



# Encryption Policy

vStream Digital Media / ShineVR

Date: 02 June 2025

Owner: Andrés Pitt, CTO

Next Review Date: 02 June 2026

Approved by: Andrés Pitt, CTO

## Definitions

Term	Definition
<b>Company</b>	means vStream Digital Media
<b>ShineVR</b>	means the ShineVR product developed and operated by vStream Digital Media
<b>GDPR</b>	means the General Data Protection Regulation
<b>Responsible Person</b>	means Andrés Pitt, CTO
<b>Encryption at Rest</b>	Encryption of data stored on disk or other storage media
<b>Encryption in Transit</b>	Encryption of data while it moves across networks
<b>AES-256</b>	Advanced Encryption Standard with 256-bit key length
<b>KMS</b>	Key Management Service - Google Cloud's centralized key management system
<b>PII</b>	Personally Identifiable Information

## 1. POLICY STATEMENT

vStream Digital Media is committed to protecting all data through comprehensive encryption measures. All ShineVR data and Company information is encrypted both at rest and in transit using industry-standard cryptographic algorithms and protocols.

This policy leverages the robust encryption capabilities of **Google Cloud Platform**, where all Company and ShineVR infrastructure is hosted, while defining additional encryption requirements specific to our operations.

## 2. PURPOSE

The purpose of this policy is to:

- Protect the confidentiality and integrity of Company and ShineVR data
- Ensure compliance with GDPR and other data protection regulations
- Define encryption standards for data at rest and in transit
- Establish secure key management practices
- Prevent unauthorized access to sensitive information
- Minimize the impact of potential data breaches

## 3. SCOPE

This policy applies to:

- All data processed, stored, or transmitted by vStream Digital Media
- All ShineVR application data including user interaction data, pain scores, and configuration data
- All data stored on Google Cloud infrastructure in Eemshaven, Netherlands (europe-west4-a) and St. Ghislain, Belgium (europe-west1-b)
- All Company employee data, customer data, and business information
- All employees, contractors, temporary staff, and third-party suppliers

This policy covers:

- Data stored in Google Cloud databases (Cloud SQL)
- Data stored in Google Cloud Storage buckets
- Data transmitted between ShineVR applications and users
- Data transmitted between Company systems and cloud infrastructure
- Backup data stored on Google Cloud
- Data in Docker containers and Cloud Run instances

## 4. ENCRYPTION ALGORITHMS AND STANDARDS

### 4.1 Approved Encryption Algorithms

**For Data at Rest:**

- **AES-256 (Advanced Encryption Standard with 256-bit keys)** - Primary standard
- AES-128 may be used only where AES-256 is not technically feasible
- All Google Cloud storage services use AES-256 by default

### For Data in Transit:

- **TLS 1.2 or higher (Transport Layer Security)** - Mandatory minimum standard
- TLS 1.3 is preferred where supported
- SSL is deprecated and must not be used

### For Key Encryption:

- Keys are encrypted using Google Cloud KMS envelope encryption
- Master keys use AES-256
- Data encryption keys (DEKs) are encrypted by key encryption keys (KEKs)

## 4.2 Prohibited Algorithms

The following are explicitly prohibited due to known vulnerabilities:

- DES (Data Encryption Standard)
- 3DES (Triple DES)
- RC4
- MD5 (for cryptographic purposes)
- SHA-1 (for cryptographic purposes)
- SSL (all versions)
- TLS 1.0 and TLS 1.1

## 5. ENCRYPTION AT REST

### 5.1 Google Cloud Infrastructure

- All data stored on Google Cloud infrastructure is **automatically encrypted at rest using AES-256**
- This applies to:
  - Cloud SQL databases (MySQL, PostgreSQL)
  - Cloud Storage buckets
  - Persistent disks attached to virtual machines
  - Cloud Run container storage
  - Backup data stored by Google Cloud services

### 5.2 ShineVR Application Data

For the trial configuration:

- ShineVR does not collect or store Personally Identifiable Information (PII)
- Users are identified by random 16-digit anonymous codes
- All user interaction data and VAS pain scores are encrypted at rest
- Data is stored in encrypted Cloud SQL databases

For other ShineVR configurations where PII may be present:

- PII is stored encrypted in the database
- Encryption keys are required to decrypt PII
- Keys are injected using Google Cloud Key Management Service

- Keys are never stored on disk inside the server

## 5.3 Company Data

- All Company business data stored on Google Drive is encrypted at rest
- Employee records and HR data benefit from Google Workspace encryption
- Financial records and business documents are encrypted by default

## 5.4 Backup Data

- All backup data is encrypted using the same AES-256 standard
- Backups are managed by Google Cloud services
- Backup encryption is automatic and requires no manual intervention
- Backup retention follows the Company's Media Retention and Disposal Policy

## 5.5 Local Device Storage

- Company-issued devices must use full-disk encryption (BitLocker for Windows, FileVault for macOS)
- Sensitive data should not be stored on local devices where possible
- Files stored on employee devices should be kept on encrypted Google Drive

# 6. ENCRYPTION IN TRANSIT

## 6.1 Network Communication

All data transmitted across networks must be encrypted using TLS:

- **Minimum TLS 1.2** for all connections
- **TLS 1.3** preferred where supported
- Certificate validation must be enabled
- Self-signed certificates are prohibited in production

## 6.2 ShineVR Application Traffic

- All communication between ShineVR mobile apps and backend servers uses **HTTPS with TLS 1.2+**
- All API calls are encrypted in transit
- WebSocket connections (if used) must use WSS (WebSocket Secure)
- No sensitive data may be transmitted over unencrypted HTTP

## 6.3 Google Cloud Internal Traffic

- Traffic between Google Cloud services is automatically encrypted by Google
- This includes traffic between Cloud Run instances, Cloud SQL databases, and Cloud Storage
- Google uses its private fiber network with encryption by default

## 6.4 Email Communication

- Company email (Google Workspace) enforces TLS for email transmission

- DMARC, DKIM, and SPF are configured for email security
- Sensitive information should be shared via encrypted links rather than email attachments where possible

## 6.5 Remote Access

- All remote access to Company systems must use encrypted connections
- Google Cloud Platform access requires TLS encryption
- SSH connections to any systems must use encrypted key-based authentication
- VPN connections (if used) must use strong encryption protocols

## 6.6 Wireless Networks

- Company wireless networks must use **WPA2** or higher encryption
- WPA3 is preferred where supported
- WEP and open wireless networks are strictly prohibited
- Guest wireless networks must be segregated from Company networks

# 7. KEY MANAGEMENT

## 7.1 Google Cloud Key Management Service (KMS)

- All encryption keys are managed using **Google Cloud Key Management Service**
- Google Cloud KMS provides:
  - Centralized key management
  - Automatic key rotation
  - Audit logging of key usage
  - Hardware security module (HSM) backing
  - Geographic key storage control (Europe)

## 7.2 Key Storage and Protection

- Encryption keys are **never stored on disk inside application servers**
- Keys are injected into applications at runtime via Google Cloud KMS
- Keys are stored in Google Cloud KMS in encrypted form (envelope encryption)
- Master keys are protected by Google-managed HSMs in European data centers

## 7.3 Key Access Control

- Access to encryption keys is restricted using **Principle of Least Privilege**
- Only authorized applications and services can access specific keys
- Google Cloud IAM policies control key access permissions
- Key access is assigned to service accounts, not individual users
- All key access attempts are logged for audit purposes

## 7.4 Key Rotation

- Encryption keys should be rotated regularly to minimize risk:
  - **Automatic rotation:** Google Cloud manages key rotation for infrastructure encryption

- **Application keys:** Rotated annually or when compromise is suspected
- **Emergency rotation:** Immediate rotation if key compromise is detected or suspected

## 7.5 Key Lifecycle

Keys follow a defined lifecycle:

1. **Generation:** Keys are generated by Google Cloud KMS using secure random number generation
2. **Active Use:** Keys are used for encryption/decryption operations
3. **Rotation:** New keys replace old keys according to rotation schedule
4. **Disabled:** Old keys are disabled but retained for decryption of existing data
5. **Destruction:** Keys are destroyed after data encrypted with them is no longer needed (follows retention schedules)

