

## 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 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.

Effective: 1 December 2023

---

**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](mailto:sc.compliance@keysight.com) and [cybersecurity@keysight.com](mailto: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.

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.