BrowserStack

Information Security Program

Information Security Policies (Summary Info)

Acceptable Usage Policy

The Acceptable Usage policy stipulates constraints and practices that our employees follow when using BrowserStack-owned equipment, electronic devices, email, the internet, etc.

The policy also defines our employees' responsibilities when it comes to ensuring the security of their equipment, Email etiquette and content, allowed use of the internet, avoiding inappropriate use of systems, and the disciplinary action that will be taken if there is a deviation from the policy.

Identity & Access Management Policy

The Identity & Access Management Policy defines high-level requirements and guidelines that our employees follow for user account management, access provisioning & de-provisioning, monitoring, separation of duties, and remote access to information systems and resources owned or operated by or on behalf of BrowserStack.

Backup and Restoration Policy

BrowserStack actively minimizes security and business continuity risks associated with data loss by defining a reliable backup regime for all the data services under the Backup & Restoration Policy.

This policy defines and applies a clear backup and restore standard for all information systems as per data prioritization and prevents data loss in the case of accidental deletion or corruption of data, system failure, or disaster.

Asset Management Policy

The Asset Management Policy defines the process to identify BrowserStack's assets and ensures that they receive an appropriate level of protection following their importance by defining responsibilities and preventing risks like unauthorized disclosure, modification, removal, or destruction of information stored on those assets.

The policy requires maintaining an inventory of assets, classification of assets based on severity, confidentiality, privacy requirements, and the value of the information they contain, determining the criticality and ownership of assets, defining acceptable use of assets, along with the return and disposal of assets.

Business Continuity and Disaster Recovery

BrowserStack has a Business Continuity and Disaster Recovery Policy that ensures that the organization can quickly recover from natural and man-made disasters while continuing to support customers and other stakeholders.

This policy covers BrowserStack’s business continuity and disaster recovery planning for all the critical business processes and service activities undertaken by BrowserStack for its business/customers in order to:

- Effectively manage any incident that may cause a business disruption to BrowserStack.
- Provide continuity of critical business processes and services managed by BrowserStack.
- Minimize the potential impact that any business disruption would have on BrowserStack and its reputation.

This is achieved by performing Business Impact Analysis, defining roles and responsibilities to various stakeholders as part of the Business Continuity & Disaster Recovery plan, and performing BC/DR tests and exercises.

Change Management Policy

BrowserStack’s Change management policy governs changes to the applications and supporting infrastructure and aids in minimizing the impact that changes have on organization processes and systems.

The policy describes the Change management process covering the lifecycle of a change, including planning, documentation, and implementation upon approval and execution, and is used for the management of changes in Software, hardware, policies, and procedures.

Code of Conduct and Ethics

BrowserStack values ethics, trust, and integrity throughout its business practices.

Our Code of Conduct and Ethics sets forth our core values, shared responsibilities, global commitments, and promises. It provides general guidance about the Company’s expectations, highlights situations that may require particular attention, and references additional resources and channels of communication available to our employees.

Customer Support and SLA Policy

At BrowserStack, we are committed to providing timely support services to our customers. BrowserStack provides Customer Support and a Service Level Agreement (SLA) to support its customers, which is governed by the Customer Support and SLA Policy.

This policy documents the SLAs and sets out our support services to assist our customers with technical queries, billing and account information, and issues pertaining to BrowserStack products.

Data Center Policy

Data Center Policy defines requirements and guidelines on physical security management of office locations and our data centers(both third parties and in-house).

Data Retention and Disposal

This policy is about the organization's approach for data retention and secure disposal.

Incident Management

BrowserStack's Incident Management Policy provides guidelines to manage security incidents that threaten the confidentiality, integrity, or availability of information assets and critical systems. It is critical to Browserstack that incidents that threaten information assets' security or confidentiality are appropriately identified, contained, investigated, and remediated.

This policy defines the Roles and Responsibilities of the Incident Management team, Incident monitoring plan describing the mechanisms put in place to monitor and quantify the types, volumes & costs of information security incidents, Incident response plan with the steps from reporting an incident to its formal closure and steps to be taken to communicate regarding the incident to customers and stakeholders.

