unsettled

# Cloud Infrastructure Architecture & Security Documentation

AWS Production Environment — Technical Reference

SOC 2 TYPE II | CONFIDENTIAL | AWS US-EAST-1

Prepared for: SOC 2 Audits · Client Due Diligence · Internal IT Reference Document Date: May 12, 2026

Version 1.0

# Table of Contents

SECTION 1

# Executive Summary

Unsettled.io operates a cloud-native production environment hosted entirely on Amazon Web Services (AWS) in the **us-east-1 (N. Virginia)** region. The infrastructure is purpose-built for the secure processing of sensitive consumer financial data submitted by client organizations for debt settlement compliance workflows.

This document provides a comprehensive technical reference of the production infrastructure, covering network topology, security controls, access management, logging, and data protection. It is intended for use in SOC 2 Type II audits, client security due diligence reviews, and by internal IT operations staff.

## Environment Purpose

The production environment hosts two customer-facing applications:

**Marketing Site**

| | |
|---|---|
| URL | `unsettled.io` |
| Technology | Next.js 15 (Node 20) |
| Process manager | PM2 |

**Client Portal**

| | |
|---|---|
| URL | `portal.unsettled.io` |
| Technology | Laravel 11 / PHP 8.3 |
| Database | MySQL 8.0 (RDS) |

## Security Posture Summary

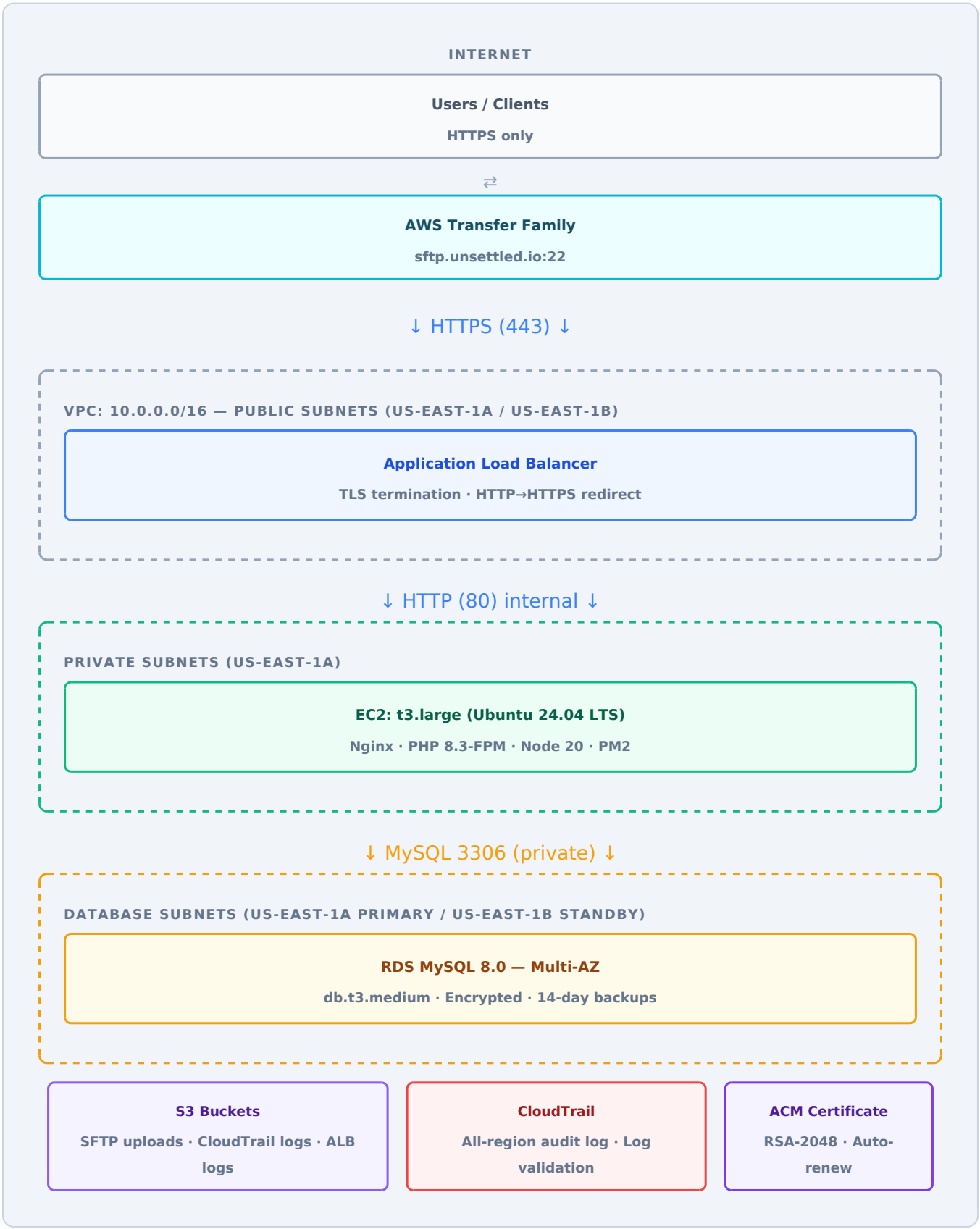
- **No public SSH access** — all administrative access via AWS Systems Manager Session Manager only
- **Encryption in transit** — TLS 1.2+ enforced at the Application Load Balancer; HTTP redirects to HTTPS
- **Encryption at rest** — all EBS volumes and RDS instances encrypted with AWS-managed KMS keys
- **Network isolation** — application server and database reside in private subnets with no direct internet exposure
- **Multi-AZ database** — automatic failover across two Availability Zones
- **Immutable audit trail** — AWS CloudTrail enabled across all regions with log file validation
- **SFTP via managed service** — AWS Transfer Family eliminates SSH daemon exposure on the application server

