zerobounce.net
US: 1.888.500.9521
UK: +44.330.808.4814

ZeroBounce Security and Risk Assessment Overview

zerobounce.net
US: 1.888.500.9521
UK: +44.330.808.4814

TABLE OF CONTENTS

zerobounce.net
US: 1.888.500.9521
UK: +44.330.808.4814

ZeroBounce Security Program

ZeroBounce maintains a written security program that complies with applicable global industry-recognized information security frameworks (for example, NIST, OWASP, SOC, and ISO 27001 criteria), includes administrative, technical, and physical safeguards reasonably designed to protect the confidentiality, integrity, and availability of Customer Data, and is appropriate to the nature, size, and complexity of ZeroBounce's business operations. ZeroBounce's corporate policies, standards, and operating procedures are reviewed, updated (as needed), and approved on an annual basis or more frequently as needs arise to maintain their continuing relevance and accuracy. All ZeroBounce personnel are required to review and acknowledge security policies during onboarding and annually thereafter.

ZeroBounce's Head of Cyber Security together with the Head of Compliance develop, maintain, review, and approve all ZeroBounce policies. These policies undergo further review by ZeroBounce's counsel and independent third-party SOC 2 and ISO 27001 auditors.

All ZeroBounce personnel are required to complete compliance and security awareness training at the time of hire and annually thereafter.

Encryption and Key Management

ZeroBounce uses industry-standard encryption techniques to encrypt Customer Data at rest and in transit when applicable. All connections are authenticated and encrypted using industry-standard encryption technology.

Incident Response and Notification

ZeroBounce has an incident response plan, including a breach notification process, to assess, escalate, and respond to identified physical and cyber security incidents that impact the organization and customers or result in data loss. Discovered intrusions and vulnerabilities are resolved in accordance with established procedures. The incident response plan is reviewed and updated annually and more frequently as needed.

If there is a breach impacting Customer Data, ZeroBounce will notify any affected parties without undue delay upon discovery of the breach, reasonably cooperate with respect to investigations, and take appropriate corrective action to mitigate any risks or damages to protect Customer Data from further compromise. ZeroBounce will take any other actions that may be required by applicable law.

Risk Management

ZeroBounce has a security risk assessment and management process to identify and remediate potential threats to ZeroBounce and its customers. Risk ratings are assigned to all identified risks, and the compliance team manages remediation in conjunction with stakeholders from applicable departments. Executive management is kept apprised of the risk posture of the organization.

Access Control

ZeroBounce assigns application and data rights based on security groups and roles, which are created based on the principle of least privilege. Security

access requests are reviewed and approved by the applicable stakeholder prior to provisioning access.

Informational assets are classified in accordance with ZeroBounce's data classification guideline.

User Access Management

All access to ZeroBounce systems and networks is disabled promptly upon notification of termination or departure. ZeroBounce reviews administrator access to confidential and restricted systems, including corporate networks, on a regular basis. Administrator access to the production environment and to select corporate systems that provide broad privileged access is reviewed quarterly.

ZeroBounce uses separate administrative accounts to perform privileged functions, and accounts are restricted to authorized personnel.

Password Management and Authentication Controls

Authentication mechanisms require users to identify and authenticate to the corporate network with their unique user ID and password. ZeroBounce requires all relevant and industry-recommended password parameters for the corporate network via a directory service system. Remote access to the corporate network is secured through a virtual private network (VPN).

Threat and Vulnerability Management

zerobounce.net
US: 1.888.500.9521
UK: +44.330.808.4814

ZeroBounce's Vulnerability Management program monitors for vulnerabilities on an ongoing basis using a combination of internal and external vulnerability scans using industry-recognized vulnerability scanning tools. Identified vulnerabilities are evaluated, documented, and remediated to address the associated risk(s).

An independent third party conducts monthly external penetration tests. The significant findings are evaluated, documented, and remediated. ZeroBounce is also included in the HackerOne and Intigriti programs, where top security researchers worldwide are contracted to find vulnerabilities in our web-facing applications.

Logging and Monitoring

ZeroBounce continuously monitors application, infrastructure, network, data storage space and system performance using anti-malware, anti-virus, and threat detection tools. Specific security events trigger alerts which are promptly reviewed by authorized personnel. Access to logs is restricted to authorized personnel and reviewed permanently. Logs contain details on the date, time, source, and type of events.

Change Management

ZeroBounce has change management policies and procedures for requesting, testing, and approving application, infrastructure, and product-related changes. All changes receive a risk score based on risk and impact criteria. Low-risk changes generate automated change tickets and have various levels of approval based on risk score. High-risk changes require manual change tickets to be created and are reviewed by approvers based on change type. Planned changes to the corporate or production environments

are reviewed regularly. Change documentation and approvals are maintained in a ticketing system.

Product development changes undergo various levels of review and testing based on change type, including security and code reviews, regression, and user acceptance testing prior to approval for deployment. Following the successful completion of testing, changes are reviewed and approved by appropriate managers prior to implementation to production. ZeroBounce uses dedicated environments separate from production for development and testing activities. Access to move code into production is limited and restricted to authorized personnel.

Secure Development

ZeroBounce's software development life cycle (SDLC) process is consistent with the corporate security policies that govern the acquisition, development, implementation, configuration, maintenance, modification, and management of ZeroBounce’s infrastructure and software components.

Prior to the final release of a new ZeroBounce system version to the production cloud environment, code is pushed through lower-tier environments for testing and certification. ZeroBounce follows secure coding guidelines based on leading industry standards. These guidelines are updated as needed and provided to all applicable personnel. ZeroBounce utilizes a code versioning control system to maintain the integrity and security of the application source code.