Data Classification Policy

Data classification is the process of assigning value to information in order to organize it according to its risk of loss or harm from disclosure.

BrowserStack's data classification policy maps out a variety of components, considers every type of data belonging to the organization, and subsequently classifies the data according to storage and permission rights. These datasets are then classified as public, internal, restricted, confidential, and highly confidential.

Information Security Policy

BrowserStack's Information Security Policy provides an integrated set of protection measures that are uniformly applied across the organization to ensure a secure operating environment for its business operations.

This policy addresses the three major information security requirements, i.e., Confidentiality, Integrity, and Availability. Other requirements such as Authenticity, Non-repudiation, Identification, Authorization, Accountability, and audit ability are also addressed in this policy.

It also sets out the Information Security Governance followed across BrowserStack, which consists of leadership, organizational structures, and processes that protect information and mitigate growing information security threats. The Roles & Responsibilities of various stakeholders under the Information Security Program are also defined under this policy.

Network Security

The organization maintains a protected, interconnected computing environment through the use of securely configured network devices to meet organizational missions, goals, and initiatives.

BrowserStack’s objective is to secure all networks under its control from intrusions and to provide and maintain the security of BrowserStack’s infrastructure and data. This policy provides guidelines to ensure the availability and reliability of all the network resources owned by BrowserStack.

Personnel Security Policy

BrowserStack’s employees understand their roles and responsibilities around security and privacy. BrowserStack’s Personnel Security Policy establishes processes and best practices for managing risks from personnel screening, onboarding, termination, transfer, and management.

This policy covers the whole employee lifecycle, from Pre-employment checks to Termination or resignation.

Risk Management Policy

BrowserStack institutes regular risk assessments and uses industry best practices in remediation. BrowserStack’s Risk Management Policy establishes the requirements to perform periodic Risk Assessments (RAs) to determine areas of vulnerability in corporate operations, products, and services and initiate appropriate remediation.

The Risk Assessment process consists of identifying, analyzing, and evaluating the risks on the basis of which a risk score is assigned. The risks are treated on the basis of Risk Acceptance criteria. To ensure that Risk management is effective and continues to support organizational performance, Risk monitoring and review is also performed in periodic intervals.

Server Security Policy

BrowserStack manages, configures, and protects organization servers and hosts based on industry best practices. BrowserStack’s Server Security Policy establishes standards for the base configuration of servers (physical and virtual) owned and/or operated by BrowserStack.

The policy describes the roles and responsibilities for ensuring server security, configuration and backup guidelines, monitoring and patch management, and decommissioning of servers.

Software Development LifeCycle Policy

BrowserStack designs and builds software with security and privacy as design principles.

BrowserStack Software Development Lifecycle Policy provides guidance and establishes standards for the development of software and applications at BrowserStack as per industry best practices to ensure that software is produced in a secure, reliable, accessible, and consistent manner.

This policy also focuses on adding security to the standard Software Development Lifecycle (SDLC) process by embedding security in each phase of the SDLC, which allows for addressing security issues in the SDLC pipeline well before deployment to production instead of just focusing on the functionality.

Vendor Management

BrowserStack actively manages risks around third-party vendors and their access to the organization's data.

BrowserStack’s Vendor Management Policy sets forth the guidelines that are followed to maintain the security of the organization's information systems and data when Browserstack enters into any arrangement with a third-party supplier/vendor, as well as to identify elements of managing vendors, due diligence, risk assessments as well as contract management.

Vulnerability & Patch Management Policy

BrowserStack conducts periodic application and network scanning and identifies, evaluates, and treats the vulnerabilities in defined timelines.

BrowserStack’s Vulnerability & Patch Management Policy ensures a higher level of security to BrowserStack’s resources & endpoints and protects the electronic information that is processed and stored across BrowserStack’s infrastructure. Regular scans are done on the entire system looking for misconfigured and/or unsecured systems, devices, and endpoints: discovered vulnerabilities and threats identified to be verified and remediated by respective system owners.