Table of Contents

# 1 Security and Compliance Specifications

## 1.1 Introduction

This document outlines comprehensive security and compliance requirements for the Signox LogX System implementation. It addresses data protection, privacy regulations, security controls, and compliance frameworks to ensure the system meets all security and regulatory requirements.

## 1.2 Security Framework Overview

### 1.2.1 Security Architecture Principles

#### 1.2.1.1 Defense in Depth

* **Multiple Security Layers**: Implement security controls at network, application, and data levels
* **Redundant Controls**: Multiple controls for critical security functions
* **Fail-Safe Defaults**: Secure default configurations and permissions
* **Least Privilege**: Minimum necessary access rights for all users
* **Separation of Duties**: Critical functions require multiple approvals

#### 1.2.1.2 Security by Design

* **Built-in Security**: Security integrated into system design
* **Threat Modeling**: Systematic identification of potential threats
* **Secure Development**: Secure coding practices and testing
* **Regular Assessment**: Continuous security evaluation and improvement
* **Incident Response**: Prepared response to security incidents

### 1.2.2 Security Domains

#### 1.2.2.1 Identity and Access Management (IAM)

* **Authentication**: Multi-factor authentication capabilities
* **Authorization**: Role-based access control (RBAC)
* **User Management**: Centralized user account management
* **Session Management**: Secure session handling
* **Single Sign-On**: Integration with enterprise SSO systems

#### 1.2.2.2 Data Protection

* **Encryption**: Data encryption at rest and in transit
* **Data Classification**: Sensitive data identification and handling
* **Data Loss Prevention**: Prevent unauthorized data disclosure
* **Backup Security**: Secure backup and recovery procedures
* **Data Retention**: Compliant data retention and disposal

#### 1.2.2.3 Network Security

* **Perimeter Security**: Firewall and intrusion prevention
* **Network Segmentation**: Isolated network zones
* **Secure Communication**: Encrypted network protocols
* **VPN Access**: Secure remote access capabilities
* **Network Monitoring**: Continuous network traffic analysis

#### 1.2.2.4 Application Security

* **Secure Coding**: Security-focused development practices
* **Input Validation**: Comprehensive input sanitization
* **Output Encoding**: Proper data output handling
* **Error Handling**: Secure error message handling
* **Security Testing**: Regular security assessments

## 1.3 Data Protection and Privacy

### 1.3.1 Data Classification Framework

#### 1.3.1.1 Data Categories

**Public Data** - **Examples**: Course catalogs, institutional information, public announcements - **Protection Level**: Basic protection against unauthorized modification - **Access Control**: Publicly accessible with read permissions - **Retention**: Indefinite retention with regular review

**Internal Data** - **Examples**: Timetables, room assignments, general statistics - **Protection Level**: Access restricted to authorized personnel - **Access Control**: Role-based access for institutional staff - **Retention**: Business need-based retention periods

**Confidential Data** - **Examples**: Student records, staff information, attendance data - **Protection Level**: Strong access controls and encryption - **Access Control**: Strict role-based access with audit logging - **Retention**: Regulatory compliance-based retention

**Restricted Data** - **Examples**: Biometric data, financial information, disciplinary records - **Protection Level**: Highest security controls - **Access Control**: Authorized personnel only with management approval - **Retention**: Minimal retention with secure disposal

#### 1.3.1.2 Data Handling Requirements

**Data Collection** - **Purpose Limitation**: Collect only necessary data - **Consent Management**: Obtain appropriate consent for data collection - **Data Minimization**: Minimal data collection principle - **Accuracy**: Ensure data accuracy and completeness - **Lawful Basis**: Establish lawful basis for data processing

**Data Processing** - **Processing Limitation**: Process only for stated purposes - **Automated Decision-Making**: Transparency in automated decisions - **Profiling**: Appropriate safeguards for user profiling - **Data Quality**: Maintain data accuracy and currency - **Processing Records**: Maintain records of processing activities

**Data Storage** - **Secure Storage**: Encrypted storage for sensitive data - **Access Controls**: Appropriate access restrictions - **Data Integrity**: Prevent unauthorized data modification - **Backup Security**: Secure backup procedures - **Geographic Restrictions**: Comply with data residency requirements

**Data Transmission** - **Encryption**: Encrypted data transmission - **Secure Protocols**: Use of secure communication protocols - **Authentication**: Authenticated data transmission - **Non-Repudiation**: Prevent denial of data transmission - **Monitoring**: Monitor data transmission for anomalies

