# Mystic Message Archival

## Secure Configuration Guide (FedRAMP Moderate)

Revision: 1.0

Revision Date: February 24, 2026

Effective Date: March 1, 2026

System Owner: 3rd Eye Technologies, Inc.

---

# 1. Purpose

This Secure Configuration Guide (SCG) defines the security configuration requirements for customer administrators using Mystic Message Archival (MMA), a FedRAMP Moderate SaaS solution hosted in AWS GovCloud (US).

This guide outlines:

- Top-level administrative responsibilities
- Privileged account configuration controls
- Secure default security settings
- Tenant-level configuration requirements
- Decommissioning procedures

---

### FedRAMP Context Notice

This Secure Configuration Guide provides customer-facing configuration requirements for Mystic Message Archival operating within a FedRAMP Moderate authorized environment. Detailed operational security procedures, monitoring configurations, and control implementation

evidence are maintained within the official FedRAMP authorization package and are not included in this public-facing document.

Configuration options available to tenant administrators are subject to user-level security enforcement controls that cannot be disabled.

Customer administrators are responsible for configuring tenant-level settings in accordance with their agency or organizational compliance requirements.

---

# 2. System Overview

Mystic Message Archival is deployed within AWS GovCloud (US) in a secure, multi-availability zone architecture.

Security architecture includes:

- Private Virtual Private Cloud (VPC) deployment
- Segmented private subnets
- No public-facing production workloads
- Enforced encryption at rest and in transit
- Continuous logging and monitoring

All production systems operate within private subnets and follow a least-privilege access model.

---

# 3. Roles and Responsibilities

## 3.1 3rd Eye Technologies (Service Provider)

3rd Eye is responsible for:

- Infrastructure security

- Network segmentation and access controls
- Logging and monitoring infrastructure
- Encryption enforcement
- Patch management
- Vulnerability monitoring
- Backup and disaster recovery
- Application and platform management

## 3.2 Customer Responsibilities

Customers are responsible for:

- Managing tenant-level user accounts
- Assigning access
- Configuring retention policies
- Conducting periodic access reviews

---

# 4. Top-Level Administrative Accounts

## 4.1 Definition

A Top-Level Administrative Account (TLAA) is the highest-privileged customer account within an MMA tenant.

This role can:

- Configuring tenant retention settings
- Add, delete, and modify user accounts

- View and export data

---

## 4.2 Secure Access Requirements

Top-Level Administrative Accounts must:

- Authenticate via tenant IDP and PKI
- Enforce MFA
- Be assigned to named individuals only

Shared or generic administrator accounts are not permitted.

---

## 4.3 Security Implications of Administrative Actions

Administrative configuration changes may impact an organization’s compliance posture.

Examples include:

- Reducing retention periods may create regulatory or legal exposure.
- Expanding access may increase insider threat risk.

Customers are responsible for ensuring configurations align with applicable regulatory and agency requirements.

---

# 5. Privileged Accounts

Privileged Accounts include:

- Account Manager
- Data Retention Policy Manager

- Data Export Manager

These roles:

- Require MFA
- Must follow least privilege principles
- Are subject to periodic access review
- Have all administrative actions logged

Customers should limit privileged access to individuals with defined operational responsibilities.

---

# 6. Secure Default Configuration

Mystic Message Archival is provisioned with secure defaults, including:

- Encryption in transit (TLS 1.2+)
- Encryption at rest (AWS KMS)
- CloudTrail enabled
- CloudWatch enabled
- GuardDuty enabled
- VPC Flow Logs enabled
- Deny-all inbound security groups
- No public subnet workloads

Certain security controls are enforced at the platform level and cannot be disabled by tenant administrators.

---

# 7. Network Security

- All workloads reside in private subnets.
- Inbound internet access to production systems is not permitted.
- Outbound internet access is controlled through a NAT gateway.
- Security groups enforce least privilege access rules.

Network configurations follow FedRAMP Moderate security control requirements.

---

# 8. Identity and Access Management

- MFA integration is required for use access
- Access revoked within tenant policy

Administrative and privileged activities are logged and monitored.

---

# 9. Encryption Standards

## Encryption in Transit

- TLS 1.2 or higher
- Approved cipher suites
- SSL/HTTPS enabled

## Encryption at Rest

- AWS-managed KMS encryption
- Encryption enabled for storage services
- Automatic key rotation enforced where supported

---

# 10. Logging and Monitoring

The platform enables:

- AWS CloudTrail
- Amazon CloudWatch
- AWS Config
- AWS GuardDuty
- VPC Flow Logs

Administrative and privileged actions are logged and monitored in accordance with FedRAMP Moderate requirements.

---

# 11. Patch and Vulnerability Management

3rd Eye maintains:

- Routine patch cycles
- Continuous vulnerability monitoring
- Annual penetration testing

Customers are notified of scheduled maintenance that may impact availability.

---

# 12. Backup and Disaster Recovery

- Automated backups are performed
- Data is encrypted at rest
- Disaster recovery procedures are maintained and periodically tested

Backup and recovery operations align with FedRAMP Moderate requirements.

---

# 13. Tenant Decommissioning

Upon tenant termination:

- Disable and remove all accounts
- Export customer data upon request
- Apply legal retention holds if required
- Preserve audit logs for Indefinitely
- Remove MFA bindings
- Terminate tenant resources after tenant and 3rd Eye agreed grace period

Customers are responsible for requesting any required data exports before termination.

---

# 14. Continuous Monitoring

Mystic Message Archival operates under a continuous monitoring program aligned with FedRAMP Moderate requirements.

Security events are monitored and addressed in accordance with documented security procedures.

---

# 15. Version Control

This Secure Configuration Guide:

- Is reviewed at least annually
- Is updated following significant architectural changes
- Is version-controlled by 3rd Eye Technologies

> The more indepth and detailed version of this Secure Configuration Guide is available through official 3rd Eye Technologies distribution channels.

---

## Contact Information

Contact: security@t3rdeyetech.com