Cloud Security Policy

vStream Digital Media / ShineVR

Last updated 02/06/2025

Definitions

Term	Definition
Company	means vStream Digital Media
ShineVR	means the ShineVR product developed and operated by vStream Digital Media
GDPR	means the General Data Protection Regulation
Responsible Person	means Andrés Pitt, CTO
Cloud Infrastructure	Computing infrastructure, platforms, and services hosted by cloud service providers
GCP	Google Cloud Platform - the Company's primary cloud infrastructure provider
Cloud Run	Google Cloud's serverless container platform used for hosting ShineVR applications
IAM	Identity and Access Management - Google Cloud's access control system
Container	Docker containerised application package including code, runtime, and dependencies
Production Environment	Live systems serving actual customers and processing real data

Term	Definition
Staging Environment	Pre-production testing environment mirroring production configuration
Development Environment	Environment for active software development and unit testing

1. POLICY STATEMENT

vStream Digital Media has adopted a cloud-first infrastructure strategy, with all Company and ShineVR systems hosted on Google Cloud Platform. This Cloud Security Policy establishes mandatory security requirements, configuration standards, and operational practices to ensure the confidentiality, integrity, and availability of all cloud-hosted systems and data.

The Company leverages Google Cloud's robust security infrastructure whilst implementing additional controls specific to our business requirements and regulatory obligations. All cloud operations must comply with this policy to maintain a secure, compliant, and resilient cloud environment.

2. PURPOSE

The purpose of this policy is to:

- Define security requirements for all cloud infrastructure and services
- Establish configuration standards for Google Cloud Platform resources
- Ensure compliance with GDPR, ISO 27001, and other regulatory requirements
- Protect Company and ShineVR data hosted in cloud environments
- Define access control and identity management requirements
- Establish monitoring, logging, and incident detection practices
- Ensure business continuity and disaster recovery capabilities
- Provide clear responsibilities for cloud security management

3. SCOPE

This policy applies to:

- All Google Cloud Platform infrastructure, services, and resources used by the Company
- All ShineVR application components hosted on Google Cloud
- All cloud-hosted data including databases, storage, and backups
- All employees, contractors, and third parties with access to Company cloud infrastructure

- Development, staging, and production environments

Geographic Scope:

- Primary regions: europe-west4-a (Eemshaven, Netherlands) and europe-west1-b (St. Ghislain, Belgium)
- All data processing and storage occurs within European Union data centres
- No data processing occurs outside the European Economic Area (EEA)

4. CLOUD SERVICE PROVIDER SELECTION

4.1 Primary Cloud Provider

Google Cloud Platform is the Company's chosen cloud infrastructure provider based on:

- Comprehensive security certifications and compliance programmes
- European data centre locations ensuring GDPR compliance
- Advanced security features including encryption, IAM, and monitoring
- Robust infrastructure reliability and availability
- Integration with Google Workspace (Company's productivity suite)
- Container-native platform (Cloud Run) aligned with Company's architecture

4.2 Provider Security Certifications

Google Cloud Platform maintains certifications including:

- **ISO 27001** (Information Security Management)
- **ISO 27017** (Cloud Security)
- **ISO 27018** (Cloud Privacy)
- **SOC 1, SOC 2, SOC 3** (Service Organization Controls)
- **PCI DSS** (Payment Card Industry Data Security Standard)
- **HIPAA** (Health Insurance Portability and Accountability Act)
- **CSA STAR** (Cloud Security Alliance Security, Trust, Assurance and Risk)

These certifications are verified annually through Google Cloud's compliance documentation.

4.3 Service Level Agreements (SLAs)

Google Cloud Platform provides SLAs for services including:

- **Cloud Run:** 99.95% monthly uptime percentage
- **Cloud SQL:** 99.95% monthly uptime percentage (regional instances)
- **Cloud Storage:** 99.95% monthly uptime percentage

- **Network:** 99.99% network uptime

Company relies on these SLAs for baseline availability commitments, with additional application-layer resilience measures implemented.

