Security Architecture

Enterprise Security Whitepaper

Version: 1.0

Date: January 2026

Classification: Public

Executive Summary

ANIMAFLOW is designed with security-first principles, implementing industry-standard security practices suitable for professional animation studios handling sensitive intellectual property. This document outlines the security architecture, compliance standards, and data protection measures.

> **Key Security Features:**
>
> - Zero-knowledge architecture - sensitive data never leaves studio premises
> - Multi-factor authentication via Google OAuth + TOTP
> - End-to-end TLS 1.3 encryption
> - SOC 2 / ISO 27001 aligned controls

Table of Contents

1. Security Standards Compliance

2. Architecture Security

3. Authentication & Authorization

4. Network Security

5. Data Protection

6. Audit & Monitoring

7. Incident Response

8. Secure Development

9. Physical Security

10. Compliance Summary

Appendix: Security Checklist for IT

1. Security Standards Compliance

1.1 SOC 2 Type II Alignment

ANIMAFLOW architecture aligns with SOC 2 Type II requirements:

Trust Service Criteria	Implementation
Security	TLS 1.3 encryption, API key authentication, 2FA
Availability	Heartbeat monitoring, automatic failover
Processing Integrity	JSON schema validation, audit logs
Confidentiality	Zero-knowledge architecture, encrypted at rest
Privacy	GDPR compliant, minimal data collection

1.2 ISO 27001 Controls

Key ISO 27001 controls implemented:

- **A.9 Access Control** - Role-based access (Admin/Artist/IT)
- **A.10 Cryptography** - AES-256 encryption, SHA-256 hashing
- **A.12 Operations Security** - Logging, monitoring, change management
- **A.13 Communications Security** - TLS 1.3, Cloudflare protection
- **A.14 System Acquisition** - Secure development lifecycle

1.3 GDPR Compliance

- No personal data stored on central servers
- All authentication via Google OAuth (user's Google account)
- Studio data remains on-premise (TrueNAS/NAS)
- Data portability: JSON format, exportable anytime

2. Architecture Security

2.1 Zero-Knowledge Design

```
┌──────────────────────────────────────────────────────────────┐
│                    ANIMAFLOW SECURITY MODEL                   │
├──────────────────────────────────────────────────────────────┤
│                                                               │
│   ┌──────────────┐          ┌──────────────┐                  │
│   │   STUDIO     │          │  CLOUDFLARE  │                  │
│   │ (On-Premise) │◄────────►│    TUNNEL    │                  │
│   │              │  TLS1.3  │              │                  │
│   │ • Project    │          │ • DDoS Prot. │                  │
│   │   Files      │          │ • WAF        │                  │
│   │ • JSON Meta  │          │ • SSL Term.  │                  │
│   │ • User Data  │          │              │                  │
│   └──────────────┘          └──────┬───────┘                  │
│          ▲                         │                          │
│          │                         ▼                          │
│          │                  ┌──────────────┐                  │
│          │                  │   ARTIST     │                  │
│          └──────────────────┤   DEVICES    │                  │
│         Direct LAN          │              │                  │
│         (Optional)          │ • Desktop    │                  │
│                             │ • Mobile     │                  │
│                             └──────────────┘                  │
│                                                               │
│  ⚠️  NO SENSITIVE DATA LEAVES THE STUDIO PREMISES              │
│                                                               │
└──────────────────────────────────────────────────────────────┘
```

> **Key Principle:** Heavy files (renders, scenes, assets) NEVER leave the studio network. Only lightweight JSON metadata is accessible remotely.

2.2 Data Flow Security

Data Type	Storage Location	Encryption	Access
Project Files (.ma, .mb, .psd)	On-premise NAS	At rest (NAS encryption)	LAN only
JSON Metadata	On-premise + API cache	TLS in transit	Authenticated users
User Credentials	Google OAuth	Google managed	OAuth tokens
2FA Secrets	Local encrypted file	AES-256	Local only
API Keys	SHA-256 hashed	One-way hash	Never stored plain

3. Authentication & Authorization

3.1 Multi-Factor Authentication (MFA)

```
┌─────────────────────────────────────────┐
│           AUTHENTICATION FLOW            │
├─────────────────────────────────────────┤
│                                          │
│  1. User clicks "Login with Google"      │
│             │                            │
│             ▼                            │
│  2. Google OAuth 2.0 Flow               │
│     • Redirect to Google                 │
│     • User authenticates                 │
│     • Token returned                     │
│             │                            │
│             ▼                            │
│  3. Email Verification                   │
│     • Check against artists.json         │
│     • Check against admins.json          │
│             │                            │
│             ▼                            │
│  4. 2FA Challenge (if enabled)          │
│     • TOTP via Google Authenticator      │
│     • 6-digit code verification          │
│     • Device remember (30 days)          │
│             │                            │
│             ▼                            │
│  5. Session Established                  │
│     • JWT token issued                   │
│     • Role-based permissions             │
│                                          │
└─────────────────────────────────────────┘
```

3.2 Role-Based Access Control (RBAC)

Role	Permissions
Admin	Full access, user management, system config
Supervisor	Project management, approve deliveries, assign tasks
Artist	View/edit assigned shots, submit reviews
IT	Server configuration, no project access
Guest	Read-only access to specific projects

