SauceLabs

DATA SHEET

Sauce Labs Security Technical and Organizational Procedures

Table of Contents

Introduction

Security is a top priority for Sauce Labs. Data from customers is treated with utmost care. To ensure trust in its professional services, Sauce Labs has implemented several technical and organizational measures. The rapid changes in technology and its open nature require constant adaptation and improvement of security measures from a technical as well as an organizational point of view. The attached document provides an overview of what is being done at Sauce Labs to protect information as well as technical infrastructure.

Fundamental Principles of Security

Security aims at providing confidentiality, integrity and availability of information. All technical and organizational measures 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.

Security Framework

In order to achieve the set goals, a framework is required to act as the foundation for an efficient security program. The Sauce Labs security framework and its information security management system consist of the cornerstones to monitor, identify, prevent, detect, respond and recover.

As of December 1, 2021, Sauce Labs has been officially re-certified according to AICPA as SOC 2 Type II compliant. The SOC 2 Type II Security Principle represents 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.

As of January 11, 2022, Sauce Labs has earned the ISO 27001 distinction for global information security.

Sauce Labs achieved ISO 27701:2013 certification on June 24, 2022, the global standard for the Privacy Information Management System (PIMS).

Strategic Approach to Security

Sauce Labs constantly develops and adapts its security strategy to actively identify, evaluate and minimize new threats and risks.

Organizational Measures

Security is more than just a technical issue. People and processes must also be taken into consideration so as to adequately address security company-wide and promote a “security first” mindset at Sauce Labs.

Security Policies

A security policy framework is defined. Standards have been established in order to constantly improve and adapt the overall security status.

Security Risk Management

Security risks are identified, assessed and prioritized for mitigation. Controls and mitigation plans are defined, implemented and tested.

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.

3rd Party Risk and Outsourcing Management

Each external partner is vetted prior to selection and onboarding by means of due diligence.

Security Awareness

Every employee must annually attend security awareness training.

Professional Development

Regular training is mandatory in order to stay up-to-date with modern technologies. Additionally, Sauce Labs has licensed LinkedIn Learning for the entire company, and curated security-specific content for introductory, mid-level and advanced security topics.

Technical & Operational Measures

Information and Cyber Security

To ensure trust in its professional services, Sauce Labs protects its business and customer data from unauthorized access, hacking attempts, malware infections, DDoS attacks, data leakages, phishing attempts, disclosure of sensitive information and other threats with technical measures. Mitigation measures are implemented to ensure an appropriate risk level concerning confidentiality, integrity, availability and resilience of all systems.

Cyber Threat Intelligence (CTI)

Internal and external specialists gain information about threats, analyze them and define security controls accordingly.

Network Security

Systems in networks are protected by technical and organizational measures: The networks are segmented and resilient, network access is protected, and traffic is analyzed and filtered.

Cryptography

Where appropriate, cryptographic measures are in place to ensure confidentiality of data and integrity.

Device Security

Devices are encrypted and centrally managed. Access to the corporate network is possible only via authorized devices.

Malware Protection

Malware services and systems are in use to detect, prevent and report (use of) malicious software and behavior.

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.

Password Security

The complexity and length of passwords are set according to best practices and adapted if necessary.

Secure Software Development

Software is developed according to defined secure software development and secure coding practices based on leading industry standards.

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.

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.

Data Loss Prevention

All devices are encrypted and the use of external media is restricted in order to prevent data loss or leakage through distribution channels. In addition, several measures are in place to detect and block connections to malicious or undesired websites and content.

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.

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.

Security Monitoring

Monitoring systems are in place to detect, analyze and react to anomalous activities indicating security incidents.

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 Planning (BCP)

BCP is a framework for identifying an organization's risk of exposure to internal and external threats. 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.

Business Continuity Policy

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.

Embedding Business Continuity

Business Continuity is continually integrated into Sauce Labs day-to-day business activities and organizational culture through training and education.

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.

Design

Appropriate strategies and tactics are identified and selected to determine how continuity and recovery from disruption can be achieved.

Implementation

The agreed strategies and tactics are executed through the process of developing the Business Continuity Plan.

Validation

Business Continuity Tests and Disaster Recovery Tests confirm that the BCP program meets the objectives set in the policy.

Physical Security

Physical Security Management restricts physical access to Sauce Labs premises in order to protect data and data systems with a mix of interacting organizational, infrastructure and technical measures in a layered defense approach.

Access Control Management and System

An access control system is used to grant and trace access to the Sauce Labs protection zones as well as maintain access permissions.

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.

