Neverfail

Security, Compliance, Privacy

Security at Neverfail is built in, not bolted on

Neverfail was built from the ground up to be a secure provider of cloud services to any industry. Our infrastructure and software are architected with security, scalability and our partners in mind.

Security Philosophy

Our philosophy is that security is an integral part of our business and that only by providing a secure platform can we enable not only our success but that of our partners. Neverfail services many partners who serve many regulated industries. It's critical that we exceed the security requirements of customers across a wide range of compliance and security standards; therefore, our employees are empowered to continually improve the confidentiality, availability and integrity of our platform.

Security is a Shared Responsibility

When a partner moves infrastructure and data to our platform, the responsibility for security becomes shared. Neverfail is responsible for security of the underlying infrastructure and the partner is responsible for the security of their environments. Neverfail takes security very seriously and we work with our partners to provide an unprecedented level of transparency into the security policies and practices we use to manage their assets. Maintaining a trusted relationship is paramount to our joint success.

Accountability and Integrity

Neverfail demonstrates an ongoing commitment to information security through the establishment and operation of an information security and compliance program that reports directly to the CEO. Neverfail employs a full-time Chief Information Security Officer (CISO) who is one-hundred percent focused on the management of information security for the organization and our offerings. The CISO provides strategy and security initiatives to ensure the highest level of security for our partners.

SECURITY COMMITMENT

- **ISO/IEC 27001:2013 information security.** Our program is aligned with international standards and tailored for our service provider partners.
- **Annual SOC2 type II audits.** Providing assurance as to the suitability of the design and operating effectiveness of our controls.
- **Regulatory compliance.** We enable our partners to achieve compliance with various regulatory requirements including HIPPA and PCI.
- **Full-time CISO.** We employ a full-time CISO with experience in creating and leading security organizations for service providers.

AICPA Service Organization Control Reports
AICPA
SERVICE ORGANIZATIONS
SOC
aicpa.org/soc
Formerly SAS 70 Reports ®

Security, Compliance and Privacy

The Neverfail platform is designed with multiple layers of security, compliance, and privacy controls. We work behind the scenes to protect our partners. Our security program was purpose-built on internationally recognized frameworks tailored to the unique requirements of cloud service providers. We use the ISO/IEC 27001:2013 standard and we are tightly aligned with the Cloud Security Alliance's Cloud Control Matrix framework. Although not indicative of the entire scope of our security efforts, the following areas reflect the key components of Neverfail's information security and compliance program.

Security Leadership and Strategy

Rapidly evolving cloud technologies expose new security vulnerabilities and increase the risk of unauthorized access and information loss. Neverfail is committed to enabling our partners to rapidly adopt secure cloud technologies with the confidence that comes from working with a security leader in the industry.

Security Governance, Risk Management and Compliance

Neverfail operates our information security program in alignment with the ISO/IEC 27001:2013 standard. Additionally, we leverage the Cloud Security Alliance's – Cloud Control Matrix to provide controls and guidance relevant to cloud service providers. Our compliance and governance efforts include annual Service Organization Control (SOC) 2 audits to provide independent third party assessment of our security controls.

Human Resources Security

Neverfail employees receive regular security training to address the unique requirements of working for a leading cloud service provider. Security awareness training is mandated to ensuring everyone understands their responsibility for security within Neverfail. Background checks are performed on all new company personnel to include both full and part time employees as well as contractors.

Physical and Environmental Security

Neverfail's infrastructure and platform are hosted only in data centers which meet our stringent security requirements. As a function of our vendor management program, Neverfail performs due diligence including on-site audits of data centers on a regular basis.

Operations and Communication Security

Neverfail operational procedures are documented and available to help ensure consistency and accountability. All changes to underlying infrastructure is tightly controlled to ensure they are visible, tested and approved prior to implementation. Development and testing are separated to reduce the risk of unauthorized changes. Robust malware controls are implemented and users are trained. Neverfail performs backup of critical management systems. We collect, aggregate and regularly review recording logs of activities including security events. Neverfail utilizes several layers of networking controls at the network edge, internal management networks, and partner environments. Firewalls are in place and segmentation with advanced threat detection is used.

