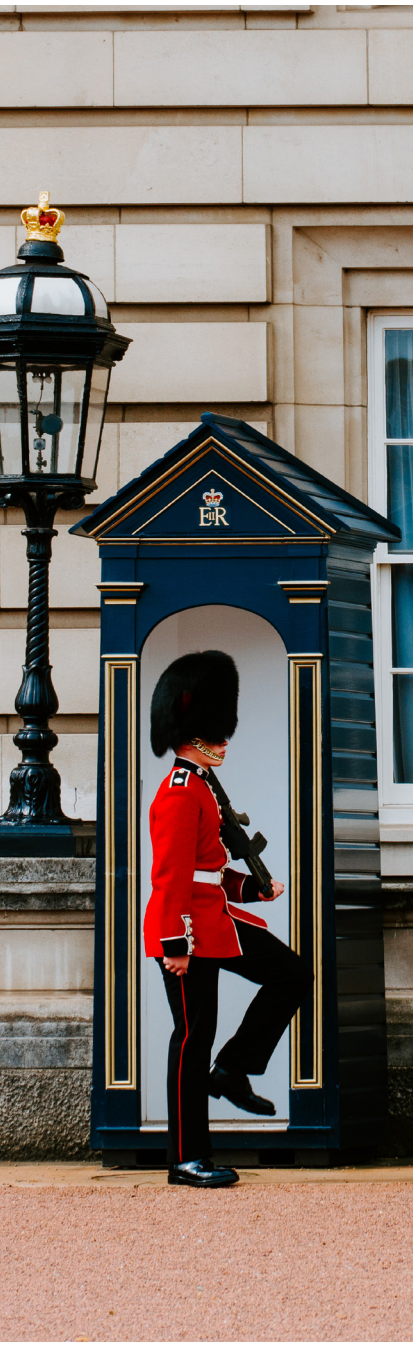
Security Controls

The security and stability of ID's information systems are both inherent to the high-quality service level we provide and critical to our clients' daily operations. ID is committed to providing the highest quality service, support, and data security to our clients, and we have invested in the best technologies available and recruited some of the industry's top professionals to realize this end.



VULNERABILITY ASSESSMENT

- Internal Vulnerability Scans
- External Vulnerability Scans
- Annual Penetration Test

GOVERNANCE, RISK & COMPLIANCE

- Annual FedRAMP Re-Authorization Audits Performed by 3PAO
- Continuous Monitoring
- Monthly Plan of Action and Milestones

DEFENSE IN-DEPTH

- Intrusion Detection Systems (IDS)
- Intrusion Prevention Systems (IPS)
- Endpoint Protection for Virus & Malware
- All traffic is denied unless explicitly approved.
- Two-Factor Authentication (2FA)

SECURITY AWARENESS

All ID employees receive a security awareness and privacy training as part of the new hire onboarding process, as well as a subsequent, job-specific training session detailing the security protocols used to perform day-to-day operations. These trainings are conducted again at least annually for all employees.

DATA BACKUP POLICIES

All client data is protected based on data classification and meets internal and client Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) ensuring no more than 15 minutes of attorney work product is at risk. All backup data is secured on hardware encrypted storage arrays utilizing industry standard encryption methods. All data can be restored in the event of disaster.

CHANGE CONTROL & PATCH MANAGEMENT

Formal change control process is used and overseen by an internal Change Control Board (CCB), which includes key stakeholders across the organization. All changes are planned, scheduled, and performed during previously agreed upon maintenance windows to minimize business impact and have detailed change, testing, and rollback procedures.

Security Controls

DISASTER RECOVERY PLAN

ID's Disaster Recovery plan is designed to scale based on the nature of the emergency, which can range from data loss prevention to catastrophic loss of primary data facilities, and contains all the information necessary to restore operational service in the event of a serious disruption.

ACCESS CONTROLS MANAGEMENT

Access to client data is determined by job role, utilizing Role Based Access Control (RBAC) and principle of least privilege enabling only authorized employees access to sensitive and confidential information they require. Computer access is monitored and restricted to continually maintain client confidentiality. Data is logically segregated by client and matter, for all directories, databases, work products, and additional uses.

SSAE 18 CERTIFIED SOC 2

HITECH COMPLIANT

GDPR COMPLIANT

ITAR COMPLIANT

FedRAMP

HIPAA COMPLIANT

Privacy Shield Framework

OTHER POLICIES COVERED IN ID'S INFO SECURITY POLICIES & THREAT ASSESSMENT STRATEGY GUIDE

- Information Security Management
- Risk Assessments
- Termination Procedures
- Monitoring
- Privacy Policy
- Incident Response Policy
- Breach Notification Policy
- Physical Security
- Workstation Usage (Acceptable Use)
- Workstation Security
- Disposal and Media Sanitization
- Technical Safeguards and Infrastructure
- Encryption
- Audit Controls
- Data Integrity
- Network Security
- Email Security
- Remote Access Policies
- Portable Device Policies
- VPN Policies
- Wireless Security Policies