SANDLINE DISCOVERY

Data Security Safeguarding client data is our top priority

A commitment to security is engrained in our culture

Sandline's pledge to provide premier eDiscovery services includes comprehensive controls, regulatory compliance and strict security measures at the physical, application and user levels. We offer safety and security in an environment that is both scalable and redundant to meet changing business needs.

Because we take the protection of client data very seriously, only qualified, experienced and certified personnel provide the layered support required to ensure security.

DATA CENTER

All client data is stored in our industry-leading facility that offers secure, dependable, high-capacity, highly scalable, raised floor, flood-controlled data storage. Equipped with fire suppression systems and 24/7 on-site monitoring, the facility also offers:

- Managed backups
- Redundant UPS power system
- N+1 redundant diesel generators
- N+1 redundant HVAC system

COMPLIANCE AND CERTIFICATION

Sandline is committed to ensuring that our infrastructure remains secure and compliant using a holistic solution that includes policy, procedure, hardware, software and qualified personnel to safeguard and monitor all systems. We also are compliant with multiple federal privacy laws, industry-enforced regulations and secure audit-reporting practices, exceeding many compliance standards to keep confidential information protected. Our data center currently has the following certifications:

- SAAE16 SOC 1 Type II
- SOC3
- PCI-DSS Level 1

SECURITY

Sandline's data security includes a comprehensive suite of monitoring systems and a multilayered approach to ensure continuous protection and assurance of data confidentiality, integrity and availability. Security features include:

- Triple-factor physical access control to data centers including biometric controls
- CCTV video surveillance with motion detection
- Intruder alarms and mantrap entries
- On-site facility monitoring 24/7 year-round
- Security Operations Center (SOC)
- Annual review of security procedures
- Edge IP filtering
- Intrusion detection and prevention system (IDPS)
- Firewall, internal network scanning and vulnerability monitoring
- Hardened OS with managed OS patches and updates
- Antivirus and malware protection
- Role-based access permissions
- Encrypted data in transit and on all physical media

AICPA SERVICE ORGANIZATIONS SOC Formerly SAS 70 Reports

PCi Security Standards Council ™

Relativity CERTIFIED ADMINISTRATOR

Relativity AUTHORIZED PARTNER