SECURITY AT-A-GLANCE

- Data center access limited to Neverfail craftsmen
- Biometric scanning for controlled access
- Security cameras monitoring all locations
- 24x7 onsite staff
- Unmarked facilities to help maintain low profile
- Physical security audited by an independent firm
- System installation using hardened, patched OS
- Dedicated firewall and VPN services
- Data protection with managed backup solutions
- Distributed DDoS mitigation services based on our proprietary Cornerstone services
- All employees trained on documented information security and privacy procedures
- Access to confidential information restricted to authorized personnel only
- Systems access logged and tracked for auditing purposes
- Fully documented change-management procedures
- Independent audited disaster recovery and business continuity plans backed up by our market leading Neverfail IT Continuity Management software
- Best practices used in the random generation of passwords
- All passwords encrypted during transmission and while in storage
- Secure media handling and destruction procedures for all data
- Security professional available to provide guidance in developing security processes for compliance programs

Access Control

Neverfail follows an established process for granting access rights to any resource. Access is always granted on a least privilege basis. Off-boarding of exiting employees follows established process with physical and logical access removed and all company assets returned within one business day of termination. Privileged access rights require additional approval and are restricted and controlled. Regular reviews of user access rights for both privileged and regular users are performed on a regular basis.

System Acquisition, Development and Maintenance

Neverfail utilizes an agile methodology of software development that incorporates secure coding practices. Software changes are controlled using established change management practices and tested prior to implementation. Secure environments are used for system and application development and testing. Security testing including acceptance testing is established and follows documented process.

Vulnerability Management

Neverfail operates a management program that identifies threats and vulnerabilities, risk rating, and tracks to resolution threat and vulnerability mitigation activities. Vulnerability management is a core competency for Neverfail and a crucial component of our overall security efforts.

Incident Management and Response

Neverfail maintains an Incident Response Plan (IRP) and tests the plan regularly. All employees and contractors receive incident response training appropriate to their role within the organization.

Business Continuity and Disaster Recovery

Business continuity and disaster recovery is a core competency of Neverfail. We maintain a Business Continuity Plan (BCP) which is tested on a regular basis. The plan scope includes both data center and corporate operations.

About Our Chief Information Security Officer

Stuart Clark is the CISO for Neverfail and is passionate on the topic of cloud computing security and is laser focused on enabling regulated organizations to adopt cloud technologies in a secure manner. Stuart has been a converged security professional for more than 20 years, consistently obliterating both security and technology roadblocks to enable business success. Stuart's career began in law enforcement where he worked in multiple capacities including patrol, investigations, crime prevention, crime victim services, and technology.

He transitioned to the corporate world in 1998, providing the strategic leadership and technical execution within a startup internet banking company, educating financial services about the Internet, and then security, on the leading edge of the internet revolution. He has served as a Senior Vice President and the Chief Security Officer of a regional Texas bank. As an Information Security Consultant to large financial services organizations, Stuart employed his wealth of experience and positive attitude to solve their complex financial security challenges. Stuart is a Certified Information Systems Security Professional (CISSP) and a Licensed Peace Officer (TCLEOSE) in the State of Texas.

ABOUT NEVERFAIL

Neverfail delivers continuously available clouds through a single pane-of-glass SaaS platform. This platform is the industry's first secure, comprehensive, multi-tenant, multi-cloud management solution for BC/DR solutions, solution catalogs, cloud service billing, service orchestration, monitoring, cloud workspaces and unified communications. Neverfail serves a global partnership of managed service providers, systems integrators, telecommunication providers, data center operators, independent software vendors, governments, healthcare institutions and enterprises exclusively through the channel.

Our Locations

Neverfail provides solutions across the globe and operates data centers in the United States and Europe. Neverfail is headquartered in Austin, Texas with offices in Melville, Chicago, Denver, Kansas City, Portland, Edinburgh, Scotland and Cluj, Romania. For more information on Neverfail solutions, contact the company at 512-600-4300 or visit our website at www.neverfail.com. You can follow Neverfail on Twitter at twitter.com/neverfail.