## 1.4 Regulatory Compliance

### 1.4.1 GDPR Compliance (General Data Protection Regulation)

#### 1.4.1.1 Key Requirements

**Lawful Basis for Processing** - **Consent**: Explicit consent for data processing - **Contract**: Processing necessary for contract performance - **Legal Obligation**: Compliance with legal requirements - **Vital Interests**: Protection of vital interests - **Public Task**: Performance of public tasks - **Legitimate Interests**: Legitimate business interests

**Data Subject Rights** - **Right to Information**: Transparent information about data processing - **Right of Access**: Access to personal data - **Right to Rectification**: Correction of inaccurate data - **Right to Erasure**: Deletion of personal data (“right to be forgotten”) - **Right to Restrict Processing**: Limitation of data processing - **Right to Data Portability**: Export data in machine-readable format - **Right to Object**: Object to certain types of processing - **Rights Related to Automated Decision-Making**: Human intervention in automated decisions

**Organizational Requirements** - **Data Protection Officer (DPO)**: Appointment of DPO if required - **Data Protection Impact Assessment (DPIA)**: Risk assessment for high-risk processing - **Data Breach Notification**: Notification within 72 hours - **Privacy by Design**: Build privacy into system design - **Records of Processing**: Maintain processing activity records

#### 1.4.1.2 Implementation Measures

**Technical Measures** - **Pseudonymization**: Use of pseudonyms for personal identifiers - **Encryption**: Strong encryption for personal data - **Access Controls**: Granular access control implementation - **Data Minimization**: Automated data minimization procedures - **Audit Logging**: Comprehensive audit trail maintenance

**Organizational Measures** - **Policies and Procedures**: GDPR compliance policies - **Staff Training**: Regular GDPR awareness training - **Vendor Management**: GDPR compliance in vendor contracts - **Incident Response**: GDPR-compliant breach response procedures - **Regular Audits**: Compliance monitoring and assessment

### 1.4.2 FERPA Compliance (Family Educational Rights and Privacy Act)

#### 1.4.2.1 Key Requirements

**Student Education Records** - **Definition**: Records directly related to students maintained by institution - **Access Rights**: Students have right to inspect and review records - **Amendment Rights**: Right to request amendment of inaccurate records - **Disclosure Limitations**: Restrictions on disclosure without consent - **Directory Information**: Publicly available student information categories

**Consent and Disclosure** - **Written Consent**: Required for most disclosures - **Legitimate Educational Interest**: Disclosure to school officials - **Audit and Evaluation**: Disclosure for audit purposes - **Financial Aid**: Disclosure for financial aid purposes - **Emergency Situations**: Disclosure in health and safety emergencies

**Implementation Requirements** - **Annual Notification**: Inform students of FERPA rights - **Record Keeping**: Maintain disclosure records - **Training**: Staff training on FERPA requirements - **Policies**: Institutional FERPA policies and procedures - **Complaint Process**: Procedures for FERPA complaints

### 1.4.3 Local Data Protection Laws

#### 1.4.3.1 Country-Specific Requirements

* **Data Residency**: Requirements for data to remain within country borders
* **Cross-Border Transfers**: Restrictions on international data transfers
* **Government Access**: Procedures for government access to data
* **Breach Notification**: Local breach notification requirements
* **Registration**: Data controller registration requirements

#### 1.4.3.2 Sector-Specific Regulations

* **Education Sector**: Specific regulations for educational institutions
* **Employment Law**: Staff data protection requirements
* **Consumer Protection**: Student consumer protection rights
* **Anti-Discrimination**: Equal access and non-discrimination requirements
* **Financial Regulations**: Payment and financial data protection

## 1.5 Authentication and Access Control

### 1.5.1 Multi-Factor Authentication (MFA)

#### 1.5.1.1 Authentication Factors

**Something You Know (Knowledge)** - **Passwords**: Strong password requirements - **PINs**: Personal identification numbers - **Security Questions**: Personalized security questions - **Passphrases**: Long, complex passphrases

**Something You Have (Possession)** - **Mobile Devices**: SMS codes or authenticator apps - **Hardware Tokens**: Physical security tokens - **Smart Cards**: Chip-based authentication cards - **USB Keys**: USB-based security keys

