SECURITY POLICY DOCUMENT

Version 1.0

Effective Date: January 2024

1. DATA ENCRYPTION POLICY

1.1 Data at Rest Encryption

All data stored in our systems is encrypted at rest using AES-256 encryption. This includes:

- Database records
- File storage systems
- Backup data
- Log files containing sensitive information

1.2 Data in Transit Encryption

All data transmitted over networks is encrypted using TLS 1.3 or higher. This applies to:

- API communications
- Web application traffic
- Database connections
- File transfers

2. ACCESS CONTROL POLICY

2.1 User Authentication

We implement multi-factor authentication (MFA) for all user accounts. Authentication methods include:

- Password-based authentication
- SMS-based verification codes
- Hardware security keys
- Biometric authentication where supported

2.2 Role-Based Access Control (RBAC)

Access to systems and data is controlled through role-based permissions:

- Admin roles: Full system access
- User roles: Limited access based on job function
- Read-only roles: View-only access to specific data sets
- Guest roles: Minimal access for temporary users

2.3 Access Review Process

Access permissions are reviewed quarterly to ensure:

- Users have appropriate access levels
- Former employees' access is properly revoked
- Privileged accounts are monitored and controlled

3. INCIDENT RESPONSE PROCEDURES

3.1 Incident Detection

Security incidents are detected through:

- Automated monitoring systems
- User reports
- Third-party security notifications
- Regular security assessments

3.2 Response Timeline

- Critical incidents: Response within 1 hour
- High priority incidents: Response within 4 hours
- Medium priority incidents: Response within 24 hours
- Low priority incidents: Response within 72 hours

3.3 Incident Classification

Incidents are classified based on:

- Data sensitivity involved
- Number of affected users
- Potential business impact
- Regulatory requirements

4. BACKUP AND DISASTER RECOVERY

4.1 Backup Procedures

We maintain regular backups of all critical data:

- Daily incremental backups
- Weekly full backups
- Monthly archival backups
- Real-time replication for critical systems

4.2 Backup Security

All backups are:

- Encrypted using AES-256
- Stored in geographically separate locations
- Protected with access controls
- Regularly tested for integrity

4.3 Disaster Recovery Plan

Our disaster recovery plan includes:

- Recovery Time Objective (RTO): 4 hours for critical systems
- Recovery Point Objective (RPO): 1 hour for critical data
- Automated failover procedures
- Manual recovery procedures for complex scenarios

5. VULNERABILITY MANAGEMENT

5.1 Vulnerability Assessment

We conduct regular vulnerability assessments:

- Automated scans: Weekly
- Manual penetration testing: Quarterly
- Third-party security audits: Annually
- Continuous monitoring for new threats

5.2 Patch Management

Security patches are applied according to risk levels:

- Critical patches: Within 24 hours
- High priority patches: Within 7 days
- Medium priority patches: Within 30 days
- Low priority patches: Within 90 days

6. EMPLOYEE SECURITY TRAINING

6.1 Training Requirements

All employees receive security training:

- New employee orientation: Security basics
- Annual refresher training: Updated policies and threats
- Role-specific training: Based on job responsibilities
- Incident response training: For designated responders

6.2 Security Awareness

We promote security awareness through:

- Regular security newsletters
- Phishing simulation exercises
- Security best practices reminders
- Recognition programs for security-conscious behavior

7. THIRD-PARTY VENDOR MANAGEMENT

7.1 Vendor Assessment

All third-party vendors are assessed for security:

- Security questionnaire completion
- Risk assessment based on data access
- Regular security reviews
- Contractual security requirements

7.2 Vendor Monitoring

We monitor vendor security through:

- Regular security reports
- Incident notification requirements
- Performance metrics
- Annual security assessments

8. COMPLIANCE AND AUDITING

8.1 Regulatory Compliance

We maintain compliance with:

- SOC 2 Type II certification
- ISO 27001 standards
- GDPR requirements
- Industry-specific regulations

8.2 Internal Auditing

Internal audits are conducted:

- Quarterly security reviews

- Annual comprehensive audits
- Ad-hoc audits for specific concerns
- Continuous monitoring and reporting

9. PHYSICAL SECURITY

9.1 Facility Security

Our facilities are protected by:

- 24/7 security monitoring
- Access control systems
- Video surveillance
- Environmental controls

9.2 Equipment Security

All equipment is secured through:

- Asset tracking systems
- Secure disposal procedures
- Inventory management
- Physical access controls

10. MONITORING AND LOGGING

10.1 System Monitoring

We monitor all systems for:

- Unusual access patterns
- Performance anomalies
- Security events
- Compliance violations

10.2 Log Management

All logs are:

- Collected centrally
- Retained for 12 months minimum
- Protected from tampering
- Regularly reviewed for security events

This security policy is reviewed and updated annually or as needed based on changes in technology, threats, or business requirements.