Política de Seguridad en la Transmisión de Datos de Tarjetas para CHRONOLOGY ENTERPRISES S.R.L.

CHRONOLOGY ENTERPRISES S.R.L. está comprometida con la protección de los datos de titulares de tarjetas procesados a través de nuestra aplicación móvil Nyzer. Esta política de seguridad integral describe nuestro enfoque para mantener los más altos estándares de seguridad en pagos con tarjeta y el cumplimiento de todos los requisitos industriales relevantes.

Introducción y Propósito

El propósito de esta Política de Seguridad en la Transmisión de Datos de Tarjetas es establecer un marco robusto para la recolección, procesamiento y transmisión segura de información de tarjetas de pago a través de la aplicación móvil Nyzer. Al implementar estos estrictos controles de seguridad, buscamos proteger la información financiera sensible de nuestros clientes, mantener el cumplimiento regulatorio y prevenir el acceso no autorizado a los datos de tarjetas. Esta política sirve como base para todos los empleados, contratistas y proveedores de servicios externos que interactúan con datos de tarjetas como parte de nuestro servicio.

Declaración de la Política

CHRONOLOGY ENTERPRISES S.R.L. está dedicada a mantener los más altos estándares de seguridad para todas las transacciones con tarjeta procesadas en nuestros sistemas. Reconocemos la importancia crítica de la protección de datos de titulares de tarjetas y nos comprometemos a implementar medidas de seguridad integrales que cumplan o superen los estándares de la industria. Esta política proporciona lineamientos para el manejo seguro de datos de tarjetas durante todo su ciclo de vida en nuestros sistemas, con énfasis especial en los protocolos de transmisión segura.

Alcance y Aplicabilidad

Esta política aplica a todos los empleados, contratistas, proveedores de servicios externos y sistemas involucrados en el procesamiento, almacenamiento o transmisión de datos de titulares de tarjetas para CHRONOLOGY ENTERPRISES S.R.L. Específicamente, esto incluye:

Elementos Incluidos en el Alcance

Esta política cubre todos los componentes de nuestro entorno de datos de titulares de tarjetas (CDE), incluyendo:

- La funcionalidad de pagos en la aplicación móvil Nyzer
- Todos los servidores, redes y sistemas que procesan, almacenan o transmiten datos de tarjetas
- Todo el personal con acceso a datos de tarjetas o sistemas dentro del CDE
- Puntos de integración con nuestro proveedor de pasarela de pagos (Azul)
- Todos los canales de transmisión por donde fluyen datos de tarjetas

Elementos Fuera de Alcance

Esta política no aplica a:

- Sistemas debidamente segmentados del entorno de datos de tarjetas
- Dispositivos personales no utilizados para fines empresariales
- Servicios de terceros donde CHRONOLOGY ENTERPRISES S.R.L. no tiene control sobre la implementación de seguridad

Roles y Responsabilidades

La protección de los datos de titulares de tarjetas es una responsabilidad compartida en todos los niveles de la organización. Los siguientes roles tienen responsabilidades específicas en cuanto a la seguridad de pagos con tarjeta:

Director de Seguridad de la Información (CISO)

- Responsabilidad general sobre la seguridad de la información en la organización
- Aprobación final de esta política y sus revisiones
- Garantizar la asignación de recursos adecuados para iniciativas de seguridad

Equipo de Seguridad de TI

- Implementación y monitoreo diario de controles de seguridad
- Revisión y prueba regular de medidas de seguridad
- Coordinación de respuesta ante incidentes de seguridad
- Realización de evaluaciones de vulnerabilidades y pruebas de penetración regulares

Equipo de Desarrollo de Aplicaciones

- Garantizar que la aplicación móvil Nyzer cumpla con prácticas de codificación segura
- Implementar y mantener funciones de seguridad en la aplicación
- Realizar pruebas de seguridad durante el ciclo de desarrollo

Todos los Empleados

- Cumplir con esta política en sus actividades diarias
- Reportar incidentes o vulnerabilidades de seguridad potenciales
- Completar toda la capacitación requerida en concienciación de seguridad

Marco de Cumplimiento PCI DSS

CHRONOLOGY ENTERPRISES S.R.L. mantiene cumplimiento con los requisitos del Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI DSS). Actualmente estamos certificados a través del Cuestionario de Autoevaluación D (SAQ-D)

y trabajamos hacia la certificación de comerciante Nivel 2, con planes de alcanzar el Nivel 1 a medida que aumente nuestro volumen de transacciones.