> **Data sensitivity:** The portal processes files containing consumer Social Security Numbers (SSNs). SSNs are stored as irreversible one-way HMAC-SHA256 hashes (server-side pepper key) before being written to the database. Stored values cannot be decrypted — hit detection hashes at query time.

SECTION 2

# Architecture Overview

## 2.1 System Components



# Architecture Overview

## 2.2 Traffic Flow

### WEB TRAFFIC (HTTPS)

All inbound web requests arrive at the **Application Load Balancer** over HTTPS (port 443). The ALB terminates TLS using the ACM-managed certificate, then forwards requests over plain HTTP (port 80) on the internal VPC network to the EC2 application server. The EC2 instance is in a private subnet and has no public IP address — it is unreachable directly from the internet.

### SFTP FILE UPLOADS

Clients who upload files via SFTP connect to **sftp.unsettled.io:22**, which resolves to the AWS Transfer Family endpoint. Transfer Family handles the SSH/SFTP protocol, authenticates users via SSH key pairs, and writes uploaded files directly to an encrypted S3 bucket. The application server polls this bucket to ingest and process new files — no SFTP daemon runs on the EC2 instance itself.

### OUTBOUND TRAFFIC

The application server routes all outbound internet traffic (package updates, AWS API calls) through the **NAT Gateway** in the public subnet. The NAT Gateway has a static Elastic IP address, providing a consistent egress IP for allow-listing purposes.

SECTION 3

# Network Architecture

## 3.1 VPC Design

| | |
|---|---|
| VPC ID | *[internal]* |
| CIDR Block | `10.0.0.0/16` |
| Region | us-east-1 (N. Virginia) |
| DNS Hostnames | Enabled |
| DNS Resolution | Enabled |
| Internet Gateway | *[internal]* |
| NAT Gateway | *[internal]* |

## 3.2 Subnet Layout

The VPC is divided into three tiers across two Availability Zones, providing network-level isolation between internet-facing, application, and database workloads.

| Subnet Name | Subnet ID | CIDR | AZ | Tier | Internet Route |
|---|---|---|---|---|---|
| `unsettled-public-a` | *[internal]* | `10.0.1.0/24` | `us-east-1a` | **Public** | Internet Gateway |
| `unsettled-public-b` | *[internal]* | `10.0.2.0/24` | `us-east-1b` | **Public** | Internet Gateway |
| `unsettled-private-a` | *[internal]* | `10.0.11.0/24` | `us-east-1a` | **Private** | NAT Gateway |
| `unsettled-private-b` | *[internal]* | `10.0.12.0/24` | `us-east-1b` | **Private** | NAT Gateway |
| `unsettled-db-a` | *[internal]* | `10.0.21.0/24` | `us-east-1a` | **Isolated** | None |
| `unsettled-db-b` | *[internal]* | `10.0.22.0/24` | `us-east-1b` | **Isolated** | None |

SECTION 3 (CONTINUED)

# Network Architecture

## 3.3 Security Groups

Three security groups implement a layered, least-privilege firewall model. Each group allows only the traffic required for its role; all other inbound traffic is implicitly denied.

