August

Security Whitepaper

How August protects your data, your matters, and your professional obligations.

- SOC 2 Type II
- ISO 27001:2022
- Annual Pen Testing
- CASA Verified

v1.1 · May 2026
august.law

CONFIDENTIAL

CONTENTS

SECTION 01

Executive Summary

August is a legal AI workspace built for law firms and in-house legal teams handling sensitive, privileged, and regulated information. Security is the foundation the platform is built on, verified by independent auditors and tested by third-party firms.

> August holds SOC 2 Type II and ISO 27001:2022 certifications, operates single-tenant architecture by default, never trains on customer data, and encrypts all data with AES-256 at rest and TLS 1.2+ in transit.

This whitepaper covers how August protects client data at the infrastructure, application, AI model, and operational layers. The claims here are backed by SOC 2 Type II and ISO 27001 audits, third-party penetration testing, and contractual commitments that are enforceable under your customer agreement.

99.9%	30 min	7 days
Monthly uptime commitment	Critical issue response time	Critical CVE remediation SLA

For legal professionals, security is an ethical obligation. August is designed to support attorney-client privilege, professional confidentiality, and regulatory compliance without requiring firms to change how they work.

Document version 1.1 · Effective May 2026 · Owner: August Security Team · Contact: legal@august.law

SECTION 02

Your Data is Never Used for Training

> **No customer prompts, outputs, metadata, or derived data are used by August or any of its subprocessors for model training, fine-tuning, analytics, or product improvement. This is contractually enforced.**

This prohibition is set out in August's Platform Agreement and Data Processing Addendum (DPA), and is contractually flowed down to every subprocessor:

- ✓ Documents, prompts, and work product uploaded to or generated within August are never used for training.
- ✓ Foundation model providers process data ephemerally. They do not store, log, review, or reuse your content.
- ✓ Metadata and derived data (usage patterns, query structures, analytical byproducts) are excluded from all training pipelines.
- ✓ August employees do not have visibility into user inputs, uploads, or outputs.
- ✓ Even within a firm, user profiles are fully siloed unless content is proactively shared.

Subprocessors

Each subprocessor is contractually bound to data use restrictions. Copies of specific clauses are available under NDA.

SUBPROCESSOR	ROLE	DATA TRAINING
Amazon Web Services	Infrastructure and hosting	**Prohibited**
Microsoft Corporation	Office integration framework	**Prohibited**
OpenAI LLC	Foundation model provider	**Prohibited**
Google Cloud Platform	Compute services	**Prohibited**
Anthropic (via AWS Bedrock)	Foundation model provider (BYOK)	**Prohibited**

SECTION 03

Single-Tenant Isolation

August operates a single-tenant architecture by default. Each customer's data is maintained in its own isolated environment. There is no co-mingling of data between customers.

What This Means in Practice

- ✓ Your firm's data lives in a dedicated environment, not shared infrastructure with other customers.
- ✓ Logical separation controls enforce tenant boundaries at the application, database, and storage layers.
- ✓ Data residency is pinned to your selected geographic region and enforced at the infrastructure level.
- ✓ Optional VPC or on-premises deployment for firms requiring additional isolation.

Intra-Firm Isolation

Isolation extends within your firm. August's Personas feature enforces hard client/matter-level walls and role-based access controls. Data is segregated not only between tenants but between matters within your own organization. One partner cannot see another partner's prompts, uploads, or outputs unless content is explicitly shared or placed in a shared Project workspace.

> August operates single-tenant architecture by default. Many commonly used legal SaaS tools, including practice management and document management platforms, typically operate multi-tenant architectures with shared infrastructure. August's per-matter ethical walls add an additional layer of isolation that is uncommon in the category.

SECTION 04

Encryption and Key Management

LAYER	STANDARD	DETAIL
Data at rest	AES-256 or better	All stored documents, database records, and backups
Data in transit	TLS 1.2 or better	All communication between clients, servers, and APIs
Key rotation	Annual	Encryption keys rotated on a defined schedule
Key protection	HSMs	Hardware security modules protect all encryption keys

Encryption is applied across the platform: the web application, Word and Outlook add-ins, DMS integrations, and API connections. All data paths are encrypted by default.

Access Control and Ethical Walls

Authentication

- ✓ SSO via SAML, OIDC, and OAuth2
- ✓ Multi-factor authentication (MFA) enforced
- ✓ SCIM Integration for automated user provisioning and deprovisioning, synced with your identity provider

Authorization

- ✓ Role-based access controls (RBAC)
- ✓ Matter-level ethical walls via Personas
- ✓ Admin controls for permissions and workspaces
- ✓ Quarterly access reviews

Audit Trails

Comprehensive audit trails log all system activity: user actions, AI outputs, document access, and administrative changes. Every action is attributable to a specific user. Retention is configurable from 1 to 10 years, with logs protected against tampering.