## 7.6 Key Backup and Recovery

- Google Cloud KMS automatically backs up keys across multiple geographic locations
- Key recovery is managed by Google's infrastructure redundancy
- Company does not maintain separate key backups
- Disaster recovery procedures include key recovery verification

# 8. DATA CLASSIFICATION AND ENCRYPTION REQUIREMENTS

Data Classification	Encryption at Rest	Encryption in Transit	Key Management
<b>PII / Sensitive Personal Data</b>	AES-256 (Mandatory)	TLS 1.2+ (Mandatory)	Google Cloud KMS with restricted IAM
<b>Health Data (Pain Scores)</b>	AES-256 (Mandatory)	TLS 1.2+ (Mandatory)	Google Cloud KMS with restricted IAM
<b>Company Confidential</b>	AES-256 (Mandatory)	TLS 1.2+ (Mandatory)	Google Cloud KMS
<b>Internal Data</b>	AES-256 (Default)	TLS 1.2+ (Mandatory)	Google Cloud KMS
<b>Public Data</b>	AES-256 (Default)	TLS 1.2+ (Recommended)	Google Cloud KMS

# 9. ANONYMIZATION AND PSEUDONYMIZATION

For ShineVR trials:

- **Anonymization** is used as the primary data protection measure
- Users are identified by random 16-digit codes
- ShineVR cannot associate codes with identified individuals
- Customer (as Data Controller) maintains the mapping between users and codes
- This approach reduces privacy risks beyond encryption alone

For other configurations:

- **Pseudonymization** may be used where full anonymization is not feasible
- User IDs are used in reports instead of PII
- Dates of events may be removed to prevent user identification

## 10. ENCRYPTION IMPLEMENTATION

### 10.1 Google Cloud Platform Configuration

- All Google Cloud storage services have encryption enabled by default
- Encryption cannot be disabled for Google Cloud services
- Company uses Google-managed encryption keys (GMEK) for base infrastructure
- Customer-managed encryption keys (CMEK) may be used for additional control where needed

### 10.2 ShineVR Application Implementation

- Docker containers are built with encryption libraries included
- Application code accesses encrypted data via secure API calls
- Sensitive configuration parameters are stored in Google Cloud Secret Manager
- Database connections use encrypted TLS connections

### 10.3 Development and Testing

- Development and testing environments use the same encryption standards as production
- Test data must not contain real PII (data is anonymized or synthetically generated)
- Encryption keys for dev/test environments are separate from production
- Production keys must never be used in development or testing

## 11. MONITORING AND COMPLIANCE

### 11.1 Encryption Monitoring

- Google Cloud Security Command Centre monitors encryption status daily
- Automated alerts trigger if encryption is disabled or misconfigured
- Weekly review of Google Command Centre by CTO
- Encryption compliance is tracked across 19 Google Cloud compliance standards including:
  - ISO 27001

- PCI DSS 3.2.1
- HIPAA
- NIST 800-53

## 11.2 Audit Logging

- All encryption key access is logged by Google Cloud KMS
- Logs are retained for audit and compliance purposes
- Unusual key access patterns trigger security alerts
- Logs are reviewed as part of incident investigation

## 11.3 Vulnerability Management

- Docker containers undergo automated vulnerability scanning
- Encryption library versions are monitored for known vulnerabilities
- Security patches for encryption components are prioritized for deployment
- If encryption vulnerabilities are discovered, deployment is blocked until remediated

# 12. INCIDENT RESPONSE

## 12.1 Encryption Failure

If encryption fails or is discovered to be misconfigured:

1. Immediate containment: Affected systems are isolated
2. CTO notification: Within 30 minutes of discovery
3. Impact assessment: Determine what data was unencrypted
4. Remediation: Enable encryption and verify configuration
5. Data breach assessment: Determine if GDPR breach notification required

## 12.2 Key Compromise

If an encryption key is compromised or suspected to be compromised:

1. Immediate key rotation: New key generated and deployed
2. Affected data re-encryption: Data is re-encrypted with new key
3. Access review: Review who had access to the compromised key
4. Incident investigation: Determine how compromise occurred
5. Monitoring: Enhanced monitoring for any use of the old key

## 12.3 Compromised Credentials

- Google Cloud services monitor for compromised passwords or keys on VMs
- Monitoring is managed by Google Cloud services
- Alerts are sent via email and Slack for prompt resolution
- Compromised credentials are immediately rotated