4.4 Data Residency Requirements

Mandatory Requirement: All Company and ShineVR data must remain within the European Economic Area (EEA)

Implementation:

- Resources provisioned only in europe-west4 (Netherlands) and europe-west1 (Belgium) regions
- Google Cloud IAM policies prevent resource creation in non-European regions
- Data residency verified through Google Cloud asset inventory
- Cross-region data transfer prohibited unless both regions are within EEA

5. CLOUD ARCHITECTURE AND INFRASTRUCTURE

5.1 Infrastructure-as-Code Approach

Principle: All cloud infrastructure is defined, version-controlled, and deployed using Infrastructure-as-Code

Implementation:

- Cloud infrastructure defined using declarative configuration
- All infrastructure changes tracked in version control (Git)
- Infrastructure changes require code review and approval
- Changes deployed through automated CI/CD pipelines
- Manual console changes prohibited for production infrastructure (except emergency incident response)

5.2 Container-Based Architecture

Architecture: ShineVR applications are containerised using Docker and deployed on Google Cloud Run

Security Benefits:

- Immutable infrastructure (containers rebuilt rather than patched)
- Consistent environments across development, staging, and production

- Automated vulnerability scanning of container images
- Rapid deployment and rollback capabilities
- Isolation between application components

Container Security Requirements:

- Base images from official, trusted sources only
- Base images updated regularly with security patches
- No secrets or credentials embedded in container images
- Container images scanned for vulnerabilities before deployment
- Failed vulnerability scans block deployment to production

5.3 Environment Separation

Mandatory Requirement: Development, staging, and production environments must be completely separated

Implementation:

- **Separate Google Cloud projects** for development, staging, and production
- **Separate databases** with different credentials for each environment
- **Separate IAM policies** controlling access to each environment
- **No cross-environment access** (developers cannot access production data)
- **Different encryption keys** for each environment
- **Separate network configurations** for isolation

Access Restrictions:

- Developers have full access to development environment
- Product Manager and CTO have access to staging environment
- CTO and designated production staff only have access to production environment
- All access logged and monitored

5.4 Network Security

Architecture: ShineVR applications deployed on Google Cloud Run with managed networking

Security Controls:

- **TLS encryption mandatory** for all external connections (HTTPS only, HTTP disabled)
- **Private networking** between internal services where possible
- **Cloud Load Balancing** with DDoS protection for public-facing services
- **Cloud Armor** (web application firewall) for additional protection
- **VPC (Virtual Private Cloud)** for network isolation

- **Firewall rules** limiting ingress/egress to required ports and protocols only

5.5 Data Storage Architecture

Databases:

- **Cloud SQL** (managed PostgreSQL/MySQL) for structured data
- Automatic backups with point-in-time recovery
- Encryption at rest using Google-managed keys
- Encrypted connections (SSL/TLS) required for all database access
- Private IP addresses (not publicly accessible)

Object Storage:

- **Cloud Storage** buckets for file storage
- Separate buckets for different data classifications
- Versioning enabled for critical data
- Lifecycle policies for automated data retention management
- Encryption at rest using Google-managed or customer-managed keys

Backup Storage:

- Automated backups to separate Google Cloud Storage buckets
- Geo-redundant backup storage within Europe
- Backups encrypted at rest
- Retention period: 6 months for non-mission-critical data
- Backup restoration tested monthly

6. ACCESS CONTROL AND IDENTITY MANAGEMENT

6.1 Identity and Access Management (IAM) Principles

Principle of Least Privilege (POLP):

- Users granted minimum permissions necessary for their role
- Service accounts granted minimum permissions necessary for their function
- Regular review and recertification of access rights
- Unused permissions revoked proactively

Separation of Duties:

- No single person has unrestricted access to all systems
- Critical operations require multiple approvals

- Developers separated from production environment access
- Financial and technical controls separated

6.2 User Authentication

Mandatory Requirements:

- All user access to Google Cloud Platform requires Google Workspace account
- **Multi-Factor Authentication (MFA) mandatory** for all users accessing GCP
- MFA methods: Google Authenticator, hardware security keys, or Google prompts
- Password requirements: Minimum 12 characters, changed every 90 days, no reuse of last 5
- Account lockout after 5 failed authentication attempts
- Session timeouts enforced (maximum 12 hours, shorter for privileged access)

6.3 Service Account Management

Service Accounts: Applications and services use service accounts (not user accounts) for API access

Security Requirements:

- Service accounts created with descriptive names indicating purpose
- Service accounts granted minimum required permissions
- Service account keys rotated annually
- Service account keys never committed to source code repositories
- Service account keys stored in Google Secret Manager
- Service account activity logged and monitored
- Unused service accounts disabled or deleted

6.4 Role-Based Access Control (RBAC)

Standard Roles Defined:

Role	Description	Access Level	Examples
SuperAdmin	Full administrative access	All projects and resources	CTO
Admin	Project administration	Specific projects	Backend Team Lead
Manager	Read/write access to specific resources	Limited resources	Product Manager

Role	Description	Access Level	Examples
User	Read-only or limited write access	Specific resources only	Developers (to dev environment)

Role Assignments:

- Roles assigned based on job function and business need
- Temporary elevated access granted for specific tasks, then revoked
- Role assignments documented and reviewed quarterly
- Changes to role assignments logged in audit trail

6.5 Access Reviews and Re-Certification

Quarterly Access Review:

- CTO reviews all IAM policies and role assignments
- Unused or excessive permissions identified and removed
- Service accounts validated for continued business need
- Role changes due to staff movements incorporated

Immediate Access Review Triggers:

- Employee role change
- Employee departure
- Security incident
- New regulatory requirement
- Significant system change

6.6 Third-Party Access

General Prohibition: Third parties do not have direct access to production environments

Exceptions:

- Google Cloud support personnel (accessed via Google support ticket system)
- External security auditors (time-limited, supervised access for audit purposes)
- Emergency incident response consultants (approved by CTO, time-limited)

All third-party access:

- Requires written approval from CTO
- Limited to minimum necessary scope

- Time-limited (typically 24-48 hours, maximum 7 days)
- Fully logged and monitored
- Reviewed and deactivated immediately after purpose completed

7. DATA PROTECTION AND ENCRYPTION

7.1 Encryption at Rest

Mandatory Requirement: All data stored in Google Cloud must be encrypted at rest

Implementation:

- Google Cloud automatically encrypts all data at rest using AES-256
- Encryption is default and cannot be disabled
- Company uses Google-managed encryption keys (GMEK) for base infrastructure
- Customer-managed encryption keys (CMEK) via Google Cloud KMS available for additional control if needed

Data Types Encrypted:

- Cloud SQL databases (all data, backups, and replicas)
- Cloud Storage buckets (all objects and metadata)
- Persistent disks attached to virtual machines or containers
- Backups and snapshots

7.2 Encryption in Transit

Mandatory Requirement: All data transmitted must be encrypted in transit

Implementation:

- **External traffic:** TLS 1.2+ for all HTTPS connections to ShineVR applications
- **Internal traffic:** Google Cloud automatically encrypts traffic between services
- **Database connections:** SSL/TLS required for all Cloud SQL connections
- **API calls:** All Google Cloud API calls use HTTPS

Certificate Management:

- TLS certificates managed by Google Cloud Load Balancer
- Automatic certificate renewal via managed certificates
- Certificate expiry monitoring and alerting

7.3 Key Management

Google Cloud Key Management Service (KMS):

- Centralised key management for all encryption operations
- Keys stored in hardware security modules (HSMs) in European data centres
- Automatic key rotation for certain key types
- Key usage audited and logged
- Key access controlled via IAM permissions

Key Access Control:

- Only authorised service accounts can access encryption keys
- Key access permissions reviewed quarterly
- Key usage anomalies trigger security alerts
- Keys never exported or stored outside Google Cloud KMS

7.4 Data Classification and Protection

Data Classifications:

Classification	Description	Examples	Protection Requirements
Sensitive Personal Data	PII, health data	Patient pain scores (if PII linked), employee personal data	AES-256 encryption, access logging, restricted IAM, GDPR compliance
Confidential	Proprietary business information	Source code, business plans, customer contracts	AES-256 encryption, restricted IAM, need-to-know access
Internal	General business data	Internal emails, project documentation	AES-256 encryption, authenticated access required
Public	Information intended for public consumption	Marketing materials, public website content	AES-256 encryption, widely accessible

ShineVR Specific:

- For Health Service Organisations: User data anonymised via 16-digit codes (ShineVR cannot link to PII)
- Pain scores and interaction data encrypted at rest and in transit
- Health Service Organisations maintains PII linkage (as Data Controller)