**Something You Are (Inherence)** - **Biometrics**: Fingerprint, facial recognition, iris scanning - **Behavioral**: Typing patterns, gait analysis - **Voice Recognition**: Voice-based authentication - **Facial Recognition**: Facial biometric authentication

#### 1.5.1.2 MFA Implementation

**User Categories and Requirements** - **Students**: Username/password + SMS or app-based MFA - **Staff**: Username/password + hardware token or app-based MFA - **Administrators**: Username/password + hardware token + biometric - **External Users**: Username/password + email verification - **Service Accounts**: Certificate-based authentication

**Risk-Based Authentication** - **Low Risk**: Standard authentication - **Medium Risk**: Additional verification step - **High Risk**: Multiple authentication factors - **Anomaly Detection**: Unusual activity triggers additional verification - **Adaptive Authentication**: Context-aware authentication requirements

### 1.5.2 Role-Based Access Control (RBAC)

#### 1.5.2.1 User Roles and Permissions

**Student/Trainee Role** - **Permissions**: View own schedule, mark attendance, view grades, update profile - **Restrictions**: Cannot access other students’ data, cannot modify system settings - **Data Access**: Own academic records only - **System Functions**: Attendance marking, schedule viewing, profile management

**Faculty/Trainer Role** - **Permissions**: Manage assigned classes, take attendance, view student progress - **Restrictions**: Cannot access other faculty’s classes, limited system configuration - **Data Access**: Assigned students and courses only - **System Functions**: Attendance management, progress tracking, reporting

**Department Head Role** - **Permissions**: Department-wide access, staff management, resource allocation - **Restrictions**: Cannot access other departments without authorization - **Data Access**: All department data and subordinate staff - **System Functions**: Department reporting, resource management, staff oversight

**Administrator Role** - **Permissions**: System configuration, user management, full reporting access - **Restrictions**: Audit logging of all administrative actions - **Data Access**: System-wide access with appropriate justification - **System Functions**: User management, system configuration, reporting

**Auditor Role** - **Permissions**: Read-only access to audit logs and reports - **Restrictions**: Cannot modify any system data or configurations - **Data Access**: Audit trails and compliance reports - **System Functions**: Compliance monitoring, audit reporting

#### 1.5.2.2 Permission Matrix

| Function | Student | Faculty | HOD | Admin | Auditor |
| --- | --- | --- | --- | --- | --- |
| View Own Schedule | ✓ | ✓ | ✓ | ✓ | ✗ |
| Mark Attendance | ✓ | ✗ | ✗ | ✗ | ✗ |
| Take Attendance | ✗ | ✓ | ✗ | ✗ | ✗ |
| View Student Progress | Own Only | Assigned | Department | All | ✗ |
| Generate Reports | Basic | Course | Department | All | Audit |
| User Management | ✗ | ✗ | Limited | ✓ | ✗ |
| System Configuration | ✗ | ✗ | Limited | ✓ | ✗ |
| Audit Logs | ✗ | ✗ | ✗ | ✓ | ✓ |

## 1.6 Data Encryption and Protection

### 1.6.1 Encryption Standards

#### 1.6.1.1 Encryption at Rest

* **Algorithm**: AES-256 encryption standard
* **Key Management**: Hardware Security Module (HSM) or Key Management Service (KMS)
* **Database Encryption**: Transparent Data Encryption (TDE)
* **File System Encryption**: Full disk encryption for servers
* **Backup Encryption**: Encrypted backups with separate key management

#### 1.6.1.2 Encryption in Transit

* **TLS Version**: TLS 1.3 minimum for all communications
* **Certificate Management**: Valid SSL/TLS certificates with proper chain of trust
* **API Security**: HTTPS for all API communications
* **Internal Communication**: Encrypted internal service communication
* **VPN**: Encrypted VPN connections for remote access

#### 1.6.1.3 Key Management

* **Key Generation**: Cryptographically secure random key generation
* **Key Storage**: Secure key storage with access controls
* **Key Rotation**: Regular key rotation procedures
* **Key Escrow**: Secure key backup and recovery procedures
* **Key Destruction**: Secure key destruction when no longer needed

### 1.6.2 Data Masking and Anonymization

#### 1.6.2.1 Production Data Protection

* **Dynamic Data Masking**: Real-time data masking for non-production environments
* **Static Data Masking**: Irreversible data masking for test environments
* **Tokenization**: Replace sensitive data with non-sensitive tokens
* **Pseudonymization**: Replace identifying information with pseudonyms
* **Data Synthesis**: Generate synthetic data for testing purposes

