INFO360 SECURITY OVERVIEW

COMPLIANCE AND PRIVACY

Innovyze aligns with AICPA SOC 2 guidelines for Service Organizations. These trust services criteria result in a type II report on core controls at a Service Organization relevant to security, availability, processing integrity, confidentiality or privacy through annual third-party audits. Auditors assess compliance on-site to evaluate staff, processes, procedures, and facilities to validate security and operational compliance.   Further, Innovyze follows GDPR and CCPA with respect to the collection and use of personal data.

ENTERPRISE-GRADE SECURITY

Innovyze is fully managed and hosted inside of the global leader in cloud infrastructure services, Amazon AWS. This secure and scalable foundation enables us to provide you with state-of-the-art performance as well as bullet-proof application and data security.

1. Network-level security. Firewalls on all servers
2. Cloud-level scalability. Core architecture designed across availability zones to provide high availability and performance.
3. File and data transfers direct to Amazon's global presence ensuring optimal performance from anywhere in the world.
4. Real-time network, server and application performance monitoring.
5. Passwords are hashed and salted using bcrypt.
6. SSL/TLS 1.2+ encryption in transit ensuring security of data transfers
7. Data and file encryption at rest – industry standard AES
8. Third-party application and network scans. Code scanning as a part of our SDLC preventing vulnerabilities in production.
9. AICPA SOC2 audits performed annually.

CONTROL DATA ACCESS

1. **User authentication**: Passwords are always hashed and salted using bcrypt and transferred over the network via TLS.
2. **User permissions**: several different roles determine what individual users can see or do
3. **Application security measures**: prevent customer data cross-over and ensure complete customer data segregation & protection.
4. **Strong encryption**: Info360 helps prevent cyber snooping and hacking by using secure HTTPS URLs with TLS 1.2+, the same kind that banks rely on. In addition, data is secure at rest leveraging AWS physical controls and cloud infrastructure features including AES encryption at rest.
5. **Password complexity**: force users to change passwords upon first use, meet password complexity requirements, and change passwords after 90 days.

DISASTER RECOVERY

Leveraging Amazon's core cloud architecture, high system availability is provided by using multiple availability zones and dynamically scaling infrastructure to meet customer demands. System-wide backup of all data are performed daily, separated from live data copies. Daily backups are kept for 90 days.   Innovyze data handling practices including DR plans are reviewed by auditors as a part of SOC2 audits.