# 13. THIRD-PARTY SERVICES

## 13.1 Cloud Service Providers

- Google Cloud Platform is the Company's primary infrastructure provider
- Google maintains comprehensive security certifications including:
  - ISO 27001, ISO 27017, ISO 27018
  - SOC 1, SOC 2, SOC 3
  - PCI DSS compliance
  - CSA STAR certification

## 13.2 Other Third-Party Services

- Any third-party service processing Company or ShineVR data must provide encryption at rest and in transit
- Third-party encryption standards must meet or exceed Company standards
- Vendor encryption capabilities are assessed during vendor selection
- Vendor compliance with encryption requirements is monitored ongoing

# 14. DATA PORTABILITY AND EXPORT

When exporting data from Company or ShineVR systems:

- Exported data must be encrypted before transfer
- Encryption keys must be communicated via separate secure channel
- Exported data should be deleted after successful import by recipient
- Export logs are maintained for audit purposes

# 15. DATA DISPOSAL

When data reaches end of retention period:

- Data is deleted such that it is **irrecoverable**
- Encrypted data is rendered unreadable by:
  - Destroying encryption keys (cryptographic erasure)
  - Overwriting storage media (if keys cannot be destroyed)
- Google Cloud handles physical media destruction for their infrastructure
- Disposal is documented in the Company's data disposal register

# 16. COMPLIANCE AND REGULATORY REQUIREMENTS

This encryption policy supports compliance with:

- **GDPR:** Article 32 (Security of Processing) requires appropriate technical measures including encryption
- **GDPR:** Article 34 allows for exemption from breach notification if data was encrypted
- **ISO 27001:** Multiple controls related to cryptographic controls
- **HIPAA:** Encryption as an addressable implementation specification
- **PCI DSS:** Requirements for encryption of cardholder data

## 17. EXCEPTIONS

Exceptions to this policy are rarely justified but may be considered for:

- Legacy systems being decommissioned where encryption is technically infeasible
- Public data with no confidentiality requirements
- Temporary development environments with synthetic data only

All exceptions must:

- Be requested in writing to the CTO
- Include detailed business and technical justification
- Document compensating controls
- Be approved in writing by the CTO
- Be reviewed quarterly
- Be limited in duration

## 18. ROLES AND RESPONSIBILITIES

Role	Responsibilities
<b>CTO (Responsible Person)</b>	Policy ownership; Google Cloud KMS configuration; key management oversight; encryption monitoring; incident response; exception approval
<b>Backend Developers</b>	Implement encryption in applications; secure key usage; avoid storing keys in code; report encryption issues
<b>Product Manager</b>	Ensure ShineVR features maintain encryption requirements; approve changes affecting encryption
<b>All Employees</b>	Protect encryption keys; use encrypted connections; report encryption issues; complete security training
<b>IT Administrators</b>	Configure Google Cloud encryption settings; monitor encryption compliance; maintain audit logs

## 19. TRAINING AND AWARENESS

- All developers receive encryption best practices training during onboarding
- Annual security awareness training includes encryption requirements
- Specific training for personnel handling encryption keys
- Training covers:
  - Importance of encryption

- How to verify encrypted connections (HTTPS, TLS)
- What to do if encryption fails
- Key management best practices
- Incident reporting procedures

## 20. POLICY REVIEW

- This policy will be reviewed **annually** by the CTO
- Reviews consider:
  - Changes in encryption standards and algorithms
  - New vulnerabilities or attacks against encryption
  - Regulatory requirement changes
  - Technology changes (e.g., quantum computing threats)
  - Lessons learned from security incidents
- Policy updates are communicated to all staff

## 21. RELATED POLICIES

This policy should be read in conjunction with:

- Information Security Policy
- Password Policy
- Access Management Process/Procedure
- Backup Policy
- Incident Management Policy and Procedure
- Media Retention and Disposal Policy

## 22. CONTACT INFORMATION

For questions regarding this policy or to report encryption-related security incidents:

**Data Protection Officer / CTO** Andrés Pitt Email: [andres@vstream.ie](mailto:andres@vstream.ie) Phone: (086) 788 6570