



Log Management Policy

vStream Digital Media

Last changed 03/02/25

1. Definitions

Log: A record of an event, action, or transaction that occurred within an information system, application, or network device. Logs provide an audit trail for security monitoring, troubleshooting, and compliance purposes.

Audit Trail: A chronological record that provides documentary evidence of the sequence of activities affecting a specific operation, procedure, or event. In ShineVR, this includes all content and data changes.

Security Event: Any occurrence that could indicate a potential security incident, policy violation, or threat to information assets, including failed login attempts, unauthorised access attempts, and configuration changes.

Google Cloud Logging: Google Cloud Platform's centralised logging service that collects, stores, and analyses logs from all GCP resources, applications, and services.

Cloud Audit Logs: Google Cloud Platform's audit logging that records who did what, when, and where within the GCP environment, including Admin Activity, Data Access, System Event, and Policy Denied logs.

Security Command Centre: Google Cloud Platform's security and risk management platform that provides centralised visibility, threat detection, and compliance monitoring across the entire GCP environment.

Term	Definition/Detail
Log	A record of an event, action, or transaction that occurred within an information system, application, or network device. Logs provide an audit trail for security monitoring, troubleshooting, and compliance purposes.
Audit Trail	A chronological record that provides documentary evidence of the sequence of activities affecting a specific operation, procedure, or event. In ShineVR, this includes all content and data changes.

Security Event	Any occurrence that could indicate a potential security incident, policy violation, or threat to information assets, including failed login attempts, unauthorised access attempts, and configuration changes.
Google Cloud Logging	Google Cloud Platform's centralised logging service that collects, stores, and analyses logs from all GCP resources, applications, and services.
Cloud Audit Logs	Google Cloud Platform's audit logging that records who did what, when, and where within the GCP environment, including Admin Activity, Data Access, System Event, and Policy Denied logs.
Security Command Centre	Google Cloud Platform's security and risk management platform that provides centralised visibility, threat detection, and compliance monitoring across the entire GCP environment.

2. Policy Statement

vStream Digital Media maintains comprehensive logging and monitoring of all systems, applications, and infrastructure to support security incident detection, investigation, compliance requirements, and operational troubleshooting. This policy establishes requirements for log generation, collection, retention, protection, and analysis across all vStream systems, with particular attention to ShineVR application activities and Google Cloud Platform infrastructure.

All systems must generate appropriate logs, and all personnel must cooperate with log analysis activities. Tampering with, disabling, or circumventing logging mechanisms is strictly prohibited and may result in disciplinary action.

Logs are treated as sensitive information assets and must be protected with appropriate access controls and encryption. Log data may contain personal information and must be handled in compliance with GDPR requirements.

3. Purpose

The purpose of this policy is to:

- Enable detection of security incidents and unauthorised activities
- Support incident investigation and forensic analysis
- Demonstrate compliance with regulatory requirements including GDPR and healthcare regulations
- Provide audit trails for ShineVR content and data changes
- Support operational troubleshooting and performance monitoring
- Enable accountability by tracking user actions and system changes

- Maintain compliance with customer contractual requirements, particularly for healthcare customers

4. Scope

This policy applies to:

- All Google Cloud Platform resources in europe-west4-a (Netherlands) and europe-west1-b (Belgium)
- ShineVR application and all associated services
- Cloud Run containers and container orchestration
- Cloud SQL databases and data storage systems
- Google Cloud IAM authentication and authorisation events
- Network traffic and firewall logs
- Development, staging, and production environments
- All employees, contractors, and systems with access to vStream infrastructure

5. Logging Requirements

5.1 Google Cloud Logging Infrastructure

vStream utilises Google Cloud Platform's centralised logging infrastructure:

- **Cloud Logging:** Centralised collection of logs from all GCP services, applications, and infrastructure components
- **Structured Logging:** JSON-formatted logs with consistent fields including timestamp, severity, resource, and message content
- **Real-Time Collection:** Logs ingested in real-time with minimal delay between event occurrence and log availability
- **Automatic Collection:** Google Cloud Platform services automatically generate logs without manual configuration
- **Log Routing:** Automatic routing of logs to appropriate storage locations based on log type and retention requirements

5.2 Cloud Audit Logs

Google Cloud Audit Logs provide comprehensive audit trails of all activities within the GCP environment:

- **Admin Activity Logs:** Records administrative actions including resource creation, deletion, configuration changes, and permission modifications. Retained for 400 days by default
- **Data Access Logs:** Records operations that read or modify user-provided data, including database queries and API calls. Retained for 30 days by default
- **System Event Logs:** Records Google Cloud Platform system events such as maintenance operations and automatic scaling. Retained for 400 days by default
- **Policy Denied Logs:** Records security policy violations when users are denied access to resources. Retained for 30 days by default
- **Audit Log Content:** Each audit log entry includes principal (who), operation (what), resource (where), timestamp (when), and outcome (success/failure)

5.3 ShineVR Application Audit Trails

The ShineVR application maintains detailed audit trails for all content and data operations:

- **Content Changes:** All modifications to ShineVR content including therapy scenarios, VR environments, and therapeutic content are logged with user identity, timestamp, and change details
- **Data Access:** All access to patient/trial data including view, export, and download operations are logged
- **User Actions:** All user authentication events, role changes, permission modifications, and administrative actions
- **System Events:** Application startup, shutdown, configuration changes, and error conditions
- **Trial Data:** Specific audit logging for Customer trial activities including VAS pain score entries, session completions, and anonymised code usage
- **Immutable Records:** Audit trail entries cannot be modified or deleted by application users, ensuring integrity of the audit record

5.4 Security Event Logging

Critical security events are logged with enhanced detail:

- **Authentication Events:** All login attempts (successful and failed), multi-factor authentication events, password changes, and session terminations
- **Authorisation Events:** Access control decisions, privilege escalations, role assignments, and permission denials
- **Network Security:** Firewall rule changes, network access violations, unusual traffic patterns, and DDoS mitigation events
- **Configuration Changes:** Infrastructure-as-Code deployments, security policy modifications, encryption key operations, and service configuration updates
- **Vulnerability Detection:** Container vulnerability scan results, Security Command Centre findings, and security test failures
- **Incident Response:** Security incident declarations, escalations, containment actions, and resolution activities

5.5 Application and System Logs

Standard operational logging includes:

- **Application Logs:** ShineVR application events, errors, warnings, and informational messages including request/response logging for API calls
- **Container Logs:** Docker container startup, shutdown, health checks, and resource utilisation from Cloud Run
- **Database Logs:** Cloud SQL query logs (when enabled), connection events, and database errors
- **Load Balancer Logs:** HTTP/HTTPS request logs including source IP, request method, response code, and latency
- **Platform Logs:** Google Cloud Platform service logs including Cloud Run, Cloud Storage, and Cloud KMS operations

6. Security Command Centre Monitoring

vStream utilises Google Cloud Security Command Centre for continuous security monitoring and compliance:

6.1 Compliance Standards Monitoring

Security Command Centre monitors 19 compliance standards including:

- **CIS Google Cloud Platform Foundation 2.0**
- **ISO 27001 2022**

- **HIPAA**
- **SOC2 2017**
- **OWASP 2017 & 2021**
- **PCI DSS 3.2.1**
- **Multiple CIS Benchmarks**

6.2 Automated Detection and Alerting

Security Command Centre provides:

- **Threat Detection:** Automated detection of security threats including malware, cryptomining, anomalous behaviour, and data exfiltration attempts
- **Vulnerability Scanning:** Continuous scanning of containers, web applications, and infrastructure for known vulnerabilities
- **Misconfiguration Detection:** Identification of security misconfigurations including overly permissive IAM policies, public storage buckets, and weak encryption settings
- **Compliance Drift:** Alerting when infrastructure configuration drifts from compliance standards
- **Real-Time Alerts:** Immediate notification of high-severity findings via email and monitoring dashboards

6.3 Review and Remediation

- **Weekly CTO Review:** CTO reviews Security Command Centre findings every week, prioritising high and critical severity issues
- **Finding Triage:** Classification of findings by severity (Critical, High, Medium, Low) and assignment to appropriate team members
- **Remediation Tracking:** Documentation of remediation actions and tracking to closure
- **Trend Analysis:** Monthly analysis of security trends, recurring issues, and compliance score changes

7. Automated Testing and Access Monitoring

vStream maintains over 400 automated tests that generate logs for security monitoring:

- **RBAC Testing:** Automated tests verify role-based access controls for all four standard roles (User, Manager, Admin, SuperAdmin) and ShineVR-specific roles
- **Access Violation Testing:** Tests attempt unauthorised access to verify that access controls properly deny invalid requests. All test results are logged
- **Security Test Failures:** Failed security tests generate high-priority logs and block deployment to production
- **Continuous Testing:** Tests run automatically on every code commit as part of the CI/CD pipeline
- **Test Result Logging:** All test executions, results, and failures are logged to Google Cloud Logging for audit and analysis

