### **AUDIT LOGS AND REPORTS MANUAL**

#### Document Control

Document Owner: Chief Compliance Officer  
Version: 1.0  
Date: May 14, 2024  
Approval Authority: Compliance and Audit Committee  
Change History: Record of document revisions and updates.

#### 1. Introduction

Purpose: Establish standardized practices for generating, storing, analyzing, and retaining audit logs and reports to ensure integrity and availability of audit data.  
RScope: Applies to all IT systems that generate audit logs.  
Audience: IT staff, security personnel, compliance officers, external auditors.

#### 2. Audit Log Generation

Log Sources: Servers, network devices, applications.  
Log Contents: User actions, system errors, security events.  
Configuration Standards: Guidelines on configuring systems to ensure comprehensive log generation.  
Example: All login and logout activities are logged with timestamp, user ID, and terminal location.

#### 3. Audit Log Storage and Protection

Storage Locations: On-site secure servers and cloud-based storage solutions.  
Protection Measures: Logs are encrypted at rest and in transit. Access is restricted to authorized personnel only.  
Redundancy and Backup: Daily backups are stored off-site and tested quarterly for integrity.  
Example: Audit logs are stored in AWS S3 buckets with AES-256 encryption and lifecycle policies to manage log retention.

#### 4. Audit Log Review and Analysis

Regular Reviews: Conducted weekly by the IT security team to identify anomalies.  
Analysis Tools: Use of Splunk for automated log analysis.  
Incident Response: If analysis reveals unauthorized access attempts, the security incident response protocol is initiated.  
Example: An automated alert is generated when multiple failed login attempts are detected, triggering a security review.

#### 5. Audit Reports

Report Generation: Monthly reports are automatically generated from logged data.  
Content Requirements: Reports include summaries of all critical events, user access patterns, and potential security breaches.  
Distribution: Reports are distributed to department heads, the security team, and compliance officers.  
Example: Monthly compliance report detailing all access to sensitive data systems, highlighting any policy violations.

#### 6. Compliance and Legal Requirements

Regulatory Compliance: Logs and reports are configured to meet GDPR and SOX requirements.  
Legal Retention Requirements: Logs are retained for a minimum of 5 years to comply with legal and regulatory standards.  
Example: Annual audit to verify compliance with HIPAA log retention and access requirements.

#### 7. Training and Awareness

Training Programs: Annual training on the importance and handling of audit logs.  
Awareness Campaigns: Quarterly newsletters on recent security updates and log management best practices.  
Example: New employee training session on the significance of audit logs in maintaining security and compliance.

#### 8. Appendices

A. Configuration Templates for Log Generation  
B. Examples of Audit Logs and Reports  
C. Compliance Checklist for Audit Logs  
D. Contact List for IT Security and Compliance Teams

#### 9. Document Distribution and Maintenance

Distribution List: IT department, HR, legal department, top management.  
Maintenance Schedule: Reviewed and updated annually or after significant changes in technology or business processes.