SECURITY COMPLIANCE POLICY

NFC Card Feedback System

Last Updated: April 30, 2025

1. INTRODUCTION

This Security Compliance Policy outlines the measures, protocols, and standards implemented by Feedback NFC to ensure the security, integrity, and confidentiality of all data collected, processed, and stored through our NFC Card Feedback System ("the Service"). Our commitment to maintaining robust security practices is fundamental to providing a trustworthy service to our subscribers and their end users.

2. SECURITY GOVERNANCE

2.1 Security Leadership

- Feedback NFC has established a dedicated security team responsible for implementing and maintaining our security program.
- A designated Security Officer oversees all security operations and compliance requirements.
- Security responsibilities are clearly defined across the organization with regular reviews of role assignments.

2.2 Risk Management

- We conduct formal risk assessments of our systems and processes at least annually.
- Identified risks are documented, prioritized, and addressed according to their severity and potential impact.
- A risk treatment plan is maintained and regularly updated to address evolving threats.

2.3 Policy Management

- All security policies are reviewed and updated at least annually or when significant changes to the system occur.
- Security policies are communicated to all employees during onboarding and through regular refresher training.
- Compliance with security policies is monitored and enforced throughout the organization.

3. PHYSICAL SECURITY

3.1 Data Center Security

- All production systems and data are hosted in secure data centers with multiple physical security controls.
- Data centers are equipped with 24/7 surveillance, biometric access controls, and environmental monitoring.
- Access to data center facilities is strictly limited to authorized personnel only.

3.2 Office Security

- Our offices implement appropriate physical security measures, including access control systems.
- Visitors must sign in, wear visitor badges, and be escorted by employees.
- Secure disposal methods are used for all physical media and documents containing sensitive information.

3.3 NFC Card Security

- NFC cards are manufactured with tamper-evident features to prevent unauthorized modification.
- Cards are stored in secure facilities before distribution to subscribers.
- Each card is assigned a unique identifier that is tracked throughout its lifecycle.
- Decommissioned cards undergo a secure disposal process to prevent unauthorized reuse.

4. INFORMATION SECURITY

4.1 Data Classification

- All data is classified according to sensitivity levels (Public, Internal, Confidential, Restricted).
- Security controls are implemented based on data classification.
- Handling procedures are defined for each classification level.

4.2 Data Encryption

- All data transmitted between system components is encrypted using TLS 1.2 or higher.
- Sensitive data stored in our databases is encrypted at rest using industry-standard encryption algorithms.
- Encryption keys are securely managed with appropriate key rotation schedules.
- NFC card communications utilize secure encryption protocols to protect data during transmission.

4.3 Access Control

- We implement the principle of least privilege for all system access.
- Multi-factor authentication is required for all administrative access and subscriber dashboard accounts.
- Access rights are regularly reviewed and promptly adjusted when role changes occur.
- Automated systems monitor for unusual access patterns or potential unauthorized access attempts.

4.4 Network Security

- Our network architecture implements defense-in-depth strategies with multiple security layers.
- Firewalls, intrusion detection/prevention systems, and web application firewalls protect our infrastructure.
- Regular network vulnerability scans are conducted to identify and remediate potential security weaknesses.
- Network traffic is monitored for suspicious activities with alerts for potential security events.

5. APPLICATION SECURITY

5.1 Secure Development

- Our development process follows secure coding practices and security by design principles.
- All code undergoes security code reviews before deployment.
- We maintain separate development, testing, and production environments.
- Regular security testing, including static and dynamic application security testing, is performed.

5.2 API Security

- All APIs are secured using industry-standard authentication and authorization mechanisms.
- API access is limited based on the principle of least privilege.
- Rate limiting and monitoring are implemented to prevent abuse.
- Regular security assessments of APIs are conducted to identify vulnerabilities.

5.3 Mobile Application Security

- Any mobile applications associated with our Service implement appropriate security controls.
- Data stored on mobile devices is encrypted and protected from unauthorized access.
- Mobile applications undergo regular security testing before release.

6. NFC TECHNOLOGY SECURITY

6.1 Card Communication Security

- NFC card communications utilize secure encryption protocols.
- Cards are designed to prevent unauthorized reading of data.
- Anti-cloning measures are implemented to prevent duplication of cards.
- Cards have limited data storage with only essential information stored on the card itself.

6.2 Tap Security

- Feedback collection through card taps implements secure communication channels.
- Transaction signing ensures the integrity of the feedback data.
- Proximity requirements limit the risk of unauthorized interception.

7. OPERATIONAL SECURITY

7.1 Change Management

- A formal change management process is implemented for all system changes.
- Changes undergo security review before implementation.
- Emergency changes follow an expedited but controlled process.
- Changes are tested in a non-production environment before deployment.