SECTIONS 05 & 06

Internal Controls & AI Model Security

How August protects production systems from internal and external threats, and how AI model interactions are secured at every layer.

∅	∅	∅
Customer data on employee devices	Model providers that retain your data	Admin-privileged service roles

SECTION 05

Internal Access Controls

- Production data access limited to a defined set of engineers on a least-privilege, just-in-time basis.
- Every production access event is logged and reviewed.
- Customer documents are never stored on employee workstations.
- Engineering workflows use anonymized or synthetic data. Real data access requires explicit approval.
- All company-issued laptops run MDM, EDR (daily signature updates), and full-disk encryption.
- Production access requires SSO, MFA, and short-lived credentials. No persistent tokens.
- No service roles have administrator privileges. All apps run on scoped IAM roles.
- CI/CD deployment via OIDC. No long-lived credentials in pipelines.

AI Model Security

August routes all AI requests through a secure gateway with policy enforcement. This gateway controls which models receive which data, enforces data boundaries, and ensures no customer content leaves the security perimeter without explicit controls.

- ✓ Zero data retention by external model providers. Prompts and outputs are processed ephemerally.
- ✓ No cross-user or cross-matter data exposure. Each request is scoped to a single user and matter.
- ✓ Multi-model redundancy across providers. Automatic failover if one provider has issues.
- ✓ BYOK (Bring Your Own Key) deployment via AWS Bedrock for complete credential control.
- ✓ Optional isolated or private model environments for maximum separation.

SECTION 06

AI Risk and Accuracy Controls

AI Risk Controls

Prompt Injection Protection

Incoming documents and inputs are processed through controlled pipelines with permission boundaries that limit blast radius if adversarial content is encountered. Audit logging captures unusual model behavior for review.

Output Guardrails

AI responses are scoped to the user's matter context and authorized knowledge sources. Cross-matter and cross-user content leakage is architecturally prevented.

August's AI processing aligns with NIST AI Risk Management Framework principles for transparency, accountability, and reliability in high-stakes applications.

Accuracy and Hallucination Controls

- Modular AI agents configured to match firm-specific decision criteria and local statutes.
- Human-in-the-loop feedback mechanisms for attorneys to refine outputs.
- Firm-specific onboarding co-built by attorneys and engineers until outputs meet firm standards.
- DMS integration (NetDocs, iManage, SharePoint, Google Drive, Dropbox) configurable to restrict outputs to validated documents.
- Personas memory layer retains format preferences, recurring facts, and style guidance.

SECTION 07

Certifications and Audits

CERTIFICATION / AUDIT	STATUS	DETAIL
SOC 2 Type II	Current	Unqualified opinion. Full report available under NDA. Bridge letter on file.
ISO 27001:2022	Certified	Issued to Credicle Corporation dba August. Certificate on request.
CASA	Verified	Cloud Application Security Assessment compliance confirmed.
Penetration Testing	Annual	Black-box and grey-box assessments by independent third parties. Most recent: Aug 2025.
Continuous Monitoring	Active	Vanta platform for automated compliance monitoring and evidence collection.

Vulnerability Management

- Critical CVEs tracked against a 7-day remediation SLA, addressed outside the regular release cycle.

- Quarterly baseline security review cycle for non-critical vulnerabilities.
- Continuous vulnerability scanning and dependency scanning as part of the secure SDLC.
- Hardened base images for infrastructure, rebuilt and redeployed rather than patched in place.
- Vulnerability scan reports and patch deployment logs available under audit-rights clause.

SECTION 08

Infrastructure and Resilience

August runs on Amazon Web Services (AWS). The architecture prioritizes managed and serverless services to minimize attack surface:

- RDS-managed PostgreSQL (AWS handles underlying OS patching).
- AWS Lambda for serverless compute.
- Guest OS instances use hardened base images, rebuilt and redeployed rather than patched in place.

- No service roles have administrator privileges. All services run on scoped IAM roles.
- CI/CD deployment via OIDC-based GitHub Actions. No long-lived credentials in pipelines.

Resilience

- Multi-AZ redundancy within each region
- Automated backups with defined RTO/RPO
- 24/7 monitoring and alerting
- Continuous logging with anomaly detection
- Formal IR and BC/DR plans

Endpoint Security

- All laptops enrolled in MDM
- EDR with daily signature updates
- Full-disk encryption on all devices
- Non-compliant devices flagged and remediated
- Mobile: comms only, no production access

Personnel and Organizational Security

- Background checks conducted for all employees with access to production systems.
- Security awareness training required for all staff.
- Secure development lifecycle (SDLC) with mandatory code review and dependency scanning.
- Change management: all production changes require peer review and approval before deployment.

