Security & Data Protection Guide

Comprehensive Security Standards for Smart Hotel Locks

This guide covers essential security measures, encryption standards, compliance requirements, and best practices for protecting guest data in smart hotel lock systems. Following these guidelines helps ensure regulatory compliance and guest privacy protection.

1. Encryption & Cryptography Standards

Standard	Application	Requirement	Compliance
AES-128/256 Encryption	Data at rest and in transit	Minimum AES-128 for key credentials, AES-256 recommended for sensitive guest data	PCI DSS, GDPR required
TLS 1.2 / 1.3	Network communication	All API calls and data transmissions must use TLS 1.2 or higher	Industry standard
RSA-2048	Key exchange and certificates	Minimum 2048-bit keys for digital certificates and key exchanges	NIST recommended
SHA-256	Hashing and verification	Password hashing, data integrity verification	FIPS 180-4 compliant

2. Data Protection Requirements

2.1 Guest Personal Data

- Name, contact information: Encrypted at rest, masked in logs
- Check-in/out dates: Stored securely, deleted per retention policy
- Room number: Logged with encryption, access controlled
- Payment information: Never stored in lock system, PCI DSS scope

2.2 Access Credentials

- Mobile key tokens: Time-limited, encrypted, unique per guest
- RFID card data: Encoded with property-specific keys
- PIN codes: Hashed (never plain text), minimum 4-6 digits
- Biometric data: If used, must comply with GDPR Article 9

2.3 Audit Logs

- Door access events: Timestamped, tamper-proof, encrypted
- System changes: Admin access logged with user ID
- Failed access attempts: Logged for security monitoring
- Log retention: Minimum 90 days, maximum per local law

3. Regulatory Compliance Standards

3.1 GDPR (EU)

Scope: Properties in EU or serving EU residents

Key Requirements:

- Right to erasure: Ability to delete guest data on request
- Data minimization: Collect only necessary information
- Consent: Clear opt-in for mobile key services
- Breach notification: Report within 72 hours
- DPO appointment: Required for large-scale processing

3.2 PCI DSS

Scope: Payment card data (if integrated with billing)

Key Requirements:

- Never store full card numbers in lock system
- Tokenization for payment references only
- Network segmentation from payment systems
- Quarterly security scans
- Annual compliance audit

3.3 CCPA (California)

Scope: Properties in California or CA residents

Key Requirements:

- Privacy notice at check-in
- Right to access: Provide data upon request
- Right to delete: Remove data on request
- Opt-out of data sale (if applicable)
- Non-discrimination for privacy requests

3.4 ISO 27001

Scope: Information security management (optional)

Key Requirements:

- Risk assessment and treatment
- Security controls implementation
- Incident response procedures
- Regular security audits
- Continuous improvement process

4. Physical Security Measures

4.1 Server & Network Equipment

- Locked server room with access control
- Environmental monitoring (temperature, humidity)
- Uninterruptible Power Supply (UPS)
- Fire suppression system
- Access logging for server room entry

4.2 Key Encoders

- Encoder stations at front desk in visible area
- Network cable physical security (prevent tapping)
- Automatic screen lock after inactivity
- No USB ports accessible to guests
- Regular inspection for tampering

4.3 Master Keys & Emergency Access

- Master keys stored in dual-control safe
- Emergency mechanical override keys secured separately
- Access log for master key removal
- Regular audits of master key inventory
- Immediate re-keying if master key compromised

5. Security Incident Response Plan

Ø=Þ¨ Scenario 1: Unauthorized Access Detected

Severity: HIGH

Immediate Actions:

1. Immediately review audit logs for affected rooms
2. Deactivate compromised credentials
3. Notify security and management
4. Re-encode new keys for affected guests
5. Document incident with timestamps
6. Review CCTV footage if available

Ø=Þ¨ Scenario 2: Data Breach (Guest Information Exposed)

Severity: CRITICAL

Immediate Actions:

1. Isolate affected systems immediately
2. Activate data breach response team
3. Assess scope: what data, how many guests
4. Notify affected guests within 72 hours (GDPR)
5. Report to supervisory authority if required
6. Offer credit monitoring services if applicable
7. Conduct forensic investigation
8. Implement corrective measures

Ø=Þ¨ Scenario 3: System Compromise (Malware/Ransomware)

Severity: CRITICAL

Immediate Actions:

1. Disconnect affected systems from network
2. Switch to manual key encoding procedures
3. Engage cybersecurity incident response team
4. Preserve evidence for forensic analysis
5. Restore from clean backups
6. Scan all systems before reconnecting
7. Change all passwords and credentials
8. Notify law enforcement if criminal activity

6. Quarterly Security Audit Checklist

Security Task	Frequency	Last Done	Next Due
Review and rotate all system passwords and API keys	Quarterly	___/___	___/___
Audit all user accounts and remove inactive users	Quarterly	___/___	___/___
Review access logs for anomalous patterns	Monthly	___/___	___/___
Update all software components (PMS, lock system, firmware)	As released	___/___	___/___
Test backup and restore procedures	Quarterly	___/___	___/___
Verify encryption settings on all communications	Quarterly	___/___	___/___
Scan network for vulnerabilities	Monthly	___/___	___/___
Review and update firewall rules	Semi-annually	___/___	___/___
Test incident response procedures	Annually	___/___	___/___
Train staff on security awareness	Annually	___/___	___/___
Review compliance with GDPR/CCPA requirements	Annually	___/___	___/___
Physical inspection of all lock hardware	Annually	___/___	___/___

7. Security Best Practices Summary

1. Use defense in depth: Multiple layers of security controls
2. Implement principle of least privilege for all user accounts
3. Encrypt all data at rest and in transit
4. Maintain comprehensive audit logs for minimum 90 days
5. Regularly test backup and disaster recovery procedures
6. Keep all software and firmware updated with latest security patches
7. Conduct annual penetration testing by qualified third party
8. Train all staff on security awareness and phishing prevention
9. Implement multi-factor authentication for administrative access
10. Monitor systems 24/7 for security anomalies