Card Data Transmission Security Policy for CHRONOLOGY ENTERPRISES S.R.L.

CHRONOLOGY ENTERPRISES S.R.L. is committed to protecting cardholder data processed through our **Nyzer** mobile application. This comprehensive security policy outlines our approach to maintaining the highest standards of payment card security and compliance with all relevant industry requirements.

Introduction and Purpose

The purpose of this **Card Data Transmission Security Policy** is to establish a robust framework for securely collecting, processing, and transmitting payment card information through the **Nyzer** mobile application. By implementing these strict security controls, we aim to protect our customers' sensitive financial information, maintain compliance with regulatory requirements, and prevent unauthorized access to cardholder data. This policy serves as a foundation for all employees, contractors, and third-party service providers who interact with payment card data as part of our service offering.

Policy Statement

CHRONOLOGY ENTERPRISES S.R.L. is dedicated to maintaining the highest standards of security for all payment card transactions processed through our systems. We recognize the critical importance of cardholder data protection and are committed to implementing comprehensive security measures that meet or exceed industry standards. This policy provides guidelines for the secure handling of cardholder data throughout its lifecycle within our systems, with particular emphasis on secure transmission protocols.

Scope and Applicability

This policy applies to all employees, contractors, third-party service providers, and systems involved in the processing, storage, or transmission of cardholder data for **CHRONOLOGY ENTERPRISES S.R.L.** Specifically, this includes:

In-Scope Elements

This policy covers all components of our **cardholder data environment (CDE)**, including:

- The **Nyzer** mobile application payment functionality
- All servers, networks, and systems that process, store, or transmit cardholder data
- All personnel who have access to cardholder data or systems within the CDE
- Integration points with our payment gateway provider (Azul)
- All transmission channels through which cardholder data flows

Out-of-Scope Elements

This policy does not apply to:

- Systems that are properly segmented from the cardholder data environment
- Personal devices not used for company business purposes
- Third-party services where **CHRONOLOGY ENTERPRISES S.R.L.** has no control over security implementations

Roles and Responsibilities

The protection of cardholder data is a shared responsibility across all levels of our organization. The following roles have specific responsibilities regarding payment card security:

Chief Information Security Officer (CISO)

- Overall responsibility for information security throughout the organization
- Final approval of this policy and any subsequent revisions
- Ensuring adequate resources are allocated for security initiatives

IT Security Team

- Daily implementation and monitoring of security controls
- Regular review and testing of security measures
- Security incident response coordination
- Conducting regular vulnerability assessments and penetration tests

Application Development Team

- Ensuring the **Nyzer** mobile application adheres to secure coding practices
- Implementing and maintaining security features within the application
- Conducting regular security testing during the development lifecycle

All Employees

- Adhering to this policy in their daily activities
- Reporting potential security incidents or vulnerabilities
- Completing all required security awareness training

PCI DSS Compliance Framework

CHRONOLOGY ENTERPRISES S.R.L. maintains compliance with the Payment Card Industry Data Security Standard (PCI DSS) requirements. We are currently certified through Self-Assessment Questionnaire D (SAQ-D) and are working toward Level 2 merchant certification, with plans to achieve Level 1 status as our transaction volume increases.

Compliance Status

Our compliance program addresses all twelve PCI DSS requirement domains:

1. Installing and maintaining a secure network and systems
2. Protecting cardholder data with strong access controls
3. Maintaining a vulnerability management program

4. Implementing strong access control measures
5. Regularly monitoring and testing networks
6. Maintaining an information security policy

Compliance Validation

We undergo regular internal and external assessments to validate our compliance status, including:

- Annual self-assessment using the appropriate SAQ
- Quarterly network vulnerability scans by an Approved Scanning Vendor (ASV)
- Penetration testing of our cardholder data environment at least annually
- Regular reviews of policies and procedures

Card Data Collection Methods

CHRONOLOGY ENTERPRISES S.R.L. collects payment card information through secure methods designed to minimize risk exposure and maintain compliance with PCI DSS requirements.

Mobile Application (Nyzer)

The Nyzer mobile application incorporates secure payment functionality that implements the following security measures:

- All payment forms use secure, encrypted connections
- Card data is never stored locally on the user's device
- Tokenization is implemented to replace sensitive card data
- Card verification values (CVV/CVC) are never stored after authorization
- Only the minimum necessary information is collected for transaction processing

Prohibited Collection Methods

The following methods of collecting cardholder data are explicitly prohibited:

- Collection via unsecured email
- Storage in plain text files or documents
- Use of messaging applications or chat programs
- Verbal communication unless directly entered into secure payment systems
- Storage on portable devices such as laptops, flash drives, or mobile phones

Card Data Transmission Security

The secure transmission of cardholder data is a critical component of our overall security strategy. **CHRONOLOGY ENTERPRISES S.R.L.** implements multiple layers of protection to ensure that cardholder data is encrypted during transmission and protected from unauthorized access.

