Keysight in investigating the occurrence, including making available all relevant data retention logs that relate to the security incident.

8. IT Disaster Recovery

8.1. Maintain an IT disaster recovery plan for any services that involve the on-going processing and maintenance of Keysight data and/or systems.

8.2. Implementation of industry standard backup and restoration capabilities.

9. Awareness and Training

9.1. Provide ongoing awareness and training on the supplier's information security policies and procedures to all the supplier personnel who have access to the data and/or systems.

10. Risk Assessment

10.1. Perform risk assessments on the information technology environment to identify potential security issues across the organization.

10.2. When requested by Keysight, completion of a cybersecurity questionnaire to provide a better understanding of suppliers' cybersecurity control level and risks to Keysight.

11. Deliverable Requirements & EU Cyber Resilience Act (CRA) Compliance

11.1. For purposes of this Section, "Deliverables" means any hardware, software, firmware, component, update, patch, documentation, and any related remote or hosted functionality supplied by or on behalf of Supplier.

11.2. Unless expressly waived by Keysight, Supplier shall ensure all Deliverables comply with the applicable requirements of the EU CRA in accordance with Supplier's role, including, but not limited to:

Security by Design
Implement and maintain security by design and by default measures throughout the Deliverables lifecycle, including as applicable secure default configurations, limitation of attack surface, appropriate access control, protection of confidentiality, integrity, and availability of data and functions, relevant logging and monitoring, and secure reset, removal, or decommissioning capabilities;

Vulnerability Handling & Updates
Identify, document, and manage vulnerabilities and third-party components used in the Deliverables, exercise appropriate due diligence over its own suppliers and open-source or other third-party components, perform appropriate security testing and reviews, and provide without undue delay patches, updates, fixes, workarounds, or other corrective or compensating measures;

Coordinated Vulnerability Disclosure Process
Maintain an effective vulnerability management and coordinated vulnerability disclosure process, and provide and maintain an accessible human point of contact for the reporting and coordination of vulnerability and security issues;

Security Incident Notification
Notify Keysight without undue delay, and for any actively exploited vulnerability, material vulnerability, compromise of Supplier's development, build, release, signing, update, or support environment, or other security incident or event affecting or reasonably likely to affect the Deliverables, no later than 24 hours after becoming aware of it; such notice shall include, as available, the nature of the issue, affected Deliverables, impact, available mitigations, containment measures, remediation plan, and expected timing for corrective action;

Cooperation and Coordination
Cooperate fully with Keysight in vulnerability triage, incident response, remediation, customer protection, regulatory assessment, and external communications, and shall not make any public statement or disclosure identifying Keysight or an affected Keysight product without prior coordination with Keysight, except to the extent required by applicable law;

Technical Information and Evidence
Provide Keysight with information and documentation reasonably necessary for Keysight to assess, evidence, achieve, or maintain the cybersecurity, safety, and regulatory compliance of the Deliverables and of Keysight products incorporating them, including, as applicable, security architecture and design information, configuration requirements, instructions for secure implementation into Keysight products, support and end-of-support information, test results, component and dependency information, software and hardware bill of materials, vulnerability handling procedures, known vulnerabilities, and any known residual cybersecurity risks, limitations, assumptions, and instructions for secure operation, updating, and decommissioning;

Support and End-of-Support
Support the Deliverables, including by providing security updates and remediation, for the period agreed in writing or, absent such agreement, for the period reasonably necessary in light of the expected service life and intended use of the Deliverables and their reasonably foreseeable use in Keysight products, and shall communicate any support limitations and any end-of-support date to Keysight sufficiently in advance; and

CRA and EU Conformity Support
Where and to the extent a Deliverable is subject to the Cyber Resilience Act or other applicable EU product conformity requirements and is placed on the EU market under Supplier's responsibility, comply with those requirements and provide the applicable Declaration of Conformity, CE marking information, certificates, and other conformity evidence reasonably requested by Keysight; where and to the extent such requirements do not directly apply to Supplier or the Deliverable, Supplier shall nevertheless comply with this Section and provide evidence of materially equivalent cybersecurity controls and vulnerability-handling practices.

Since every IT environment is unique, Keysight acknowledges that implementation will vary from environment to environment, but the principles that necessitate these policies must be met and adhered to. Additionally, Supplier shall also comply with all regulatory and local governing laws that are applicable.