3.3 API Key Security

- Keys generated with cryptographically secure random
- Stored as SHA-256 hash (irreversible)
- Transmitted only once at setup
- Rotation supported without downtime

4. Network Security

4.1 Cloudflare Protection

All external traffic passes through Cloudflare:

- **DDoS Mitigation** - Layer 3/4/7 protection
- **Web Application Firewall** - OWASP Top 10 rules
- **Bot Management** - Automated threat blocking
- **SSL/TLS** - Full (strict) mode, TLS 1.3
- **Access Control** - IP whitelisting optional

4.2 Tunnel Architecture

```
Studio Server ──→ cloudflared ──→ Cloudflare Edge ──→ Internet
                  (outbound)       (no inbound
                                    ports open)
```

> **Security Benefits:**
>
> - No open ports on studio firewall
> - No public IP exposure
> - All connections initiated from inside
> - Cloudflare handles SSL termination

4.3 Internal Network

- API server binds to localhost by default
- Cloudflared connects locally only
- Optional LAN access for high-speed transfers
- VPN compatible for remote workers

5. Data Protection

5.1 Encryption Standards

Layer	Standard	Implementation
Transport	TLS 1.3	Cloudflare managed
At Rest	AES-256	NAS-level encryption
Passwords	SHA-256 + salt	bcrypt for sensitive
2FA Secrets	AES-256-CBC	Local keyfile
Backups	AES-256	NAS snapshot encryption

5.2 Data Minimization

ANIMAFLOW collects minimal data:

Collected	NOT Collected
Email address (from Google OAuth)	Passwords (Google handles auth)
Studio ID	Payment info (Stripe handles)
Project metadata (JSON)	Project files (stays on-premise)
Usage statistics (anonymous)	Personal info beyond email

5.3 Data Retention

- Session tokens: 24 hours (configurable)
- 2FA device tokens: 30 days
- Audit logs: 90 days
- Project data: Studio controlled

6. Audit & Monitoring

6.1 Audit Logging

All security events are logged:

```
{
  "timestamp": "2026-01-30T00:10:00Z",
  "event": "login_success",
  "user": "artist@studio.com",
  "ip": "192.168.1.100",
  "device": "ANIMAFLOW-Desktop/3.0",
  "mfa_used": true
}
```

Logged Events:

- Login attempts (success/failure)
- 2FA challenges
- Permission changes
- File access (metadata only)
- API key usage
- Configuration changes

6.2 Heartbeat Monitoring

- Studio servers ping central API every 5 minutes
- Alerts on missed heartbeats
- Status dashboard for admins
- Automatic status updates

6.3 Anomaly Detection

- Failed login threshold alerts
- Unusual access patterns
- Geographic anomaly detection
- Rate limiting on sensitive endpoints

7. Incident Response

7.1 Response Procedure

1. **Detection** - Automated monitoring or user report
2. **Containment** - Revoke API keys, disable accounts
3. **Investigation** - Review audit logs
4. **Remediation** - Patch, rotate credentials
5. **Communication** - Notify affected studios
6. **Review** - Post-incident analysis

7.2 API Key Compromise

If an API key is compromised:

1. Regenerate key via dashboard
2. Update server configuration
3. Old key immediately invalidated
4. Audit log review for unauthorized access

7.3 Contact

Security issues: **security@animaflow.xyz**

8. Secure Development

8.1 Development Practices

- Code review required for all changes
- Static analysis for vulnerabilities
- Dependency scanning (CVE monitoring)
- No secrets in source code
- Environment-based configuration

8.2 Third-Party Security

Component	Security Measure
Google OAuth	Google's security infrastructure
Cloudflare	SOC 2, ISO 27001 certified
Stripe	PCI DSS Level 1
TrueNAS	ZFS checksums, encryption

9. Physical Security

9.1 On-Premise Requirements

Studios are responsible for:

- Physical server access control
- Network segmentation
- Backup power (UPS)
- Environmental controls

9.2 Recommended Setup

- Dedicated VLAN for ANIMAFLOW server
- Firewall rules: outbound HTTPS only
- Locked server room/cabinet
- Regular physical security audits

10. Compliance Summary

Standard	Status	Notes
SOC 2 Type II	✅ Aligned	Architecture follows principles
ISO 27001	✅ Aligned	Key controls implemented
GDPR	✅ Compliant	Minimal data, EU hosting available
CCPA	✅ Compliant	No personal data sale
MPAA	✅ Compatible	On-premise data storage

Appendix A: Security Checklist for IT

Pre-Deployment

- ☐ TrueNAS encryption enabled
- ☐ Dedicated VLAN configured
- ☐ Firewall rules: allow outbound 443 only
- ☐ UPS connected
- ☐ Backup schedule configured

Post-Deployment

- ☐ API key stored securely
- ☐ 2FA enabled for all admins
- ☐ Test failover procedure
- ☐ Document emergency contacts
- ☐ Schedule security review (quarterly)

Ongoing

- ☐ Monitor heartbeat status
- ☐ Review audit logs weekly
- ☐ Update software when prompted
- ☐ Rotate API keys annually
- ☐ Test backup restoration

Document History

Version	Date	Changes
1.0	January 2026	Initial release

ANIMAFLOW
Professional Animation Pipeline
https://animaflow.xyz