Estado de Cumplimiento

Nuestro programa de cumplimiento aborda los doce dominios de requisitos PCI DSS:

1. Instalación y mantenimiento de una red y sistemas seguros
2. Protección de datos de titulares de tarjetas con controles de acceso sólidos
3. Mantenimiento de un programa de gestión de vulnerabilidades
4. Implementación de medidas sólidas de control de acceso
5. Monitoreo y prueba regular de redes
6. Mantenimiento de una política de seguridad de la información

Validación de Cumplimiento

Realizamos evaluaciones internas y externas regulares para validar nuestro estado de cumplimiento, incluyendo:

- Autoevaluación anual usando el SAQ correspondiente
- Escaneos trimestrales de vulnerabilidad de red por un Proveedor de Escaneo Aprobado (ASV)
- Pruebas de penetración del entorno de datos de tarjetas al menos una vez al año
- Revisión regular de políticas y procedimientos

Métodos de Recolección de Datos de Tarjetas

CHRONOLOGY ENTERPRISES S.R.L. recolecta información de tarjetas de pago mediante métodos seguros diseñados para minimizar la exposición al riesgo y mantener el cumplimiento con PCI DSS.

Aplicación Móvil (Nyzer)

- Todos los formularios de pago usan conexiones seguras y cifradas
- Los datos de tarjetas nunca se almacenan localmente en el dispositivo del usuario
- Se implementa tokenización para reemplazar datos sensibles
- Los valores de verificación de tarjeta (CVV/CVC) nunca se almacenan después de la autorización
- Solo se recolecta la información mínima necesaria para procesar la transacción

Métodos Prohibidos de Recolección

- Recolección a través de correo electrónico no seguro
- Almacenamiento en archivos o documentos en texto plano
- Uso de aplicaciones de mensajería o chat
- Comunicación verbal a menos que se ingrese directamente en sistemas de pago seguros
- Almacenamiento en dispositivos portátiles como laptops, memorias USB o teléfonos móviles

Seguridad en la Transmisión de Datos de Tarjetas

La transmisión segura de datos de tarjetas es un componente crítico de nuestra estrategia de seguridad. CHRONOLOGY ENTERPRISES S.R.L. implementa múltiples capas de protección para asegurar que los datos de tarjetas estén cifrados durante la transmisión y protegidos contra accesos no autorizados.

Requisitos de Cifrado

Toda transmisión de datos de tarjetas debe cumplir con los siguientes requisitos:

- Implementación de TLS 1.2 o superior para todas las transmisiones web
- Uso de cifrado AES-256 para la protección de datos

- Criptografía robusta para todas las transmisiones por redes públicas
- Implementación de procesos adecuados de gestión de certificados
- Pruebas regulares de la efectividad del cifrado

Seguridad en la Transmisión desde la Aplicación Móvil

La aplicación móvil Nyzer implementa medidas de seguridad adicionales para la transmisión de pagos:

- Entorno de ejecución confiable para el procesamiento de pagos
- Canal de comunicación seguro entre la app y la pasarela de pagos
- Fijación de certificados para prevenir ataques de intermediarios (man-in-the-middle)
- Validación robusta de entradas para prevenir ataques de inyección
- Principios de minimización de datos para limitar la exposición de información sensible

Seguridad en la Integración con Terceros

Para la integración con nuestra pasarela de pagos (Azul), implementamos:

- Conexiones API seguras con autenticación mutua
- Revisión regular de puntos de integración para detectar vulnerabilidades
- Delimitación clara de responsabilidades de seguridad entre las partes
- Monitoreo de todas las transmisiones de datos entre sistemas
- Pruebas regulares de controles de seguridad en la integración

Tecnologías de Cifrado y Estándares de Seguridad

CHRONOLOGY ENTERPRISES S.R.L. utiliza tecnologías y estándares líderes en la industria para proteger los datos de tarjetas durante todo su ciclo de vida.

Tecnologías de Cifrado

- TLS 1.2+ para todas las comunicaciones web
- AES-256 para cifrado de datos
- Algoritmos de hash robustos (SHA-256 o superior) para verificación de integridad
- Tokenización para reemplazar datos sensibles por equivalentes no sensibles
- 3D Secure (3DS) para autenticación adicional en transacciones sin tarjeta presente

Gestión de Claves

Las claves criptográficas se gestionan según las mejores prácticas de la industria:

- Generación segura de claves criptográficas fuertes
- Almacenamiento seguro de claves usando módulos de seguridad hardware (HSM) cuando corresponda
- Conocimiento dividido y control dual para operaciones de gestión de claves
- Rotación regular de claves según cronogramas definidos
- Destrucción segura de claves retiradas

Seguridad de Autenticación

Se implementan mecanismos de autenticación robustos en todos los sistemas:

- Autenticación multifactor para acceso administrativo a sistemas sensibles
- Requisitos de contraseñas fuertes alineados con los estándares PCI DSS
- Identificación única para todos los usuarios con acceso a datos de tarjetas
- Cierre de sesión automático tras periodos de inactividad
- Bloqueo de cuentas tras múltiples intentos fallidos de autenticación

Seguridad en la Aplicación Móvil

La aplicación Nyzer está diseñada con la seguridad como principio fundamental, incorporando múltiples protecciones específicas para datos de tarjetas.

