

SECURITY

MEASURES



AXDRAFT
An Onit Company

WE PROTECT YOUR DATA
BETTER
THAN YOUR BANK DOES

Security tops the list of companies' concerns when it comes to legal technology. 50% of legal experts claim that confidentiality is the key factor driving their decision-making when adopting new cloud software.

Knowing that, we've made data protection a #1 priority at **AXDRAFT**. We value the trust of every client, and for that, we endlessly improve our platform security.

AXDRAFT'S

Baseline Security

SOC-2 CERTIFICATION

This proves that **AXDRAFT** manages data under the security protocols, protects the interests, and guarantees data integrity to all clients. The main areas subject to the certification are Policies, Communications, Procedures, and Monitoring. To get certified, we needed to comply in all of these areas.

TLS 1.2+ AND AES-256 DATA ENCRYPTION

This protocol secures data transmission over the Internet. As a SaaS solution, **AXDRAFT** website connection is encrypted and authenticated using a strong protocol, key exchange, and cipher. Our databases, template files, and even the disks of our servers are stored in an encrypted state.

CLOUD-BASED DEPLOYMENT

AXDRAFT is a Software-as-a-Service solution, which means it is deployed on third-party servers: US-hosted Google Cloud and AWS. We use backup servers across multiple locations to ensure **AXDRAFT** remains operational in case of local outages.

GDPR COMPLIANCE

AXDRAFT operates in compliance with the PCI/PII standards in EU and GDPR which has gone into effect May 25th.

ON-DEMAND FIELD-LEVEL DATABASE ENCRYPTION

We offer encryption of confidential data in the database itself. Encryption keys are unique to each client and are stored exclusively on servers that encrypt information.

SECURED COMMUNICATION AND USAGE AUDIT

All communication inside **AXDRAFT** is encrypted and is not distributed across any third-party services. **AXDRAFT** also maintains an audit of user actions to help identify unauthorized behavior.

SOME OF THE STEPS AXDRAFT TAKES TO MAINTAIN DATA SECURITY

MULTI-FACTOR AUTHENTICATION:

All AXDRAFT employees must use multi-factor authentication to authenticate to corporate accounts whenever available. AXDRAFT provides two-factor authentication to its users to protect sensitive data.

BACKGROUND CHECKS:

Background checks are performed on new hires before the new hire's start date, as permitted by local laws. The results are reviewed by HR and appropriate action is taken if deemed necessary.

SECURITY TRAINING:

AXDRAFT has established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with the Company's security policies and procedures, including the identification and reporting of incidents. All full-time employees are required to regularly complete these trainings.

USER ACCESS CONTROLS:

Prior to issuing system credentials and granting system access, AXDRAFT registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by AXDRAFT, user system credentials are removed when user access is no longer authorized. AXDRAFT authorizes access to information resources, including data and the systems that store or process customer data, based on the principle of least privilege.

CUSTOMER DATA POLICIES:

Company management has approved AXDRAFT policies that detail how customer data may be made accessible and should be handled. These policies are accessible to all employees and contractors.

VENDOR MANAGEMENT:

AXDRAFT team collects and reviews the SOC reports (or equivalent) of its sub-service organizations and software vendors.

SECURITY POLICIES:

AXDRAFT's security policies outline requirements for securing the company's operations, services, and systems.

INTERNAL CONTROL TOOL:

AXDRAFT uses an automated tool that objectively and continuously monitors AXDRAFT's control environment and alerts management when internal control and security issues arise.

PENETRATION TESTING:

AXDRAFT engages third-parties to regularly conduct penetration tests of the production environment. Results are reviewed by management and findings are tracked to resolution.

EMPLOYEE DEVICE SECURITY:

All mobile and computing devices used by employees that connect to the internal network comply with the Asset Management Policies. Employees must encrypt their devices, and must not interfere or otherwise reduce the level of encryption on their devices.

DATABASE BACKUPS:

Backups are performed daily and retained in accordance with a pre-defined schedule in the Backup Policy.

PASSWORD PROTECTION:

Employees must use a password manager to avoid insecure or shared passwords with accounts.



AXDRAFT
An Onit Company

“

Axdraft is very easy to use and produces documents quickly. It is entirely customizable, and customer support is extremely responsive. In our case it allows attorneys to be more productive and less reliant on the availability of a legal assistant to draft estate planning documents and probate pleadings and related documents. The system could be used for any practice area where the same or similar documents are prepared on a regular basis.

Amy L.
Attorney & Managing Member
Law Practice

”

For any specific policies

(Acceptable Use Policy, Code of Conduct,

Data Protection Policy, Change Management Policy, Risk Assessment Policy)

or if you'd like a copy of our SOC-2 certification report,

please feel free to reach out to us

at security@axdraft.com.

If you'd like to see **AXDRAFT** in action and the way we implement our security policies inside our platform, please **book a demo** and we'll be happy to show you.