### unsettled-sg-alb — ALB

| | |
|---|---|
| Inbound TCP 80 | 0.0.0.0/0 (any) |
| Inbound TCP 443 | 0.0.0.0/0 (any) |
| Outbound | All traffic |

Accepts public web traffic. Port 80 traffic is immediately redirected to HTTPS by the ALB listener rule.

### unsettled-sg-ec2 — App Server

| | |
|---|---|
| Inbound TCP 80 | sg-alb only |
| Inbound TCP 443 | sg-alb only |
| Inbound TCP 22 | Not permitted |
| Outbound | All traffic |

Only accepts traffic from the ALB security group. No SSH port open; admin access via SSM only.

### unsettled-sg-rds — Database

| | |
|---|---|
| Inbound TCP 3306 | sg-ec2 only |
| All other inbound | Not permitted |

The database is accessible exclusively from the application server. No public access is possible.

SECTION 4

# Compute — Application Server

### EC2 Instance Specification

| | |
|---|---|
| Instance ID | *[internal]* |
| Instance Type | t3.large (2 vCPU, 8 GiB RAM) |
| AMI | *[internal]* |
| Operating System | Ubuntu 24.04 LTS (Noble Numbat) |
| Availability Zone | us-east-1a |
| Subnet | Private (10.0.11.0/24) — no public IP |
| Private IP | *[internal]* |
| Launched | 2026-05-12 |

### Storage

| | |
|---|---|
| Volume type | gp3 (SSD) |
| Volume size | 40 GiB |
| Encryption | Enabled (AWS-managed KMS key) |
| Delete on termination | Enabled |

## Software Stack

### Web Server

- Nginx 1.24 (reverse proxy)
- PHP 8.3-FPM (portal backend)
- Node.js 20 LTS (marketing site)
- PM2 (Node process manager)

### Application

- Laravel 11 / PHP 8.3
- Next.js 15
- Composer (PHP deps)
- AWS SDK for PHP v3

## Administrative Access

**SSH is disabled.** Port 22 is not open in the EC2 security group. All administrative shell access is performed exclusively via **AWS Systems Manager (SSM) Session Manager**, which provides a browser-based or CLI terminal session authenticated through IAM, fully logged in CloudTrail, and requires no open inbound ports.

# Compute — Application Server

## IAM Instance Role

The EC2 instance is assigned an IAM role (**unsettled-ec2-role**) that grants the minimum permissions required for operation:

- **AmazonSSMManagedInstanceCore** — Systems Manager access for remote administration
- **CloudWatchAgentServerPolicy** — CloudWatch metrics and log shipping
- **unsettled-s3-deploy** — Read access to the deployment S3 bucket
- **unsettled-sftp-management** — Transfer Family user lifecycle management + S3 SFTP bucket read

The instance does not use long-term access keys. All AWS SDK calls use the instance metadata service (IMDSv2, tokens required) to obtain temporary credentials automatically rotated by AWS.

SECTION 5

# Database

### RDS Instance Specification

| | |
|---|---|
| Identifier | `unsettled-portal-db` |
| Engine | MySQL 8.0.45 |
| Instance Class | db.t3.medium (2 vCPU, 4 GiB RAM) |
| Endpoint | *[internal hostname]* |
| Port | 3306 |
| Multi-AZ | Yes — automatic failover to us-east-1b standby |
| Storage | 20 GiB gp3 (auto-scaling enabled) |
| Encryption at rest | Enabled (AWS-managed KMS key) |
| Publicly accessible | No — isolated subnet, no public endpoint |
| Deletion protection | Enabled |

## Backup Configuration

| | |
|---|---|
| Automated backups | Enabled — retained for 14 days |
| Backup window | 03:00–04:00 UTC daily |
| Maintenance window | Monday 04:00–05:00 UTC |
| Point-in-time recovery | Supported — restore to any point within retention window |

## High Availability

The RDS instance is deployed in a Multi-AZ configuration. AWS automatically maintains a synchronous standby replica in **us-east-1b**. In the event of an infrastructure failure, AZ outage, or maintenance event, RDS automatically fails over to the standby with no application configuration changes required. DNS for the endpoint is automatically updated. Typical failover time is 60–120 seconds.

