1. Overview

EFORCE Software delivers secure, reliable SaaS solutions hosted on Amazon Web Services (AWS) infrastructure.

This Service Level Agreement (SLA) establishes EFORCE Software's commitment to CJIS Security Policy compliance, focusing on system availability, recovery, and data integrity.

All service operations and data handling practices are aligned with CJIS Security Policy Sections 5.9 (Continuity of Operations) and 5.10 (System Availability and Backup) to ensure criminal justice information (CJI) remains protected and accessible under all operational conditions.

2. Service Availability

EFORCE Software maintains and is accountable for AWS-managed services that meet or exceed industry-standard uptime expectations. Each core component of the SaaS environment is covered under AWS's published Service Level Agreements:

- Compute (EC2): https://aws.amazon.com/compute/sla/
- EBS (Block Storage): https://aws.amazon.com/ebs/sla/
- Elastic Load Balancing: https://aws.amazon.com/elasticloadbalancing/sla/
- Network Firewall: https://aws.amazon.com/network-firewall/sla/
- Messaging (SQS/SNS): https://aws.amazon.com/messaging/sla/
- Web Application Firewall (WAF): https://aws.amazon.com/waf/sla/
- Route 53 (DNS): https://aws.amazon.com/route53/sla/
- S3 (Object Storage): https://aws.amazon.com/s3/sla/
- API Gateway: https://aws.amazon.com/api-gateway/sla/

EFORCE Service Availability Commitment:
EFORCE Software targets 99.9% monthly uptime, excluding planned maintenance.
Availability is calculated as:
Availability (%) = ((Total Minutes – Downtime Minutes) ÷ Total Minutes) × 100

Adequate notice will be given to end users for planned maintenance.
Minor Outages (low impact, short duration): 1 to 2 days' notice.
Major Outages (critical systems, significant downtime): At least one week's notice
Regular, recurring maintenance windows: At least one week's notice
Performance and uptime metrics are continuously monitored and reviewed quarterly for internal reporting and customer audit readiness.

3. Recovery Objectives

In compliance with CJIS Security Policy Section 5.9.4 (Contingency Plan Testing, Training, and Exercises) and 5.10.1 (Information System Backup), EFORCE Software maintains formal recovery objectives that protect data continuity and system access in the event of service interruption.

- Recovery Time Objective (RTO): 8 hours
- Recovery Point Objective (RPO): < 1 hour

These recovery goals are achieved through distributed backups, and fault-tolerant AWS infrastructure across multiple Availability Zones.

4. Data Protection and Backup

To meet CJIS Security Policy Sections 5.10.1 – 5.10.3, EFORCE Software enforces the following data protection practices:

- Encryption: All data is encrypted in transit and at rest using FIPS 140-2 validated cryptographic modules.
- Redundancy: All production data is stored redundantly across multiple AWS Availability Zones.
- Backup Frequency: Incremental backups occur continuously; full backups are retained according to CJIS-compliant retention schedules.
- Storage Controls: Backups are isolated, access-controlled, and regularly validated.

5. Monitoring and Reporting

EFORCE Software continuously monitors its systems using AWS CloudWatch, AWS CloudTrail.
Service uptime, incident metrics, and recovery data are reviewed monthly and maintained for CJIS audit review.

6. Compliance Statement

EFORCE Software's operational controls and disaster recovery practices are designed to meet or exceed the following CJIS Security Policy requirements:

- Section 5.9 – Continuity of Operations:
  EFORCE maintains a documented contingency plan, including regular testing, staff training, and validation of recovery procedures to ensure continuity during unexpected outages.
- Section 5.9.3 – Alternate Storage and Processing:
  Critical data and services are hosted in multiple AWS Availability Zones, providing geographic redundancy and failover capabilities.
- Section 5.10 – System Availability:
  EFORCE targets 99.9% uptime through continuous monitoring, proactive maintenance, and AWS infrastructure designed for high availability.
- Section 5.10.1 – Information System Backup:
  Backups are performed automatically, encrypted at rest and in transit, and stored in multiple secure locations in accordance with CJIS retention standards.
- Section 5.10.3 – Recovery Testing:
  Restoration and data recovery processes are regularly tested to confirm system integrity and data accessibility.
- Section 5.11 – Incident Response:
  A documented incident response plan defines escalation paths, reporting requirements, and containment procedures. AWS CloudWatch and CloudTrail are leveraged for real-time detection and response.

7. Alignment with NIST 800-53 (Supporting Reference)

EFORCE Software's controls are mapped to relevant NIST SP 800-53 Rev. 5 control families, including:

- CP-2 (Contingency Planning)
- CP-9 (Information System Backup)
- CP-10 (System Recovery and Reconstitution)
- SC-5 (Denial of Service Protection)

These NIST controls are used as a supporting reference framework for CJIS alignment but are not the governing policy. Upon termination, EFORCE will return or destroy CJI within 30 days, In accordance to industry standard and NIST 800-88 recommendations.