#### 1.6.2.2 Anonymization Techniques

* **Identifier Removal**: Remove direct identifiers
* **Quasi-Identifier Treatment**: Handle indirect identifiers
* **Sensitive Attribute Protection**: Protect sensitive attributes
* **k-Anonymity**: Ensure k-anonymous datasets
* **Differential Privacy**: Add statistical noise for privacy protection

## 1.7 Network Security

### 1.7.1 Perimeter Security

#### 1.7.1.1 Firewall Configuration

* **Ingress Rules**: Restrict incoming traffic to necessary ports and protocols
* **Egress Rules**: Control outgoing traffic and prevent data exfiltration
* **Application Layer**: Layer 7 filtering for application-specific threats
* **Geographic Filtering**: Block traffic from high-risk geographic locations
* **Threat Intelligence**: Integration with threat intelligence feeds

#### 1.7.1.2 Intrusion Detection and Prevention

* **Network IDS/IPS**: Monitor network traffic for malicious activity
* **Host-based IDS**: Monitor individual hosts for security events
* **Behavioral Analysis**: Detect anomalous network behavior
* **Signature-based Detection**: Identify known attack patterns
* **Heuristic Analysis**: Detect previously unknown threats

### 1.7.2 Network Segmentation

#### 1.7.2.1 Network Zones

* **DMZ**: Public-facing services with restricted access to internal networks
* **Internal Network**: Private network for internal services
* **Management Network**: Separate network for system administration
* **Guest Network**: Isolated network for visitor access
* **IoT Network**: Separate network for Internet of Things devices

#### 1.7.2.2 Micro-segmentation

* **Application Segmentation**: Separate networks for different applications
* **User Segmentation**: Separate networks based on user roles
* **Data Segmentation**: Separate networks based on data sensitivity
* **Compliance Segmentation**: Separate networks for compliance requirements
* **Zero Trust**: Verify every connection and transaction

### 1.7.3 Secure Communication

#### 1.7.3.1 VPN Access

* **Remote Access VPN**: Secure remote access for authorized users
* **Site-to-Site VPN**: Secure connections between multiple locations
* **Certificate-based Authentication**: Strong authentication for VPN access
* **Split Tunneling Control**: Control which traffic goes through VPN
* **Session Monitoring**: Monitor VPN sessions for security issues

#### 1.7.3.2 Wireless Security

* **WPA3 Enterprise**: Latest wireless security standard
* **Certificate-based Authentication**: 802.1X authentication
* **Network Isolation**: Separate wireless networks for different user types
* **Rogue Access Point Detection**: Detect unauthorized wireless access points
* **Wireless Intrusion Detection**: Monitor wireless traffic for threats

## 1.8 Application Security

### 1.8.1 Secure Development Practices

#### 1.8.1.1 Security Development Lifecycle (SDL)

* **Security Requirements**: Define security requirements early in development
* **Threat Modeling**: Identify and analyze potential threats
* **Secure Design**: Implement security controls in system design
* **Secure Coding**: Follow secure coding practices and standards
* **Security Testing**: Comprehensive security testing throughout development

#### 1.8.1.2 Code Security

* **Input Validation**: Validate all user inputs
* **Output Encoding**: Properly encode all outputs
* **SQL Injection Prevention**: Use parameterized queries
* **Cross-Site Scripting (XSS) Prevention**: Implement output encoding and CSP
* **Cross-Site Request Forgery (CSRF) Prevention**: Use CSRF tokens

### 1.8.2 Application Security Controls

#### 1.8.2.1 Authentication Controls

* **Password Policies**: Strong password requirements
* **Account Lockout**: Automatic lockout after failed attempts
* **Session Management**: Secure session handling
* **Multi-Factor Authentication**: Additional authentication factors
* **Single Sign-On**: Integration with enterprise authentication systems

#### 1.8.2.2 Authorization Controls

* **Role-Based Access Control**: Granular permission management
* **Attribute-Based Access Control**: Fine-grained access decisions
* **Principle of Least Privilege**: Minimum necessary permissions
* **Segregation of Duties**: Separate conflicting responsibilities
* **Regular Access Reviews**: Periodic review of user permissions

#### 1.8.2.3 Data Validation

* **Input Sanitization**: Clean and validate all user inputs
* **Data Type Validation**: Ensure data matches expected types
* **Range Validation**: Verify data falls within acceptable ranges
* **Format Validation**: Check data format compliance
* **Business Logic Validation**: Ensure data meets business rules