# Database

## Application-Level Encryption

The portal applies field-level protection to sensitive data before writing to the database. The protection method differs by data type:

- Consumer SSNs (upload records and DSC inventory) — stored as irreversible HMAC-SHA256 hashes using PHP hash_hmac() with a server-side pepper key (SSN_HASH_KEY). Values cannot be decrypted back to plaintext.
- SFTP SSH private keys — AES-256-CBC encryption via Crypt::encryptString().

SECTION 6

# Load Balancing & TLS

### Application Load Balancer

| | |
|---|---|
| Name | `unsettled-alb` |
| ARN | *[internal]* |
| DNS Name | *[internal hostname]* |
| Scheme | Internet-facing |
| Availability Zones | us-east-1a, us-east-1b (public subnets) |
| Deletion protection | Enabled |
| Access logging | S3 bucket (encrypted, access-blocked) |

## Listeners

### Port 443 — HTTPS

| | |
|---|---|
| TLS Policy | ELBSecurityPolicy-TLS13-1-2-2021-06 |
| Min TLS version | TLS 1.2 |
| TLS 1.3 | Supported |
| Action | Forward → target group |

### Port 80 — HTTP

| | |
|---|---|
| Action | 301 redirect to HTTPS |
| Permanent redirect | Yes (HTTP 301) |

All plaintext HTTP connections are immediately and permanently upgraded to HTTPS.

## TLS Certificate

| | |
|---|---|
| Provider | AWS Certificate Manager (ACM) |
| Algorithm | RSA 2048-bit |
| Domains covered | unsettled.io, portal.unsettled.io |
| Validation method | DNS (Route 53 CNAME records) |
| Expiry | 2026-11-25 (auto-renews via ACM) |
| Status | **ISSUED** |

ACM certificates are automatically renewed by AWS before expiry. No manual certificate management is required.

SECTION 7

# SFTP File Transfer

Client file uploads via SFTP are handled by **AWS Transfer Family**, a fully managed SFTP service. This architecture eliminates the need to run an SSH daemon on the application server, removing port 22 exposure from the EC2 instance entirely.

**Transfer Family Server**

| | |
|---|---|
| Server ID | *[internal]* |
| Endpoint | *[internal hostname]* |
| Hostname (DNS) | `sftp.unsettled.io` |
| Protocol | SFTP (SSH File Transfer Protocol) |
| Port | 22 |
| Identity provider | Service-managed |
| Authentication | SSH public key (RSA 3072-bit key pairs) |
| Status | ONLINE |

**SFTP Storage Bucket**

| | |
|---|---|
| Bucket | unsettled-sftp |
| Encryption | SSE-S3 (AES-256) |
| Versioning | Enabled |
| Public access | Blocked (all public access denied) |
| User path structure | `/{username}/upload/` |

## User Isolation

Each portal user who enables SFTP receives a dedicated Transfer Family user account. IAM policy conditions using  ensure each user can only read and write to their own S3 prefix. No user can access another user's files.

## Key Management

When a user provisions SFTP access, the portal generates a **3072-bit RSA key pair** server-side. The public key is registered with Transfer Family. The private key is displayed to the user once and encrypted with AES-256 before storage. Users use the private key file to authenticate their SFTP client — no passwords are used.

# SFTP File Transfer

## File Processing Flow

1. User uploads file to `sftp.unsettled.io` → Transfer Family → S3 bucket
2. Scheduled job on application server polls S3 for new files (hourly, or on-demand)
3. New files are downloaded, processed through the file pipeline, and stored
4. Processed file fingerprint (name + size) recorded to prevent duplicate imports

SECTION 8

# Identity & Access Management

## AWS IAM Roles

| Role Name | Principal | Purpose | Policies |
|---|---|---|---|
| unsettled-ec2-role | ec2.amazonaws.com | Application server instance profile | SSMManagedInstanceCore, CloudWatchAgentServerPolicy, custom S3/Transfer policies |
| unsettled-sftp-user-role | transfer.amazonaws.com | Assumed by Transfer Family per-user; scoped S3 access via | Custom S3 read/write restricted to user prefix |
| unsettled-sftp-logging-role | transfer.amazonaws.com | Transfer Family CloudWatch logging | AWSTransferLoggingAccess |