Prácticas de Desarrollo Seguro

- Implementación del Estándar de Verificación de Seguridad de Aplicaciones Móviles (MASVS) de OWASP
- Revisiones regulares de código con enfoque en seguridad
- Pruebas de seguridad durante todo el ciclo de desarrollo
- Análisis de componentes de terceros para identificar vulnerabilidades
- Capacitación regular en seguridad para todos los desarrolladores

Controles de Seguridad en la Aplicación

- Tecnología de autoprotección en tiempo de ejecución (RASP)
- Cifrado local de cualquier almacenamiento temporal
- Prevención de uso en dispositivos con jailbreak o rooteados
- Comunicación segura con servicios backend
- Actualizaciones automáticas de seguridad

Funciones de Seguridad para el Usuario

Para mejorar la seguridad desde la perspectiva del usuario, la aplicación incluye:

- Opciones de autenticación biométrica (huella, reconocimiento facial)
- Notificaciones de transacciones para concienciación sobre fraude
- Información clara sobre seguridad y buenas prácticas
- Capacidad de desactivar remotamente la funcionalidad de pagos

Respuesta ante Incidentes

CHRONOLOGY ENTERPRISES S.R.L. mantiene un plan integral de respuesta ante incidentes enfocado específicamente en brechas de seguridad de pagos con tarjeta.

Detección de Incidentes

- Monitoreo en tiempo real de todos los sistemas dentro del entorno de datos de tarjetas
- Alertas sobre actividades sospechosas o comportamientos anómalos
- Análisis y correlación de registros
- Escaneos regulares de vulnerabilidades y configuraciones incorrectas
- Canales de reporte para usuarios ante incidentes sospechosos

Gestión de Incidentes

Cuando se detecta un incidente de seguridad, seguimos un proceso estructurado:

1. Evaluación inicial y contención
2. Recolección y preservación de evidencia
3. Eliminación de la amenaza
4. Recuperación de sistemas afectados
5. Análisis posterior e implementación de mejoras

Requisitos de Notificación

En caso de una brecha confirmada o sospechosa que involucre datos de tarjetas, las notificaciones se realizarán según:

- Requisitos de PCI DSS
- Reglas de las marcas de pago
- Leyes aplicables de notificación de brechas de datos
- Obligaciones contractuales con nuestro procesador de pagos

Capacitación y Concienciación

Todo el personal con acceso a datos de tarjetas o sistemas dentro del CDE recibe capacitación regular en seguridad específica para su rol.

Programa de Concienciación en Seguridad

- Capacitación anual en seguridad para todos los empleados
- Capacitación específica por rol para personal con acceso directo a datos de tarjetas
- Actualizaciones y comunicaciones regulares sobre seguridad
- Ejercicios simulados de phishing para probar la concienciación
- Documentación clara de políticas y procedimientos de seguridad

Capacitación para Desarrolladores

- Prácticas de codificación segura para aplicaciones móviles
- Requisitos de seguridad para pagos con tarjeta
- Vulnerabilidades comunes y estrategias de mitigación
- Técnicas de implementación segura de APIs
- Metodologías de pruebas de seguridad

Mantenimiento y Revisión de la Política

Esta política será revisada al menos una vez al año y actualizada según sea necesario para reflejar cambios en tecnología, procesos de negocio o requisitos de cumplimiento.

Proceso de Revisión

- Evaluación del cumplimiento con los requisitos actuales de PCI DSS
- Evaluación de amenazas y vulnerabilidades emergentes

- Revisión del historial de incidentes de seguridad
- Validación de la efectividad de la política
- Incorporación de retroalimentación de las partes interesadas

Distribución de la Política

Al ser aprobada, esta política será:

- Publicada en nuestro repositorio interno de políticas
- Distribuida a todo el personal afectado
- Incorporada en materiales de capacitación relevantes
- Disponibilizada a auditores y evaluadores según sea requerido

Información de Contacto

Para preguntas o inquietudes sobre esta política, por favor contacte a:

CHRONOLOGY ENTERPRISES S.R.L.

Teléfono: +1 849-868-1908

Correo electrónico: Contact@Nyzerapp.com

Sitio web: https://www.nyzerapp.com/

Conclusión

CHRONOLOGY ENTERPRISES S.R.L. está comprometida con mantener los más altos estándares de seguridad en pagos con tarjeta mediante la implementación de esta política integral de seguridad en la transmisión de datos de tarjetas. Al adherirnos a estas directrices y mejorar continuamente nuestra postura de seguridad, buscamos proteger la información sensible de nuestros clientes y mantener su confianza en nuestros servicios.

Esta política entra en vigor de inmediato y reemplaza cualquier versión anterior.

Aprobado por:

Frankelly David Guzman Legreaux

Luis Alfonzo Guzman Legreaux

Fecha: 5 de marzo de 2025