7.2 Vulnerability Management

- Regular vulnerability scans are performed across our infrastructure.
- A formal patch management process ensures timely application of security updates.
- Critical vulnerabilities are addressed according to defined timeframes based on severity.
- Third-party security assessments are conducted at least annually.

7.3 Logging and Monitoring

- Comprehensive logging is implemented across all system components.
- Logs are centralized, protected from unauthorized modification, and retained according to defined retention policies.
- Security monitoring systems provide real-time alerts for potential security events.
- Log reviews are conducted regularly to identify potential security issues.

7.4 Incident Response

- A documented incident response plan defines procedures for addressing security incidents.
- The incident response team receives regular training and participates in simulated incident exercises.
- Post-incident reviews are conducted to improve security controls and response procedures.

- Relevant incidents are reported to affected subscribers in accordance with contractual and regulatory requirements.

8 VENDOR MANAGEMENT

8.1 Third-Party Risk Assessment

- Security assessments are conducted for all vendors with access to our systems or data.
- Vendors must meet defined security requirements based on the sensitivity of accessed data.
- Regular reviews of vendor security practices are conducted.

8.2 Contract Requirements

- Security requirements are included in all vendor contracts.
- Data processing agreements are implemented for vendors processing personal data.
- Right-to-audit clauses are included in contracts with critical vendors.

9. COMPLIANCE AND CERTIFICATIONS

9.1 Regulatory Compliance

- Our security program complies with all applicable Saudi Arabian regulations, including:
    - National Cybersecurity Authority (NCA) frameworks and guidelines
    - Saudi Data and Privacy Protection Law (SDPPL) requirements
    - Communications and Information Technology Commission (CITC) regulations
    - Saudi Central Bank (SAMA) requirements for payment processing

9.2 Industry Standards

- Our security practices align with international standards and frameworks, including:
    - ISO/IEC 27001 Information Security Management
    - NIST Cybersecurity Framework
    - PCI DSS for payment card data protection
    - OWASP security best practices for web applications

9.3 Compliance Monitoring

- Regular internal audits assess compliance with security policies and regulatory requirements.
- Independent third-party assessments validate our security controls.
- Compliance gaps are documented and addressed through a formal remediation process.

10. BUSINESS CONTINUITY AND DISASTER RECOVERY

10.1 Backup Procedures

- Critical system data is backed up according to defined schedules.
- Backups are encrypted and stored securely with geographic redundancy.
- Backup restoration is tested regularly to ensure data recoverability.

10.2 Disaster Recovery

- A formal disaster recovery plan defines procedures for recovering from significant disruptions.
- Recovery time objectives (RTOs) and recovery point objectives (RPOs) are established for critical systems.
- Disaster recovery procedures are tested at least annually.

11. SUBSCRIBER SECURITY RESPONSIBILITIES

11.1 Access Management

- Subscribers are responsible for managing access to their dashboard accounts.
- Strong passwords and multi-factor authentication should be used for all subscriber accounts.
- Subscribers must promptly notify Feedback NFC of any suspected security incidents related to their account.

11.2 NFC Card Management

- Subscribers are responsible for the physical security of NFC cards at their locations.
- Lost or stolen cards must be reported immediately to prevent unauthorized use.
- Proper card allocation procedures should be followed to maintain card security.

12. SECURITY AWARENESS AND TRAINING

12.1 Employee Training

- All employees receive security awareness training during onboarding and at least annually thereafter.
- Role-specific security training is provided based on job responsibilities.
- Regular security communications keep employees informed about emerging threats and security best practices.

12.2 Subscriber Education

- Security guidance is provided to subscribers through documentation and support channels.
- Security bulletins are issued when relevant threats or vulnerabilities are identified.
- Best practices for secure system usage are communicated to subscribers.

13. REPORTING SECURITY CONCERNS

- Security concerns or suspected vulnerabilities can be reported to ML@feedbacknfc.com.
- A responsible disclosure process is established for reporting security vulnerabilities.
- We are committed to investigating all reported security concerns promptly and thoroughly.

14. POLICY UPDATES

This Security Compliance Policy will be reviewed and updated at least annually or when significant changes to our security program occur. Subscribers will be notified of material changes to this policy.

15. CONTACT INFORMATION

For questions about our security practices or to report security concerns, please contact us at:

- Email: ML@feedbacknfc.com
- Address: Level 18, Faisaliah Towers, King Fahd Road, Riyadh, Kingdom of Saudi Arabia

---

سياسة الأمن والامتثال متوفرة باللغة العربية عند الطلب. (Security Compliance Policy is available in Arabic upon request.)