SECTION 09

Product Security

Microsoft Word Add-in

- ✓ Built on Microsoft Office Add-in framework
- ✓ Operates within your M365 security boundary
- ✓ SSO via SAML / OAuth
- ✓ No local file storage
- ✓ Sandboxed execution

Outlook Integration

- ✓ No passive inbox access
- ✓ No background syncing or indexing
- ✓ Session-based processing only
- ✓ Explicit user-triggered actions
- ✓ M365 environment stays isolated

Integration Security

All integrations authenticate via OAuth 2.0. August never stores user passwords for any connected service. Tokens are scoped to the minimum permissions required and can be revoked by the customer at any time.

Document Management Integrations

August integrates securely with the DMS platforms law firms rely on:

iManage	NetDocs	SharePoint	OneDrive
Google Drive	Dropbox	Box	More on roadmap

Live Assist

August's Live Assist feature enables real-time collaboration between attorneys and AI. When Live Assist sessions involve audio or screen recording, the customer is responsible for obtaining appropriate consent from all participants in accordance with applicable recording laws and firm policy.

Data Residency and Deployment Options

DEPLOYMENT MODEL	DESCRIPTION
Standard (AWS Cloud)	Single-tenant environment in customer-selected AWS region. Data residency enforced at the infrastructure level.
Regional Pinning	Data stored and processed exclusively in the specified geographic region.
Behind Firewall	August deployments can run behind a firm's internal firewall.
VPC / Private Cloud	Dedicated Virtual Private Cloud for network-level isolation.
On-Premises	Full on-premises deployment for firms prohibiting cloud-hosted solutions.

SECTION 11

Compliance and Privacy

REQUIREMENT	AUGUST'S POSITION
GDPR	August acts as a data processor. DPA executed with each customer. SCCs for international transfers. Key subprocessors (AWS, Microsoft, Google) are EU-US DPF certified.
CCPA	Compliant. August acts as a service provider under CCPA.
DPA	Available for all customers. Covers processing purposes, security measures, sub-processor obligations, deletion, breach notification, audit rights, and DSAR procedures.
DPIA	Data Protection Impact Assessment maintained for AI processing of sensitive legal data.
Breach Notification	August notifies affected customers within 72 hours of confirming a security incident involving their data.
Right to Deletion	Customers can delete all data at any time. DSARs processed per DPA terms.
Subprocessor Changes	Customers notified in advance and may object per DPA terms.
Attorney-Client Privilege	Ethical walls, matter-level isolation, zero-training, and configurable data residency for regulated professionals.

SECTION 12

SLA and Shared Responsibility

METRIC	COMMITMENT
Platform Uptime	99.9% monthly
Critical Issue Response	30 minutes
Critical CVE Remediation	7 days
AI Provider Failover	Automatic routing to alternative model provider
Audit Rights	100-question annual audit allowance (Security Addendum, Section 10)
Audit Log Retention	Configurable: 1 to 10 years
Data Deletion	Available at any time on customer request

Shared Responsibility

Security is a partnership. The table below clarifies ownership:

AUGUST OWNS	CUSTOMER OWNS
Platform infrastructure, encryption, patching	Managing SSO provider and identity lifecycle
Tenant isolation and data segregation	Configuring matter-level ethical walls and RBAC
AI model security and zero-training enforcement	Training users on appropriate use of AI tools
Audit logging and tamper protection	Setting retention policies and reviewing logs
Vulnerability management and incident response	Reporting suspected security issues promptly
Certifications and compliance	DPA signing, DSAR forwarding, regulatory obligations

SECTION 13

Documents Available on Request

The following documents are available to customers and prospective customers. Documents marked NDA require a signed non-disclosure agreement.

DOCUMENT	ACCESS
SOC 2 Type II Report (full audit)	NDA
SOC 2 Bridge Letter	NDA
ISO 27001:2022 Certificate	On request
CASA Compliance Documentation	On request
Penetration Test Report (most recent: Aug 2025)	NDA
Data Processing Addendum (DPA)	On request
Platform Agreement (security commitments)	On request
Security Addendum (incl. audit rights)	On request
Subprocessor List	On request
Environment / Architecture Diagram	On request
Security Questionnaire Responses (SIG, CAIQ)	On request

To request documents or schedule a security review

legal@august.law

legal@august.law

august.law

v1.1 · May 2026