## Application Authentication

### Portal User Authentication

| | |
|---|---|
| Method | Username + password + TOTP MFA (mandatory) |
| Password hashing | bcrypt (cost factor 12) |
| MFA | Time-based OTP (Google Authenticator / compatible apps) |
| Session timeout | 30 minutes of inactivity |
| Session encryption | Enabled (Laravel encrypted sessions) |
| API authentication | Bearer tokens (API keys) with per-key scoping |

## Role-Based Access Control (Portal)

### Administrator

- Manage users and clients
- View all upload history
- Access audit log
- Manage DSC companies
- Generate and view invoices
- Provision/deprovision SFTP for any user

### Standard User

- Upload and view own files
- Download result files and certificates
- Manage own SFTP credentials
- Manage own API keys
- Configure own file retention period

SECTION 9

# Logging & Monitoring

## AWS CloudTrail

| | |
|---|---|
| Trail name | `unsettled-trail` |
| Coverage | All AWS regions (multi-region trail) |
| Log file validation | Enabled — SHA-256 digest files for tamper detection |
| Storage | S3 bucket (encrypted, versioning enabled) |
| S3 encryption | SSE-S3 (AES-256) |
| S3 versioning | Enabled |
| Public access | Blocked |

CloudTrail records all AWS API calls made by IAM users, roles, and AWS services. This provides a complete, immutable record of infrastructure changes, access events, and administrative actions. Log file validation using SHA-256 digests allows detection of any post-delivery log tampering.

## ALB Access Logs

| | |
|---|---|
| Storage | S3 bucket (encrypted) |
| Contents | Client IP, timestamp, request path, response code, latency, TLS version, user agent |

## Application Audit Log

The portal application maintains its own audit log in the database, recording application-level security events:

- User login and logout events
- File uploads, downloads, and deletions (with certificate of destruction)
- User account creation, modification, and deletion
- Client account changes
- SFTP provisioning, deprovisioning, and key resets
- API key creation and revocation

# Logging & Monitoring

## S3 Buckets Summary

| Bucket Name | Purpose | Encryption | Versioning | Public Access |
|---|---|---|---|---|
| unsettled-cloudtrail-logs | CloudTrail audit logs | SSE-S3 | Enabled | Blocked |
| unsettled-alb-logs- | ALB access logs | SSE-S3 | — | Blocked |
| unsettled-sftp- | SFTP file uploads (Transfer Family) | SSE-S3 | Enabled | Blocked |
| unsettled-deploy- | Application deployment artifacts | SSE-S3 | — | Blocked |

SECTION 10

# Backup & Recovery

## Database Backups

| Attribute | Configuration |
|---|---|
| Automated daily snapshots | Enabled — retained for 14 days |
| Backup window | 03:00–04:00 UTC |
| Point-in-time recovery | Supported — any second within retention window |
| Manual snapshots | On demand before major changes; retained indefinitely |
| Backup encryption | Encrypted with same KMS key as source instance |
| Cross-region copy | Available on demand |

## Uploaded File Data

User-uploaded files and processed results are stored on the EC2 EBS volume. The EBS volume is encrypted at rest. For additional durability, the SFTP bucket (S3) has versioning enabled. Future consideration: migrate application file storage to S3 for native durability (11 nines) and cross-region replication.

## Multi-AZ Failover

The RDS Multi-AZ standby provides automatic, synchronous failover for database availability:

- RTO (Recovery Time Objective): ~60–120 seconds for database failover
- RPO (Recovery Point Objective): Zero data loss — synchronous replication
- Failover is automatic — no manual intervention required
- Application reconnects automatically via the stable DNS endpoint

## Disaster Recovery Considerations

> **Current state:** The application server (EC2) is a single instance in us-east-1a. In an AZ failure, the EC2 instance would be unavailable until manually launched in another AZ. The database would automatically fail over via Multi-AZ. RTO for a full EC2 failure is estimated at 15–30 minutes (launch new instance from AMI, restore application from deployment pipeline).