Intruder Alarm System

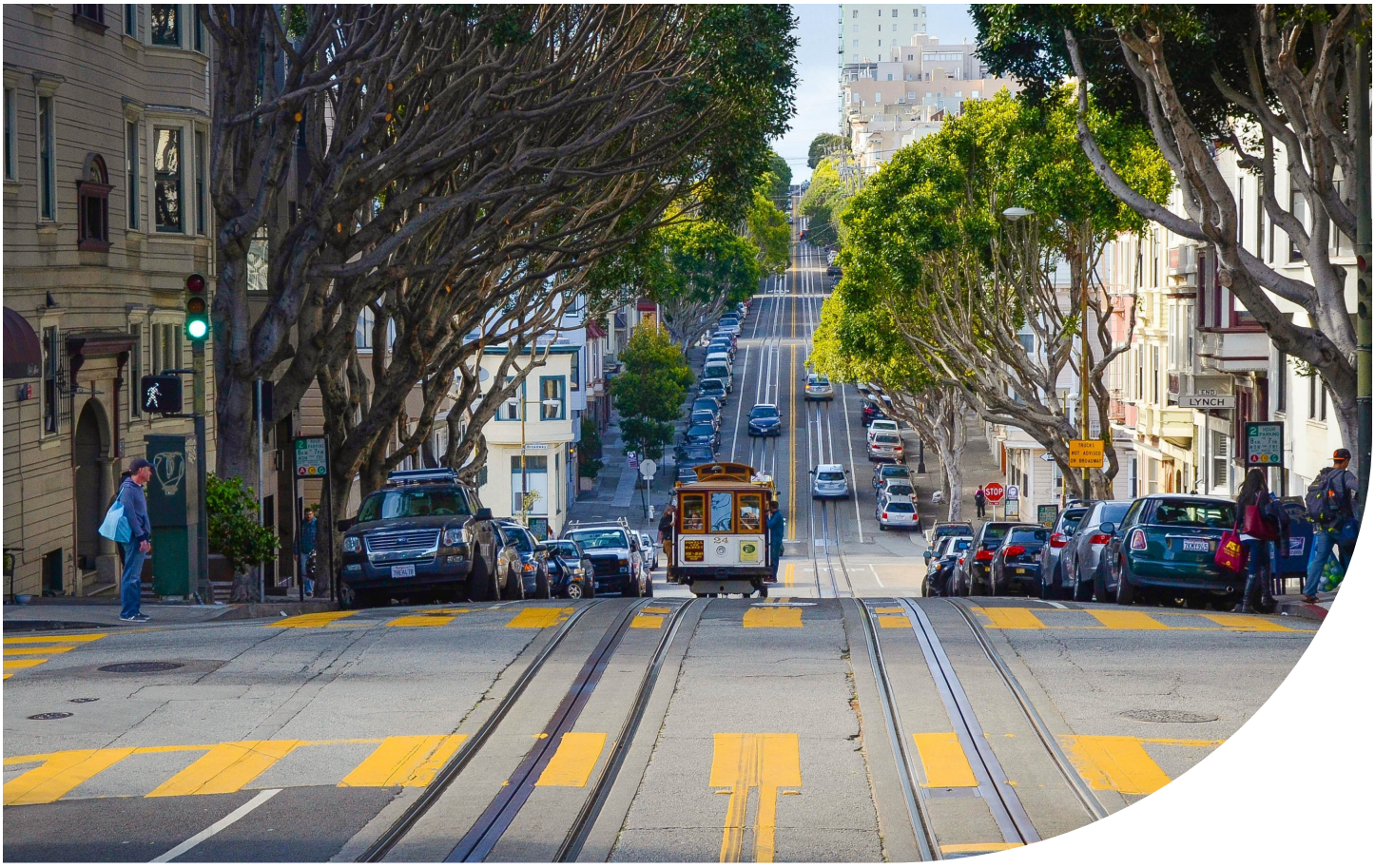
An intruder alarm system is used to detect unauthorized entry into any protection zones.

Video Surveillance

Video surveillance supports security management in deterring, detecting and documenting unauthorized access and any kind of inappropriate or unlawful activities.

Secure Disposal

Sauce Labs enforces a secure waste management protocol to securely eliminate sensitive data. Appropriate means are provided by external sources.



About Sauce Labs

Sauce Labs is the leading provider of continuous test and error reporting solutions that gives companies confidence to develop, deliver and update high quality software at speed. The Sauce Labs Continuous Testing Cloud identifies quality signals in development and production, accelerating the ability to release and update web and mobile applications that look, function and perform exactly as they should on every browser, operating system and device, every single time. Sauce Labs is a privately held company funded by TPG, Salesforce Ventures, IVP, Adams Street Partners, and Riverwood Capital.

For more information, please visit
→ saucelabs.com

saucelabs.com/sign-up

FREE TRIAL

SAUCE LABS INC. - HQ 450 Sansome Street, 9th Floor, San Francisco, Ca Usa 94111

SauceLabs