Software and Asset Inventory

ZeroBounce maintains an inventory of all software components (including, but not limited to, open-source software) used in ZeroBounce products and an inventory of all media and equipment where Customer Data is stored. ZeroBounce, Inc. reviews the legal terms and requirements of all software components and updates, as applicable, and includes references to source materials or any such relevant terms in its inventory.

Data Management

ZeroBounce Customer Data will only be hosted in data centers that have attained SOC 2 Type 2 attestations or have ISO 27001 certifications (or equivalent or successor attestations or certifications). ZeroBounce backs up all Customer Data in accordance with ZeroBounce's standard operating procedure. Customer Data is only kept for the duration of the contract or as long as there is a business purpose or legal obligation.

Customers can request copies of their data or to have their data removed at any time by contacting privacy@zerobounce.com.

Workstation Security

ZeroBounce implements and maintains security mechanisms on personnel workstations, including firewalls, anti-virus, and full disk encryption. All onsite personnel are required to follow clean desk guidelines and lock or log off of devices when away from workstations.

Network Security

ZeroBounce uses network perimeter defense solutions, including IDS and firewalls, to monitor, detect, and prevent malicious network activity. Security personnel monitor items detected and take appropriate action. Firewall rule changes (that meet the criteria for the corporate change management criteria) follow the change management process and require approval by the appropriate stakeholders. ZeroBounce's corporate networks are logically segmented by virtual local area networks (VLANs), and firewalls monitor traffic to restrict access to authorized users, systems, and services.

Third-Party Security

ZeroBounce assesses and manages the risks associated with existing and new third-party vendors and employs a risk-based scoring model for each third party. ZeroBounce requires all third parties to enter into contractual commitments that contain security, availability, processing integrity, confidentiality requirements, and operational responsibilities as necessary.

ZeroBounce evaluates the physical security controls and assurance reports for data centers on an annual basis, assesses the impact of any issues identified, and tracks any remediation efforts.

Physical Security

ZeroBounce's operations are primarily remote-based. ZeroBounce restricts access to its facilities, equipment, and devices to employees with authorized access on a need-to-know basis. Any access to physical locations is reviewed and determined by job responsibility, and access is removed as part of the ZeroBounce separation or internal job transfer process when access is no longer required.

Oversight and Audit

Internal audits are aligned with ZeroBounce's information security program and compliance requirements. ZeroBounce conducts internal control assessments to validate that those controls are operating effectively. Issues identified from assessments are documented, tracked, and remediated. Internal controls related to security, availability, processing integrity, and confidentiality are audited by an external independent auditor at least annually and in accordance with applicable regulatory and industry standards.

Business Continuity and Disaster Recovery Plan

ZeroBounce maintains a Business Continuity Plan and a Disaster Recovery Plan to manage significant disruptions to operations and infrastructure. These plans are reviewed, updated, and approved by the Head of Cyber Security and the Chief Technology Officer on an annual basis. ZeroBounce conducts periodic business continuity exercises to evaluate tools, processes, and subject matter expertise in response to specific incidents. The results of these exercises are documented, and issues identified are tracked to remediation.

Human Resources Security

ZeroBounce has standard procedures in place to guide the hiring process. Background verification is required for ZeroBounce personnel in accordance with relevant laws and regulations. ZeroBounce requires personnel to sign a confidentiality agreement as a condition of employment. All personnel are also required to review and acknowledge ZeroBounce's Information Security policy, which includes acknowledging responsibility for reporting security

incidents involving Customer Data. ZeroBounce maintains a disciplinary process to take action against personnel who do not comply with company policies, including ZeroBounce security policies.

GDPR/ Data Privacy Legislation

ZeroBounce continuously reviews and adheres to all global data privacy legislation with assistance from in-house counsel and a third-party data privacy vendor. All ZeroBounce personnel receive data privacy training at the time of hire as well as on an annual basis thereafter. ZeroBounce vendors, subprocessors, and contractors with access to Customer Data are required to sign a Data Processing Agreement (DPA).

Customer DPA's are available for ZeroBounce service on our website at: https://www.zerobounce.net/docs/about-zerobounce#data_processing_agreement

ZeroBounce's Universal Customer-Facing DPA includes the European Union 2021 Standard Contractual Clauses (SCCs) and the United Kingdom ("UK") International Data Transfer Agreement and the UK Transfer Addendum and has the following Exhibits:

• Universal Customer-Facing Data Processing Agreement
• Data Processing Terms

Security Certifications

ZeroBounce has the following active security certifications:

- SOC 2 Type 2

- HIPAA
- ISO 27001:2022

ZeroBounce is compliant with:

- EU-US, EU-UK, US-Swiss DPF
- EU GDPR
- CCPA

Active customers may request copies of SOC 2 or ISO 27001 reports by contacting their ZeroBounce Account Manager. Prospective customers will be required to sign an NDA with the sales.

The following are ZeroBounce's governing documents:

- Business Continuity and Disaster Recovery
- Change Management and Control
- Data Classification
- Data Retention and Destruction
- Data Storage
- Encryption Management
- ZeroBounce Information Security
- ZeroBounce Code of Conduct
- Incident Management
- Information Security Management System
- Internal Audit
- Network Security
- Privacy Policy
- Privileged Access
- Risk Management
- Software Development Lifecycle
- System Access Management
- System Hardening

- Third-Party Vendor Diligence
- User Access Control
- Vulnerability and Patch Management

ZeroBounce does not disclose full policies to external parties, however, these policies have been reviewed in their entirety by an independent third-party auditor as part of the SOC 2 Type 2 and ISO 27001 audit processes.

Active and prospective customers may download copies of the policies by following the steps from ZeroBounce Trust Center:
https://trust.zerobounce.net