SECTION 11

# Data Protection

## Encryption Summary

| Data | At Rest | In Transit |
|---|---|---|
| Database (MySQL) | KMS-encrypted RDS volume | TLS within VPC; connection required |
| SSNs (upload records & DSC inventory) | HMAC-SHA256 one-way hash (server-side pepper) + KMS (RDS layer) | TLS |
| EC2 application files | KMS-encrypted EBS gp3 volume | N/A (internal) |
| SFTP uploads (S3) | SSE-S3 (AES-256) | TLS (SFTP/SSH, HTTPS) |
| CloudTrail logs (S3) | SSE-S3 (AES-256) | TLS |
| Web traffic | N/A | TLS 1.2+ (ALB, ACM cert) |
| SFTP SSH keys | | TLS |

## Data Retention

- Users can configure file retention periods of 1–90 days per account
- A scheduled job purges expired uploads and their associated data automatically
- Deleted files generate a **Certificate of Destruction** PDF documenting the deletion event, timestamp, and file hash
- Deletion records are retained in the database even after file data is removed

## Data Isolation

- Each portal user can only access their own uploaded files and results
- SFTP users are scoped to their own S3 prefix via IAM conditions
- Client organizations are logically isolated — users see only data belonging to their client account
- Admin users have cross-account visibility for support and compliance purposes

SECTION 12

# SOC 2 Control Mapping

The following table maps the infrastructure controls described in this document to the SOC 2 Trust Services Criteria (TSC) under the Security (CC) and Availability (A1) categories.

| Criteria | Control Description | Implementation |
|---|---|---|
| **CC6.1** | Logical access security controls | Username + password + mandatory TOTP MFA for portal access. API key authentication for programmatic access. bcrypt (cost 12) password hashing. 30-minute session timeout. |
| **CC6.2** | Credentials and authentication | No shared credentials. Each user has unique credentials. SFTP uses individual RSA 3072-bit key pairs — no shared passwords. AWS IAM roles use temporary credentials (no long-term access keys on EC2). |
| **CC6.3** | Role-based access control | Admin and standard user roles with clearly delineated permissions. IAM roles scoped to minimum required permissions. SFTP IAM policy restricts each user to their own S3 prefix. |
| **CC6.6** | Network access restrictions | EC2 and RDS in private subnets. Security groups enforce least-privilege: EC2 accepts traffic only from ALB; RDS accepts MySQL only from EC2. No public IPs on application or database tier. No SSH port open. |
| **CC6.7** | Transmission integrity and encryption | TLS 1.2+ enforced at ALB (ELBSecurityPolicy-TLS13-1-2-2021-06). HTTP permanently redirected to HTTPS. ACM certificate auto-renews. SFTP uses SSH transport encryption. Internal traffic within VPC. |
| **CC6.8** | Prevention of unauthorized disclosure | All storage encrypted at rest (KMS for EBS and RDS; SSE-S3 for all S3 buckets). SSNs stored as irreversible HMAC-SHA256 hashes (application layer). All S3 buckets block public access. No data exposed via public endpoints |
| **CC7.1** | System configuration | IMDSv2 required on EC2 (prevents SSRF attacks against metadata service). Deletion protection on RDS and ALB. Security groups reviewed and documented. No default VPC used for production workloads. |
| **CC7.2** | System monitoring | AWS CloudTrail enabled across all regions with log file validation. ALB access logs retained in S3. Application-level audit log records all security-relevant events. Transfer Family CloudWatch logging enabled. |
| **CC8.1** | Change management | All infrastructure changes recorded in CloudTrail. Application deployments performed via documented, repeatable process using S3 artifact staging and SSM. No direct code changes on production server. |

# SOC 2 Control Mapping

| Criteria | Control Description | Implementation |
|---|---|---|
| **CC9.2** | Risk monitoring | AWS Transfer Family eliminates SSH daemon on EC2. No port 22 on application server. Separate security groups per tier. RDS deletion protection prevents accidental data loss. |
| **A1.1** | Availability capacity | t3.large EC2 (2 vCPU, 8 GB RAM). db.t3.medium RDS (2 vCPU, 4 GB RAM). ALB spans two AZs. RDS Multi-AZ with automatic failover. NAT Gateway in dedicated public subnet. |
| **A1.2** | Backup and recovery | RDS automated daily backups with 14-day retention and point-in-time recovery. Multi-AZ synchronous replication with RPO of zero. S3 SFTP bucket versioning enabled. Estimated RTO: 15–30 min (EC2), 2 min (RDS failover). |
| **C1.1** | Confidentiality of data | User data isolated by account. SFTP files isolated by IAM prefix. SSNs stored as irreversible one-way hashes before database storage. Certificates of Destruction issued on file deletion. Configurable retention periods. |