## 1.9 Monitoring and Incident Response

### 1.9.1 Security Monitoring

#### 1.9.1.1 Security Information and Event Management (SIEM)

* **Log Aggregation**: Collect logs from all system components
* **Event Correlation**: Identify patterns and relationships in security events
* **Real-time Monitoring**: Continuous monitoring of security events
* **Alerting**: Automatic alerts for security incidents
* **Reporting**: Regular security reports and dashboards

#### 1.9.1.2 Security Metrics and KPIs

* **Failed Login Attempts**: Monitor authentication failures
* **Privilege Escalation**: Detect unauthorized privilege changes
* **Data Access Patterns**: Monitor unusual data access patterns
* **Network Traffic Anomalies**: Detect abnormal network behavior
* **System Performance**: Monitor system performance for security impacts

### 1.9.2 Incident Response

#### 1.9.2.1 Incident Response Plan

* **Preparation**: Develop incident response procedures and train staff
* **Detection and Analysis**: Identify and analyze security incidents
* **Containment**: Limit the scope and impact of incidents
* **Eradication**: Remove the cause of the incident
* **Recovery**: Restore normal operations
* **Post-Incident Review**: Learn from incidents and improve procedures

#### 1.9.2.2 Incident Classification

* **Low Priority**: Minor security events with minimal impact
* **Medium Priority**: Moderate security events requiring investigation
* **High Priority**: Significant security events requiring immediate attention
* **Critical Priority**: Severe security events threatening system integrity
* **Emergency**: Incidents requiring immediate senior management involvement

#### 1.9.2.3 Response Teams

* **Incident Commander**: Overall incident response coordination
* **Technical Team**: Technical analysis and response actions
* **Communications Team**: Internal and external communication
* **Legal Team**: Legal and regulatory compliance
* **Management Team**: Senior management oversight and decision-making

## 1.10 Compliance Monitoring and Auditing

### 1.10.1 Audit Requirements

#### 1.10.1.1 Internal Audits

* **Regular Assessments**: Periodic security and compliance assessments
* **Control Testing**: Test effectiveness of security controls
* **Vulnerability Assessments**: Identify and assess security vulnerabilities
* **Penetration Testing**: Simulate real-world attacks
* **Compliance Reviews**: Review compliance with regulations and policies

#### 1.10.1.2 External Audits

* **Third-Party Assessments**: Independent security assessments
* **Certification Audits**: Audits for security certifications
* **Regulatory Audits**: Compliance audits by regulatory bodies
* **Customer Audits**: Security assessments by customers
* **Vendor Audits**: Security assessments of vendors and suppliers

### 1.10.2 Audit Logging

#### 1.10.2.1 Log Requirements

* **User Activity**: All user actions and system access
* **Administrative Activity**: All administrative actions and changes
* **Data Access**: All access to sensitive data
* **System Events**: All system events and errors
* **Security Events**: All security-related events and incidents

#### 1.10.2.2 Log Management

* **Centralized Logging**: Collect all logs in central location
* **Log Integrity**: Ensure logs cannot be tampered with
* **Log Retention**: Retain logs for required periods
* **Log Analysis**: Regular analysis of log data
* **Log Backup**: Secure backup of audit logs

### 1.10.3 Compliance Reporting

#### 1.10.3.1 Regulatory Reporting

* **Data Breach Notifications**: Timely notification of data breaches
* **Compliance Status Reports**: Regular compliance status reporting
* **Risk Assessments**: Periodic risk assessment reports
* **Control Effectiveness**: Reports on security control effectiveness
* **Incident Reports**: Detailed incident reporting and analysis

#### 1.10.3.2 Management Reporting

* **Security Dashboards**: Real-time security status dashboards
* **Risk Metrics**: Key risk indicators and metrics
* **Compliance Metrics**: Compliance status and trends
* **Performance Metrics**: Security program performance indicators
* **Trend Analysis**: Analysis of security trends and patterns

## 1.11 Vendor and Third-Party Security

### 1.11.1 Vendor Risk Management

#### 1.11.1.1 Vendor Assessment

* **Security Questionnaires**: Comprehensive security assessments
* **Certifications**: Verify relevant security certifications
* **Financial Stability**: Assess vendor financial stability
* **References**: Check vendor references and reputation
* **Site Visits**: Physical security assessments when appropriate

