INFO SHEET

HOW WE SAFEGUARD OUR CLIENTS

The safety and security of your data has always been our highest priority. As the threat landscape changes and attacks become more common, rest assured we remain hypervigilant. We take these steps and many others to protect internal & client infrastructure:

Annual SOC® Audit

AICPA SOC

Atomic Data's controls around data security, availability, and confidentiality are **audited and certified annually.**

You can view the results in the public SOC 3 report.

24×7 Monitoring

The Network & Security Operations Center (NSOC) **watches for, responds to, and mitigates security incidents.**

- LogRhythm SIEM logging of all infrastructure
- CrowdStrike threat detection and response
- War Room response for rapid event handling
- Atomic Monitoring™ of network, servers, apps, and endpoints

Controls

Data and systems are only accessible to those that require it. They're also **segregated, encrypted in-transit, patched, and monitored.** View our approach to Security & Compliance.

- 24×7 monitoring, surveillance, & on-site security
- Physical/logical network isolation
- Annual background checks
- Unique identifiers for each user, zero-trust principles
- Use of unique tokens, card keys, biometric readers, complex passwords, and MFA

Oversight

At every level of Atomic Data, **security is always top of mind.**

- Enterprise Governance Board oversees control environment and reviews/approves changes
- Internal Security & Compliance identifies, monitors, evaluates, & mitigates risks
- Also operates, maintains, and improves Atomic Data's control environment

Policies & Procedures

Staff adhere to **written policies and procedures** that address risk assessments, change management, access, education, and much more.

- Change & Risk Management policies
- Mandatory Security Awareness training
- Event Management System for planned maintenance, unexpected events, and exceptions
- Contact verification before all client interactions

Disaster Recovery

Atomic Data's systems are **built for resiliency**, geographic isolation, and uptime.

- Robust BCDR plans maintained and tested
- Redundant data center power and environmental systems
- Redundant routing, Internet, and switching infrastructure
- Redundant, high-availability cloud infrastructure
- Backup NSOC/Service Desk systems