RESILIENT IT

Resilient IT Security Statement

Our Security, Briefly Stated

Resilient IT's number one concern is the protection and reliability of customer data and systems. Our servers are protected by high-end firewalls and layered security applications, as well as scans performed regularly to ensure that any vulnerabilities are quickly found and patched. All Resilient systems, including cloud based, are protected by multi-factor authentication and/or trusted hosts as available. All services have quick failover / recovery points, with backups being performed daily – backups are encrypted with AES-256 at rest, and FIPS 140-2 for data in transit.

Access to systems is restricted to specific individuals who have a need-to-know such information and who are bound by confidentiality obligations. Access is monitored and audited for compliance. Resilient IT has implemented and follows a rigorous set of security policies aligned to NIST SP 800-171, the CIS controls, and other relevant frameworks.

Resilient IT uses Transport Layer Security (TLS) encryption (also known as HTTPS) for all transmitted data. Surveys may be protected with passwords. Our services are hosted by a trusted data center that is independently audited using the industry standard SSAE-18 method and are SOC 2 Type II Certified as well as Azure Government which is certified against several standards including FedRAMP Moderate, FedRAMP High, ISO 27001:2013, NIST SP 800-53 R4&5, NIST SP 800-171 R2 and CIS Azure Foundations 1.1.0 and 1.3.0.

More Information

Resilient IT customers may request various security-related documents and questionnaires by contacting their account executive.

Security has been our highest priority from day one, beginning with vetting our vendors and how technology is deployed across our infrastructure. We follow industry best practices, including end-to-end encryption and layered security to provide defense in depth.

Additionally, we invest in recurring independent audits conducted by reputable third parties that are external to Resilient IT. These audits involve a comprehensive examination of our systems, including backend infrastructure, as well as an assessment of the networks, computing devices, and processes used to transmit, process, and store data.

We will continue to pursue comprehensive security measures as our company evolves and address all reports of potential vulnerabilities with the highest degree of urgency and scrutiny.

Revision Date: 12/04/2023