8. Log Retention

8.1 Retention Periods

Log retention periods are based on log type and regulatory requirements:

- **Cloud Audit Logs (Admin Activity):** 400 days (Google Cloud default)
- **Cloud Audit Logs (Data Access):** 30 days (Google Cloud default), extended to 90 days for ShineVR production database access

- **Security Event Logs:** 1 year minimum for incident investigation and forensic purposes
- **ShineVR Application Audit Trails:** 7 years for trial data audit trails to support potential future audits and investigations
- **Application Logs:** 30 days for operational troubleshooting
- **System Performance Logs:** 30 days for capacity planning and performance analysis
- **Security Command Centre Findings:** Retained indefinitely for trend analysis and compliance reporting

8.2 Log Storage and Protection

- **Encrypted Storage:** All logs encrypted at rest using AES-256 via Google Cloud KMS
- **Access Controls:** Logs accessible only to authorised personnel (CTO, backend developers with specific IAM permissions)
- **Immutability:** Cloud Audit Logs and ShineVR audit trails are immutable and cannot be modified or deleted by users
- **Secure Transmission:** All log transmission encrypted using TLS 1.2 or higher
- **Geographic Restrictions:** Logs stored exclusively in EU data centres (europe-west4-a and europe-west1-b) for data residency compliance

9. Log Analysis and Monitoring

9.1 Continuous Monitoring

- **Real-Time Analysis:** Automated analysis of logs in real-time to detect security events, anomalies, and policy violations
- **Automated Alerting:** Immediate alerts for critical events including failed authentication attempts, unauthorised access attempts, security test failures, and infrastructure changes
- **Dashboard Monitoring:** Google Cloud Console dashboards for real-time visibility into security events, system health, and compliance status
- **Anomaly Detection:** Machine learning-based anomaly detection for unusual patterns in authentication, data access, and system behaviour

9.2 Regular Reviews

- **Weekly Security Review:** CTO reviews Security Command Centre findings, security event logs, and failed access attempts
- **Monthly Analysis:** Trend analysis of security events, access patterns, and compliance scores
- **Quarterly Audit:** Comprehensive review of log completeness, retention compliance, and access controls
- **Incident Investigation:** Detailed log analysis during security incident investigations to determine root cause, scope of impact, and remediation requirements

10. Integration with Incident Response

Log management is closely integrated with vStream's Incident Response Plan:

- **Incident Detection:** Security event logs trigger automated incident detection and alerting
- **Forensic Analysis:** Comprehensive log analysis supports investigation of P1, P2, and P3 incidents
- **Evidence Preservation:** Relevant logs preserved as evidence during incident response, with chain of custody documentation

- **Timeline Reconstruction:** Audit logs enable reconstruction of event timelines for incident investigation
- **Regulatory Reporting:** Logs provide evidence for GDPR breach notifications and regulatory compliance reporting

11. Roles and Responsibilities

11.1 Chief Technology Officer

- Weekly review of Security Command Centre findings and critical security logs
- Approval of log retention policies and monitoring procedures
- Investigation of security incidents using log data
- Coordination with regulatory authorities for log-based evidence

11.2 Backend Developers

- Implementation of application logging in ShineVR and supporting services
- Configuration of Google Cloud Logging and monitoring
- Response to security alerts and investigation of anomalies
- Remediation of security findings identified through log analysis

11.3 All Employees

- Awareness that actions are logged and subject to monitoring
- Cooperation with log-based investigations
- Prohibition on tampering with, disabling, or circumventing logging mechanisms

12. Privacy Considerations

Log data may contain personal information and must be handled in compliance with GDPR:

- **Lawful Basis:** Logging is necessary for legitimate interests (security, fraud prevention, regulatory compliance) and contractual obligations
- **Data Minimisation:** Logs contain only information necessary for security monitoring and operational purposes
- **Access Restrictions:** Log access limited to authorised personnel with legitimate business need
- **Transparency:** Employees informed that their actions are logged and monitored
- **Retention Limits:** Logs automatically deleted after retention period expires unless required for ongoing investigation

13. Related Policies and Documents

- Information Security Policy
- Incident Response Plan
- Access Management Policy
- Cloud Security Policy
- Change Control Policy
- Media Retention and Disposal Policy

14. 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