Technical and Organizational Measures Including Technical and Organizational Measures to Ensure the Security of the Data

Sauce Labs aims to provide confidentiality, integrity and availability of information.

Sauce Labs is SOC 2 Type II certified by the AICPA (American Institute of Certified Public Accountants) in security, confidentiality, integrity and availability principles. The SOC 2 Type II principles represent that Sauce Labs has designed systems to ensure the protection of system resources against unauthorized access.

Sauce Labs has processes and procedures in place to adequately address and continuously improve Security in a structured way throughout the entire company. The current SOC 2 Type II certification expires on December 1, 2024. Sauce Labs has retained 1stSecure as the auditor for 2024 with certification prior to December 1, 2024.

Sauce Labs has current certifications for ISO 27001:2013 Standard (Information Management Security Standard) and ISO 27701:2019 (Privacy Information Management Standard). Sauce Labs will recertify prior to January 10, 2025 on ISO 27001:2022 Standard and ISO 27701:2019 Standard.

The following technical and organizational measures (TOMs) at Sauce Labs are designed to protect these principles. "Confidentiality" means that information is not made available to unauthorized individuals, entities or processes. "Integrity" refers to accuracy and completeness of information. "Availability" means information being accessible and usable upon demand by an authorized entity.

Organizational Measures

1. **Security Risk Management**: Security risks are identified, assessed and prioritized for mitigation. Controls and mitigation plans are defined, implemented and tested.
2. **Security Policies**: A Security policy framework is defined. Standards have been established in order to constantly improve and adapt the overall Security status.
3. **Contact with Authorities and Interest Groups**: Sauce Labs is in regular contact and closely cooperates with relevant authorities and interest groups to stay abreast of the latest trends and regulations in security.
4. **3rd Party Risk and Outsourcing Management**: Each external partner is vetted prior to selection and onboarding by means of due diligence.
5. **Security Awareness**: Every employee must annually attend security awareness training.
6. **Professional Development**: Regular training is expected in order to stay up to date with modern technologies.

Technical & Operational Measures

Information and Cyber Security

1. **Cyber Threat Intelligence (CTI)**: Internal and external specialists gain information about threats, analyze them and define security controls accordingly.
2. **Network Security**: The networks are segmented and resilient, network access is protected, and traffic is analyzed and filtered.
3. **Cryptography**: Where appropriate, cryptographic measures are in place to ensure confidentiality of data and integrity.
4. **Device Security**: Devices are encrypted and centrally managed. Access to the corporate network is possible only via authorized account credentials.
5. **Malware Protection**: Malware services and systems are in use to detect, prevent and report (use of) malicious software and behavior.
6. **Access Control/Authentication and Authorization**: As a part of the user lifecycle management, defined processes for adding, changing and removing users and their access rights are applied. Access rights are provisioned according to need-to-know, need-to-have or need-to-do principles. Regular reviews of access rights are conducted.
7. **Password Security**: The complexity and length of passwords are set according to best practices and adapted if necessary.

8. **Secure Software Development**: Software is developed according to defined secure software development and secure coding practices based on leading industry standards.
9. **Security Tests**: The Sauce Labs Platform is penetration-tested by external, accredited, highly reputable security companies so as to further mitigate the risk of security software vulnerabilities.
10. **Data Classification**: Sauce Labs has implemented a classification model consisting of distinct levels which must be followed by all Sauce Labs employees. The protection level and requirements for data processing are defined for each classification category.
11. **Data Loss Prevention**: In addition to cryptographic controls, several measures are in place to detect, monitor, and observe malicious or undesired websites and content.
12. **Test Data/Data Security**: Sauce Labs requires that customers upload "test data". Test data should not include any sensitive or personal data regarding customer personnel, customers, end users, or other third parties.
13. **Vulnerability and Patch Management**: Both internal and external vulnerability scans are regularly performed to ensure that vulnerabilities are detected promptly and fixed based on their criticality.
14. **Security Monitoring**: Monitoring systems are in place to detect, analyze and react to anomalous activities indicating security incidents.
15. **Incident Management**: An incident management process is established so as to handle incidents in a timely manner. The main objective is to return to normal business as soon as possible.

Business Continuity (BCP)

1. In Sauce Labs, the objective of BCP is to provide the ability to effectively respond to threats such as natural disasters or data breaches and protect Sauce Labs and its customers. The BCP lifecycle shows the stages of activity that must be gone through and repeats itself with the overall objective of improving organizational resilience.
2. Policy and Program Management: The Business Continuity policy provides the framework around which the BCP program is designed and built. It is the key document defining scope and governance.
3. Embedding Business Continuity: Business Continuity is continually integrated into Sauce Labs day-to-day business activities and organizational culture through training and education.

4. Analysis: Objectives, processes and constraints of the environment in which Sauce Labs operates are reviewed and assessed. The main technique used is the Business Impact Analysis.
5. Design: Appropriate strategies and tactics are identified and selected to determine how continuity and recovery from disruption can be achieved.
6. Implementation: The agreed strategies and tactics are executed through the process of developing the Business Continuity Plan.
7. Validation: Business Continuity Tests and Disaster Recovery Tests confirm that the BCP program meets the objectives set in the policy.

Physical Security

1. Security Zoning: Colocation data center premises are categorized in various protection zones. A zone's security level depends on the criticality of assets in it.
2. Access Control Management and System: An access control system is used to grant and trace access to the protection zones as well as maintain access permissions.
3. Security Personnel: 24/7 Colocation Security staff is employed to detect or ward off problems at the earliest possible stage and also acts as a response team in the monitoring center.
4. Intruder Alarm System: An intruder alarm system is used to detect unauthorized entry into any protection zones.
5. Video Surveillance: Video surveillance supports security management in deterring, detecting and documenting unauthorized access and any kind of inappropriate or unlawful activities.
6. Secure Disposal: Sauce Labs enforces a secure waste management protocol to securely eliminate sensitive data. Appropriate means are provided by external sources.