Encryption Requirements

All transmission of cardholder data must adhere to the following encryption requirements:

- Implementation of TLS 1.2 or higher for all web-based transmissions
- Use of AES-256 encryption for data protection
- Strong cryptography for all transmissions over public networks
- Implementation of proper certificate management processes
- Regular testing of encryption effectiveness

Mobile Application Transmission Security

The **Nyzer** mobile application implements additional security measures for payment card transmission:

- Implementation of a trusted execution environment for processing payments
- Secure communication channel between the app and payment gateway

- Certificate pinning to prevent man-in-the-middle attacks
- Robust input validation to prevent injection attacks
- Data minimization principles to limit sensitive data exposure

Third-Party Integration Security

For integration with our payment gateway (Azul), we implement:

- Secure API connections using mutual authentication
- Regular review of integration points for security vulnerabilities
- Clear delineation of security responsibilities between parties
- Monitoring of all data transmission between systems
- Regular testing of integration security controls

Encryption and Security Standards

CHRONOLOGY ENTERPRISES S.R.L. implements industry-leading encryption and security standards to protect cardholder data throughout its lifecycle.

Encryption Technologies

We utilize the following encryption technologies:

- TLS 1.2+ for all web communications
- AES-256 for data encryption
- Strong hashing algorithms (SHA-256 or higher) for integrity verification
- Tokenization to replace sensitive data with non-sensitive equivalents
- 3D Secure (3DS) for additional authentication during card-not-present transactions

Key Management

Cryptographic keys are managed according to industry best practices:

- Secure generation of strong cryptographic keys
- Secure key storage using hardware security modules (HSMs) where appropriate
- Split knowledge and dual control for key management operations
- Regular key rotation according to defined schedules
- Secure destruction of retired keys

Authentication Security

Strong authentication mechanisms are implemented across all systems:

- Multi-factor authentication for administrative access to sensitive systems
- Strong password requirements aligned with PCI DSS standards
- Unique identification for all users accessing cardholder data
- Automatic logoff after periods of inactivity
- Account lockout after multiple failed authentication attempts

Mobile Application Security

The **Nyzer** mobile application is designed with security as a core principle, incorporating numerous protections specifically for payment card data.

Secure Development Practices

Our development team follows secure coding practices, including:

- Implementation of the OWASP Mobile Application Security Verification Standard (MASVS)
- Regular code reviews with a focus on security
- Security testing throughout the development lifecycle
- Third-party component analysis to identify vulnerabilities

- Regular security training for all developers

Application Security Controls

The Nyzer application implements the following security controls:

- Runtime application self-protection (RASP) technology
- Local data encryption for any temporary storage
- Prevention of jailbreak/rooted device usage
- Secure communication with backend services
- Automated security updates

User Security Features

To enhance security from the user perspective, the application includes:

- Biometric authentication options (fingerprint, face recognition)
- Transaction notifications for fraud awareness
- Clear security information and best practices
- Ability to remotely disable payment functionality

Incident Response

CHRONOLOGY ENTERPRISES S.R.L. maintains a comprehensive incident response plan specifically addressing payment card security breaches.

Incident Detection

We implement multiple detection mechanisms, including:

- Real-time monitoring of all systems within the cardholder data environment
- Alerting on suspicious activities or anomalous behavior
- Log analysis and correlation

- Regular scanning for vulnerabilities and misconfigurations
- User reporting channels for suspected security incidents

Incident Handling

When a security incident is detected, we follow a structured response process:

1. Initial assessment and containment
2. Evidence collection and preservation
3. Eradication of the threat
4. Recovery of affected systems
5. Post-incident analysis and improvement implementation

Notification Requirements

In the event of a confirmed or suspected breach involving cardholder data, notifications will be made according to:

- PCI DSS requirements
- Payment brand rules
- Applicable data breach notification laws
- Contractual obligations with our payment processor

Training and Awareness

All personnel with access to cardholder data or systems within the CDE receive regular security training specific to their roles.

Security Awareness Program

Our security awareness program includes:

- Annual security awareness training for all employees

- Role-specific training for personnel with direct access to cardholder data
- Regular security updates and communications
- Simulated phishing exercises to test awareness
- Clear documentation of security policies and procedures

Developer Training

Application developers receive specialized security training:

- Secure coding practices for mobile applications
- Payment card security requirements
- Common vulnerabilities and mitigation strategies
- Secure API implementation techniques
- Security testing methodologies

Policy Maintenance and Review

This policy will be reviewed at least annually and updated as necessary to reflect changes in technology, business processes, or compliance requirements.

Review Process

The policy review process includes:

- Assessment of compliance with current PCI DSS requirements
- Evaluation of emerging threats and vulnerabilities
- Review of security incident history
- Validation of policy effectiveness
- Incorporation of feedback from stakeholders

Policy Distribution

Upon approval, this policy will be:

- Published to our internal policy repository
- Distributed to all affected personnel
- Incorporated into relevant training materials
- Made available to auditors and assessors as required

Contact Information

For questions or concerns regarding this policy, please contact:

CHRONOLOGY ENTERPRISES S.R.L.

Phone: +1 849-868-1908

Email: Contact@Nyzerapp.com

Website: https://www.nyzerapp.com/

Conclusion

CHRONOLOGY ENTERPRISES S.R.L. is committed to maintaining the highest standards of payment card security through the implementation of this comprehensive Card Data Transmission Security Policy. By adhering to these guidelines and continually improving our security posture, we aim to protect our customers' sensitive information and maintain their trust in our services.

This policy is effective immediately and supersedes any previous versions.

Approved by:

Frankelly David Guzman Legreaux

Luis Alfonzo Guzman Legreaux

Date: March 5, 2025