#### 1.11.1.2 Contractual Requirements

* **Security Standards**: Require compliance with security standards
* **Data Protection**: Specific data protection requirements
* **Incident Notification**: Require timely incident notification
* **Audit Rights**: Right to audit vendor security practices
* **Indemnification**: Appropriate liability and indemnification clauses

### 1.11.2 Third-Party Integrations

#### 1.11.2.1 Integration Security

* **API Security**: Secure API design and implementation
* **Authentication**: Strong authentication for all integrations
* **Authorization**: Granular authorization for integrated systems
* **Data Encryption**: Encrypt all data in transit and at rest
* **Error Handling**: Secure error handling and logging

#### 1.11.2.2 Integration Monitoring

* **Connection Monitoring**: Monitor all third-party connections
* **Data Flow Monitoring**: Track data flows between systems
* **Performance Monitoring**: Monitor integration performance
* **Security Monitoring**: Monitor for security events and anomalies
* **Compliance Monitoring**: Ensure ongoing compliance of integrations

## 1.12 Business Continuity and Disaster Recovery

### 1.12.1 Business Continuity Planning

#### 1.12.1.1 Risk Assessment

* **Threat Identification**: Identify potential threats to business operations
* **Impact Analysis**: Assess potential impact of various threats
* **Probability Assessment**: Evaluate likelihood of different scenarios
* **Risk Prioritization**: Prioritize risks based on impact and probability
* **Mitigation Strategies**: Develop strategies to reduce risks

#### 1.12.1.2 Continuity Strategies

* **Backup Systems**: Redundant systems and infrastructure
* **Alternative Locations**: Backup facilities and work locations
* **Remote Work**: Capabilities for remote work and access
* **Communication**: Emergency communication procedures
* **Vendor Relationships**: Agreements with alternative vendors

### 1.12.2 Disaster Recovery

#### 1.12.2.1 Recovery Objectives

* **Recovery Time Objective (RTO)**: Maximum acceptable downtime
* **Recovery Point Objective (RPO)**: Maximum acceptable data loss
* **Critical Functions**: Identification of critical business functions
* **Recovery Priorities**: Prioritization of recovery activities
* **Resource Requirements**: Resources needed for recovery

#### 1.12.2.2 Recovery Procedures

* **Backup Procedures**: Regular backup of all critical data and systems
* **Restoration Procedures**: Step-by-step recovery procedures
* **Testing Procedures**: Regular testing of recovery procedures
* **Communication Procedures**: Emergency communication protocols
* **Training Procedures**: Training for disaster recovery team

### 1.12.3 Security During Incidents

#### 1.12.3.1 Incident Security

* **Access Controls**: Maintain access controls during incidents
* **Data Protection**: Ensure data protection during recovery
* **Communication Security**: Secure communication during incidents
* **Vendor Security**: Maintain vendor security during incidents
* **Audit Trails**: Maintain audit trails during incidents

#### 1.12.3.2 Post-Incident Security

* **Security Assessment**: Assess security posture after incidents
* **Vulnerability Assessment**: Identify vulnerabilities exposed during incidents
* **Control Updates**: Update security controls based on lessons learned
* **Training Updates**: Update training based on incident experience
* **Process Improvements**: Improve security processes based on incidents

## 1.13 Conclusion

The security and compliance specifications outlined in this document provide a comprehensive framework for implementing robust security controls and maintaining regulatory compliance for the Signox LogX System. These specifications must be carefully implemented and continuously monitored to ensure ongoing security and compliance.

### 1.13.1 Key Implementation Priorities

1. **Data Protection**: Implement comprehensive data protection measures
2. **Access Controls**: Establish strong authentication and authorization controls
3. **Monitoring**: Deploy comprehensive security monitoring capabilities
4. **Compliance**: Ensure ongoing compliance with all applicable regulations
5. **Incident Response**: Develop and maintain effective incident response capabilities

### 1.13.2 Ongoing Requirements

* **Regular Security Assessments**: Conduct periodic security reviews and assessments
* **Compliance Monitoring**: Continuously monitor compliance with regulations
* **Security Training**: Provide ongoing security awareness training
* **Incident Management**: Maintain and improve incident response capabilities
* **Vendor Management**: Continuously assess and manage vendor security risks

**Document Version:** 1.0  
**Last Updated:** June 2025  
**Document Owner:** Signox LogX Security and Compliance Team