Information Security Policy

vStream Digital Media

Last updated 03/02/25

1. Definitions

Information Security: The protection of information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Information Assets: Any data, information system, application, hardware, or digital resource owned or managed by vStream Digital Media, including ShineVR application data, source code, customer information, and business records.

ShineVR: vStream's immersive Cognitive Behavioural Therapy (CBT) platform for pain management, delivered as a virtual reality application to healthcare customers.

Personal Data: Any information relating to an identified or identifiable natural person, as defined by the General Data Protection Regulation (GDPR).

Security Incident: Any event that could compromise the confidentiality, integrity, or availability of information assets, including data breaches, system failures, unauthorised access attempts, and security policy violations.

Data Processor: An entity that processes personal data on behalf of a Data Controller. vStream acts as a Data Processor for customer trials, where the customer is the Data Controller.

2. Policy Statement

vStream Digital Media is committed to protecting the confidentiality, integrity, and availability of all information assets, including those related to our ShineVR product and services provided to healthcare customers. This policy establishes the framework for information security across all aspects of our business operations, development activities, and customer service delivery.

All employees, contractors, and third parties with access to vStream systems or information must comply with this policy and all referenced security policies. Non-compliance may result in disciplinary action, including termination of employment or contract, and may be reported to relevant authorities where legally required.

This policy applies to all information systems, applications, data, and infrastructure operated by vStream, including our Google Cloud Platform environment where ShineVR and associated services are hosted.

3. Purpose

The purpose of this policy is to:

- Establish clear information security requirements for all vStream operations

- Protect customer data, particularly sensitive healthcare information in ShineVR applications
- Ensure compliance with legal and regulatory requirements including GDPR, healthcare regulations, and customer contractual obligations
- Protect vStream's intellectual property, including ShineVR source code, proprietary algorithms, and business information
- Maintain the trust of customers, partners, and stakeholders through demonstrable security practices
- Provide a framework that supports business objectives while managing security risks

4. Scope

This policy applies to all:

- Employees, contractors, consultants, and temporary staff working for vStream Digital Media
- Information systems, applications, and infrastructure, including the ShineVR platform
- Google Cloud Platform resources in europe-west4-a (Netherlands) and europe-west1-b (Belgium) data centres
- Development, staging, and production environments
- Customer data, including anonymised trial data and other healthcare information
- Business information, intellectual property, and proprietary data
- Third-party systems and services that process vStream or customer data

5. Information Security Framework

5.1 Infrastructure Security

vStream operates entirely on Google Cloud Platform with no on-premise data hosting. Our infrastructure security strategy relies on:

- **Google Cloud Platform:** All systems hosted in europe-west4-a (Netherlands, primary) and europe-west1-b (Belgium, secondary) data centres, ensuring EU data residency
- **Container-Based Architecture:** Docker containers deployed via Google Cloud Run, replacing legacy VM infrastructure as of 2025
- **Infrastructure-as-Code:** All infrastructure configuration managed in version control with code review and approval requirements
- **Google Cloud Security Command Centre:** Continuous monitoring across 19 compliance standards including ISO 27001, CIS benchmarks, HIPAA, SOC2, OWASP, and PCI DSS
- **Physical Security:** Reliance on Google's data centre security controls with no customer data stored at vStream premises (see Physical Security Policy)

Related Policies: Cloud Security Policy, Network Security Policy, Physical Security Policy

5.2 Access Control

Access to vStream systems and ShineVR applications is controlled through:

- **Role-Based Access Control (RBAC):** Four standard roles (User, Manager, Admin, SuperAdmin) with specific ShineVR application roles for healthcare users
- **Multi-Factor Authentication (MFA):** Mandatory for all Google Cloud Platform access, privileged accounts, and remote system access. Enforced via Google Workspace

- **Google Cloud IAM:** Centralised identity and access management with principle of least privilege
- **Environment Segregation:** Separate access controls for development, staging, and production environments
- **Regular Access Reviews:** Quarterly reviews of all user access rights and annual comprehensive audits
- **Automated Testing:** Over 400 automated tests including RBAC and access violation testing

Related Policies: Access Management Policy, Password Policy

5.3 Data Protection and Encryption

All vStream and ShineVR data is protected through:

- **Encryption at Rest:** AES-256 encryption for all data stored in Google Cloud Storage, Cloud SQL databases, and persistent disks. Managed via Google Cloud Key Management Service (KMS)
- **Encryption in Transit:** TLS 1.2 or higher for all data transmission, including internal service-to-service communication
- **Key Management:** Encryption keys never stored on disk, managed exclusively through Google Cloud KMS with automated rotation
- **Data Anonymisation:** ShineVR trial data uses 16-digit random codes, ensuring no personally identifiable information (PII) is stored. Customer maintains the linkage between codes and individuals as Data Controller
- **EU Data Residency:** All customer data remains within EU data centres (Netherlands and Belgium), with no international data transfers

Related Policies: Encryption Policy, Media Retention and Disposal Policy

5.4 Password Management

vStream enforces strong password requirements:

- **Minimum Length:** 12 characters
- **Complexity:** Must include uppercase, lowercase, numbers, and special characters
- **Refresh Cycle:** 90-day mandatory password change
- **History Restriction:** Cannot reuse last 5 passwords
- **Account Lockout:** Automatic lockout after 5 failed login attempts
- **Enforcement:** Technical controls implemented via Google Workspace with policy compliance monitoring

Related Policies: Password Policy

5.5 Backup and Recovery

Business continuity is ensured through:

- **Automated Backups:** Daily automated backups of all production databases and critical systems
- **Retention Periods:** Mission-critical data retained indefinitely, non-mission-critical data retained for 6 months, transaction logs for 30 days
- **Recovery Objectives:** Recovery Time Objective (RTO) of 8 hours and Recovery Point Objective (RPO) of 24 hours for application layer
- **Testing:** Monthly restoration testing, quarterly disaster recovery simulations, annual comprehensive exercises

- **ShineVR Trial Data:** trial data ringfenced for easy deletion at end of contract while maintaining whole-of-database backup capability

Related Policies: Backup and Recovery Policy

5.6 Change Control and System Development

vStream follows a "release early, release often" development philosophy with robust security controls:

- **Mandatory Code Review:** All production deployments require approval from CTO or Product Manager. No self-approval permitted
- **Automated Testing:** Over 400 automated tests including security tests, RBAC tests, and access violation tests. Failed tests block deployment
- **CI/CD Pipeline:** Five-stage automated pipeline (Build, Test, Scan, Staging, Production) with approval gates
- **Environment Segregation:** Separate development, staging, and production environments with distinct access controls
- **Security by Design:** Security requirements incorporated from initial design phase
- **Audit Trails:** ShineVR maintains full audit trails for all content and data changes

Related Policies: Change Control Policy, System Development Methodology

5.7 Incident Response

vStream maintains a comprehensive incident response framework:

- **Severity Classification:** Three-tier system (P1 Critical, P2 High, P3 Low) with defined response timeframes
- **Response Times:** P1 incidents: 15 minutes initial response; P2 incidents: 2 hours; P3 incidents: 24 hours
- **24/7 Escalation:** Direct phone lines for CTO, CPO, and Account Director for critical incidents
- **Breach Notification:** GDPR-compliant notification procedures with 72-hour reporting requirement to Data Protection Commission
- **Post-Incident Review:** Mandatory review process for all P1 and P2 incidents with lessons learned documentation

Related Policies: Incident Response Plan

5.8 Logging and Monitoring

Comprehensive logging and monitoring provides visibility into security events:

- **Google Cloud Logging:** Centralised logging for all system events, application logs, and security events
- **Cloud Audit Logs:** Complete audit trail of who did what, when, and where in Google Cloud Platform
- **Security Command Centre:** Continuous monitoring across 19 compliance standards with weekly CTO review of findings
- **Application Audit Trails:** ShineVR maintains detailed audit trails for all content and data changes
- **Automated Alerting:** Real-time alerts for security events, failed access attempts, and system anomalies

Related Policies: Log Management Policy

5.9 Network Security

vStream's cloud-native architecture provides network security through:

- **Google Cloud Firewall:** Software-defined networking with granular firewall rules controlling traffic flow
- **Private Networks:** Cloud SQL databases accessible only via private IP addresses, not exposed to public internet
- **Network Segmentation:** Logical isolation between development, staging, and production environments
- **DDoS Protection:** Google Cloud Load Balancer provides distributed denial-of-service protection
- **No VPN Required:** Cloud-native architecture eliminates need for traditional VPN with secure access via Google Cloud IAM and MFA
- **Wireless Security:** WPA2 minimum for all wireless networks, WPA3 preferred

Related Policies: Network Security Policy

5.10 Vendor Management

Third-party vendors are managed through:

- **Risk Classification:** Four-tier system (Low, Medium, High, Critical) based on data access and business impact
- **Security Assessments:** Evaluation of vendor security practices, certifications, and compliance before engagement
- **Data Processing Agreements:** GDPR-compliant DPAs required for all vendors processing customer data
- **EU Preference:** Preference for EU-based vendors to maintain data residency and GDPR compliance
- **Ongoing Monitoring:** Annual vendor security reviews and performance monitoring

Related Policies: Vendor Management Policy

5.11 Personnel Security

Employee and contractor security measures include:

- **Background Checks:** Comprehensive background verification including identity verification for all employees with system access
- **Staged Access:** New employees receive development and staging access only until background checks complete; production access granted after verification
- **Security Training:** Mandatory security awareness training for all staff, with specialised training for developers and system administrators
- **BYOD Security:** Security requirements for personal devices used for work, including encryption, anti-malware, and home network security
- **Termination Process:** Systematic removal of access within 24 hours of employment termination

Related Policies: Background Check Policy, BYOD Policy

6. Compliance and Regulatory Requirements

6.1 General Data Protection Regulation (GDPR)

vStream complies with GDPR requirements through:

- **Lawful Processing:** Clear legal basis for all data processing activities

- **Data Minimisation:** Collection of only necessary data; use of anonymisation where possible (e.g., 16-digit codes for trial)
- **Storage Limitation:** Defined retention periods with systematic deletion procedures
- **Data Subject Rights:** Procedures to support rights of access, rectification, erasure, and portability
- **Breach Notification:** 72-hour notification to Data Protection Commission for qualifying breaches
- **Data Protection Officer:** Andrés Pitt (CTO) serves as DPO, contactable at andres@vstream.ie

6.2 Healthcare Regulations

For healthcare customers:

- **Data Controller/Processor Relationship:** Clear delineation where customers act as Data Controller and vStream as Data Processor
- **Anonymisation:** ShineVR trial uses anonymised data with no PII stored by vStream
- **Data Residency:** All data maintained within EU data centres
- **Security Standards:** Compliance with healthcare security requirements and customer contractual obligations

6.3 ISO 27001 Alignment

vStream security practices align with ISO 27001 information security management standards. Google Cloud Security Command Centre monitors compliance with ISO 27001 2022 controls.

Our policies and procedures address all ISO 27001 Annex A control domains including access control, cryptography, operations security, communications security, system development, supplier relationships, incident management, business continuity, and compliance.

7. Roles and Responsibilities

7.1 Chief Technology Officer (CTO) / Data Protection Officer

- Overall responsibility for information security strategy and implementation
- Approval of all security policies and procedures
- Weekly review of Security Command Centre findings
- Data protection compliance and regulatory liaison
- Incident response coordination for P1 incidents

7.2 Product Manager

- Code review and approval for production deployments
- Security requirements definition for ShineVR features
- Customer security requirement coordination

7.3 Backend Developers

- Secure coding practices implementation
- Security testing and vulnerability remediation
- Infrastructure-as-Code development and maintenance
- Security incident investigation and resolution

7.4 All Employees

- Compliance with all security policies and procedures

- Protection of credentials and access tokens
- Reporting of security incidents and suspicious activities
- Completion of mandatory security training
- BYOD security requirements compliance

8. Policy Review and Maintenance

This Information Security Policy is reviewed annually by the CTO to ensure continued relevance and effectiveness. Reviews are also triggered by:

- Significant security incidents or data breaches
- Changes to regulatory requirements or legal obligations
- Major infrastructure or architectural changes
- New customer requirements or contractual obligations
- Introduction of new products or services

All policy updates require CTO approval and are communicated to all staff within 10 working days of approval.

9. Related Policies and Documents

This policy should be read in conjunction with the following vStream policies:

- Password Policy
- Encryption Policy
- Access Management Policy
- Incident Response Plan
- Backup and Recovery Policy
- Change Control Policy
- Log Management Policy
- Media Retention and Disposal Policy
- Cloud Security Policy
- Network Security Policy
- Physical Security Policy
- Vendor Management Policy
- Background Check Policy
- BYOD Policy
- System Development Methodology

10. Contact Information

Data Protection Officer / Chief Technology Officer:

Andrés Pitt

Email: andres@vstream.ie

Phone: (086) 788 6570

Available 24/7 for P1 security incidents

Company Address:

vStream Digital Media

37 Leeson Close

Dublin 2, D02 H344

Ireland

Website: vstream.ie