8. MONITORING, LOGGING, AND ALERTING

8.1 Google Cloud Security Command Centre

Mandatory Requirement: Google Cloud Security Command Centre monitored continuously

Implementation:

- Security Command Centre Premium tier enabled
- Daily automated compliance scanning against 19 compliance standards
- Weekly manual review by CTO
- Security findings triaged and remediated based on severity
- Compliance reports generated monthly

Compliance Standards Monitored

- CIS Controls 8.0
- CIS Google Cloud Platform Foundation 2.0
- ISO 27001 2022
- NIST 800-53 R5
- PCI DSS 3.2.1
- HIPAA
- SOC2 2017
- OWASP 2017 and 2021
- Plus 10 additional standards

8.2 Logging and Audit Trails

Mandatory Logging:

- **Cloud Audit Logs:** All administrative actions and data access logged
- **Application logs:** ShineVR applications generate structured logs
- **Database query logs:** All database queries logged (configurable detail level)
- **Authentication logs:** All login attempts, MFA events, and access denials logged
- **Network logs:** Flow logs for network traffic analysis
- **Security logs:** Firewall denials, security policy violations

Log Retention:

- Audit logs: Minimum 1 year, extended to 7 years for compliance-critical logs
- Application logs: 90 days in Cloud Logging, archived to Cloud Storage for 1 year
- Security logs: 1 year minimum
- Database logs: 30 days online, archived for 1 year

Log Access Control:

- Logs accessible only to authorised personnel (CTO, security team)
- Log access itself logged (audit trail of log access)
- Logs protected from modification or deletion (write-once)

8.3 Alerting and Notifications

Critical Alerts (Immediate Notification):

- Unauthorised access attempts or IAM policy changes
- Security Command Centre critical findings
- Data exfiltration or unusual data transfer patterns
- Service outages or availability degradation
- Encryption key access anomalies
- Malware or vulnerability detections

Alert Channels:

- **Primary:** Slack dedicated security channel with @channel mentions
- **Secondary:** Email to CTO and relevant team members
- **Tertiary:** SMS for P1 critical incidents

Alert Response:

- P1 alerts: Immediate investigation (within 15 minutes)
- P2 alerts: Investigation within 2 hours
- P3 alerts: Investigation within 24 hours
- All alerts logged in incident tracking system
- False positives tuned out to reduce alert fatigue

8.4 Security Monitoring Tools

Automated Monitoring:

- **Google Cloud Security Command Centre:** Continuous security posture monitoring
- **Cloud Monitoring:** Performance and availability monitoring
- **Uptime Checks:** External availability monitoring for ShineVR applications

- **Anomaly Detection:** Machine learning-based detection of unusual patterns
- **Vulnerability Scanning:** Container image and dependency scanning

Manual Monitoring:

- **Weekly CTO Review:** Google Cloud Security Command Centre findings
- **Monthly Security Review:** Comprehensive security posture assessment
- **Quarterly Access Review:** IAM policies and permissions audit
- **Annual Policy Review:** Complete security policy and compliance review

9. VULNERABILITY MANAGEMENT

9.1 Container Vulnerability Scanning

Mandatory Requirement: All Docker container images must be scanned for vulnerabilities before deployment

Implementation:

- Automated vulnerability scanning integrated into CI/CD pipeline
- Container Registry Vulnerability Scanning enabled
- Binary Authorization blocks deployment of images with critical vulnerabilities
- Vulnerability scan results reviewed before production deployment
- Known vulnerabilities must be remediated before deployment proceeds

Scanning Frequency:

- On every container image build
- Daily rescanning of existing images for newly discovered vulnerabilities
- Immediate scanning when new critical vulnerabilities announced

9.2 Dependency Vulnerability Management

Application Dependencies:

- Automated scanning of application dependencies (npm, pip, etc.)
- Dependency updates prioritised based on vulnerability severity
- Critical vulnerabilities patched within 7 days
- High vulnerabilities patched within 30 days
- Automated dependency update pull requests reviewed and merged

Base Image Updates:

- Docker base images (Alpine Linux, etc.) updated monthly
- Critical security updates applied immediately
- Base image updates trigger rebuilding and redeployment of all containers

9.3 Infrastructure Vulnerability Management

Google Cloud Platform:

- Google responsible for infrastructure and platform-level security
- Google applies security patches automatically to managed services
- Company monitors Google Cloud security bulletins for customer action items

Application Layer:

- Application code vulnerabilities identified through code review
- Security testing integrated into development process (400+ automated tests)
- Penetration testing conducted annually by external specialists (recommended)

9.4 Patch Management Process

Patching Strategy:

- **Infrastructure:** Rely on Google Cloud's automated patching for managed services
- **Containers:** Rebuild and redeploy containers with updated base images and dependencies
- **Applications:** Deploy application updates through standard CI/CD pipeline

Patching Timelines:

- **Critical vulnerabilities:** Patched within 7 days
- **High vulnerabilities:** Patched within 30 days
- **Medium vulnerabilities:** Patched within 90 days
- **Low vulnerabilities:** Addressed in regular development cycle

Emergency Patching:

- Zero-day vulnerabilities or active exploits patched immediately
- Emergency change control process for urgent patches
- Rollback plan prepared before applying emergency patches

10. CONTAINER SECURITY

10.1 Docker Container Best Practices

Mandatory Requirements:

- **Official base images only:** Use official images from Docker Hub or Google Container Registry
- **Minimal base images:** Use Alpine Linux or distroless images to reduce attack surface
- **No secrets in images:** Never embed credentials, API keys, or secrets in container images
- **Non-root users:** Containers must run as non-root users where possible
- **Read-only file systems:** Container file systems set to read-only where possible
- **Resource limits:** Memory and CPU limits set for all containers
- **Health checks:** Containers must implement health check endpoints

10.2 Container Image Management

Image Repository:

- **Google Container Registry** or **Artifact Registry** used for image storage
- Private registry (not publicly accessible)
- Vulnerability scanning enabled for all images
- Image signing and verification implemented
- Automated cleanup of old images

Image Tagging:

- Semantic versioning for all images (e.g., v1.2.3)
- Git commit SHA included in image tags for traceability
- "Latest" tag used only for development, never production

10.3 Container Runtime Security

Cloud Run Security:

- Containers run in Google-managed, hardened sandbox environment
- Automatic scaling based on load
- Container instances ephemeral (no persistent state in containers)
- Network ingress restricted to HTTPS only
- Egress to allowed destinations only (if network policy configured)

Runtime Monitoring:

- Container behaviour monitored for anomalies
- Resource usage monitored and alerted
- Container crashes and errors logged and investigated
- Security Command Centre monitors container security posture

10.4 Container Build Pipeline Security

CI/CD Security:

- All code changes require pull request and code review
- Automated testing (400+ tests) includes security tests
- Vulnerability scanning occurs before container image creation
- Failed tests or vulnerability scans block deployment
- Deployment to production requires CTO or Product Manager approval
- Full audit trail of all deployments maintained

11. INFRASTRUCTURE SECURITY

11.1 Compute Security (Cloud Run)

Migration from VMs to Cloud Run (2025):

- Eliminated OS-level security concerns by moving to serverless containers
- Google manages underlying infrastructure security
- Automatic security patching by Google
- Reduced attack surface significantly

Cloud Run Security Features:

- **Automatic scaling:** Scales to zero when not in use (reduced exposure)
- **Immutable deployments:** Each deployment is a new container instance
- **Isolation:** Containers run in isolated sandboxes
- **Managed HTTPS:** Automatic TLS certificate management
- **IAM integration:** Fine-grained access control for services

11.2 Network Security

Virtual Private Cloud (VPC):

- Dedicated VPC for production environment
- Subnet segmentation for different service tiers

- Private Google Access enabled for accessing Google services without public IPs
- VPC Flow Logs enabled for network traffic analysis

Firewall Rules:

- Default deny all traffic
- Explicit allow rules only for required traffic
- Firewall rules reviewed quarterly
- Changes to firewall rules require CTO approval

DDoS Protection:

- Google Cloud Load Balancer provides built-in DDoS protection
- Google Cloud Armor for additional web application firewall protection
- Rate limiting configured for API endpoints

11.3 Database Security (Cloud SQL)

Access Control:

- **Private IP only** (no public IP addresses for production databases)
- **IAM database authentication** where supported
- **SSL/TLS required** for all database connections
- **IP whitelisting** for any external access (rare, emergency only)

Configuration Security:

- Automated backups enabled (daily, retained per retention policy)
- Point-in-time recovery enabled
- Binary logging enabled for audit purposes
- Database flags configured according to security best practices
- High availability configuration for production (automatic failover)

Database Auditing:

- All database connections logged
- Slow query logs monitored for potential issues
- Failed authentication attempts alerted
- Database schema changes logged and reviewed

11.4 Serverless Security

Cloud Functions (if used):

- Functions use least privilege service accounts
- Functions deployed with maximum timeout limits
- Functions have memory and execution limits
- Function invocation logged
- Unused functions deleted

Security Best Practices:

- Minimal dependencies in function code
- Regular dependency updates
- Environment variables for configuration (not hardcoded)
- Secrets stored in Secret Manager, not environment variables

12. DATA BACKUP AND RECOVERY

12.1 Backup Strategy

Automated Backups:

- **Cloud SQL databases:** Daily automated backups with 7-day retention for transaction logs
- **Cloud Storage:** Versioning enabled, previous versions retained
- **Whole-of-database backups:** Retained for 6 months for non-mission-critical data
- **Backup location:** europe-west1 (Belgium) for production data stored in europe-west4 (Netherlands) and vice versa

Backup Encryption:

- All backups encrypted using AES-256
- Same encryption as primary data
- Backup encryption keys managed via Google Cloud KMS

12.2 Recovery Objectives

Application Layer (ShineVR):

- **Recovery Time Objective (RTO):** 8 hours during business hours
- **Recovery Point Objective (RPO):** 24 hours (maximum acceptable data loss)

Infrastructure Layer:

- Refer to Google Cloud SLAs for compute, network, and storage layers
- Google Cloud maintains 99.95%+ availability SLAs

12.3 Backup Testing

Regular Testing:

- Backup restoration tested monthly
- Full disaster recovery simulation conducted annually
- Test results documented and reviewed
- Issues identified during testing remediated promptly

Continuous Testing:

- "Release early, release often" practice means frequent builds and deployments
- Deployment process inherently tests recovery procedures
- Infrastructure-as-Code approach means infrastructure can be rebuilt rapidly

12.4 Business Continuity and Disaster Recovery

Disaster Recovery Plan:

- Every system component has documented recovery procedure
- Support documents maintained for all recovery scenarios
- Documents updated as part of system development lifecycle
- Regular drills to validate procedures

Continuity Measures:

- Multi-zone deployment within regions for high availability
- Cross-region backup storage for disaster recovery
- Infrastructure-as-Code enables rapid rebuild in different region if necessary
- Data and configuration backed up separately from infrastructure

13. COMPLIANCE AND GOVERNANCE

13.1 Regulatory Compliance

GDPR Compliance:

- All data processing within European Union
- Data Protection Impact Assessments (DPIA) conducted for high-risk processing
- Data Processing Agreements with Google Cloud in place
- Data subject rights (access, rectification, erasure) supported by technical architecture
- Breach notification procedures defined and tested

Industry Standards:

- ISO 27001 information security practices implemented
- Regular review against ISO 27001 controls
- Documentation of compliance with NIST frameworks
- Compliance monitoring via Google Cloud Security Command Centre

13.2 Google Cloud Compliance Posture

Leveraging Google's Certifications:

- Company benefits from Google Cloud's extensive compliance certifications
- Google provides compliance reports and attestations
- Company reviews Google's compliance status quarterly
- Any changes to Google's compliance status trigger Company review

Shared Responsibility Model:

- Google responsible for security "of" the cloud (infrastructure, platform)
- Company responsible for security "in" the cloud (applications, data, access control)
- Clear delineation of responsibilities documented
- Regular review of responsibility boundaries

13.3 Audit and Assessment

Internal Audits:

- Quarterly access review
- Monthly security posture assessment
- Weekly Security Command Centre review
- Daily automated compliance scanning

External Audits:

- Annual security assessment (recommended)
- Regulatory audits as required
- Customer audits supported (questionnaires, on-site visits if needed)
- Audit findings tracked and remediated

Audit Trail Maintenance:

- All audits documented with findings and remediation plans
- Audit documentation retained for minimum 7 years

- Audit results reported to senior management
- Trends and patterns analysed for continuous improvement

13.4 Policy Compliance Monitoring

Automated Compliance:

- Google Cloud Security Command Centre provides automated policy compliance monitoring
- Infrastructure-as-Code ensures configuration compliance
- Policy violations detected automatically
- Non-compliant resources flagged for remediation

Manual Compliance Reviews:

- CTO reviews compliance status weekly
- Quarterly comprehensive policy compliance review
- Annual policy review and update
- Policy violations investigated and remediated

14. THIRD-PARTY CLOUD SERVICES

14.1 Approved Third-Party Services

Current Approved Services:

- **Google Cloud Platform** (primary infrastructure provider)
- **Google Workspace** (email, productivity, collaboration)
- **GitHub/GitLab** (source code repository, CI/CD) - if used
- **Slack** (team communication)

Approval Process for New Services:

- Security assessment required before adoption
- Privacy and data protection review
- Contractual review (Data Processing Agreement, Terms of Service)
- CTO approval required
- Risk assessment documented

14.2 Third-Party Service Security Requirements

Any third-party cloud service must:

- Provide appropriate security certifications (SOC 2, ISO 27001, etc.)
- Offer data residency control (EU data centres)
- Provide encryption at rest and in transit
- Offer adequate access control and authentication
- Provide audit logs and monitoring capabilities
- Have acceptable SLAs for availability and support
- Support GDPR compliance requirements

14.3 Third-Party Service Monitoring

Ongoing Monitoring:

- Security posture reviewed annually
- Service availability monitored continuously
- Compliance status checked quarterly
- Vendor security incidents monitored via industry news
- Contract renewal triggers comprehensive review

Vendor Management:

- List of approved vendors maintained by CTO
- Vendor risk assessments documented
- Vendor contacts and escalation procedures documented
- Vendor incident notification procedures defined

15. INCIDENT RESPONSE IN CLOUD ENVIRONMENTS

15.1 Cloud-Specific Incident Types

Google Cloud Platform Incidents:

- GCP service outages or degradation
- GCP security vulnerabilities
- Unauthorised access to GCP console or resources
- IAM policy violations or misconfigurations
- Encryption key compromise
- Container vulnerability exploits
- DDoS attacks

Detection Methods:

- Google Cloud Security Command Centre alerts
- Google Cloud Monitoring alerts

- Anomaly detection in Cloud Logging
- User reports of service issues
- Google Cloud status dashboard
- Security research community disclosures

15.2 Cloud Incident Response Procedures

Refer to **Incident Response Plan** for detailed procedures. Cloud-specific considerations:

Immediate Actions:

- Review Google Cloud Status Dashboard for platform-wide issues
- Review Security Command Centre for security-specific alerts
- Isolate affected Cloud Run services or database instances if necessary
- Review Cloud Audit Logs for unauthorised actions
- Engage Google Cloud Support (priority based on incident severity)

Containment:

- Revoke compromised IAM credentials immediately
- Update firewall rules to block attack sources
- Deploy updated container images with security fixes
- Rotate encryption keys if compromise suspected
- Implement additional monitoring for affected resources

Recovery:

- Restore from backups if data compromised
- Rebuild affected infrastructure using Infrastructure-as-Code
- Re-deploy containers with security fixes
- Validate security posture before restoring service
- Enhanced monitoring for 7 days post-incident

15.3 Google Cloud Support Engagement

Support Tiers:

- **Critical (P1):** Production system down, data loss, security breach
- **High (P2):** System degradation, security vulnerability
- **Normal (P3):** General questions, non-critical issues

Engagement Process:

- Open support case via Google Cloud Console

- Provide detailed incident description and impact
- Escalate if response time inadequate
- Document all interactions with Google support
- Include support interactions in incident report

16. SECURE SOFTWARE DEVELOPMENT LIFECYCLE (SDLC)

16.1 Development Environment Security

Separation from Production:

- Development environment in separate Google Cloud project
- No access to production data from development environment
- Synthetic or anonymised test data only in development
- Separate encryption keys for development environment

Development Practices:

- Security testing integrated into development process
- Code review required before merging to main branch
- Static application security testing (SAST) in CI/CD pipeline
- Dependency vulnerability scanning before deployment

16.2 Continuous Integration / Continuous Deployment (CI/CD)

Pipeline Security:

- Source code stored in private repositories
- CI/CD pipelines triggered by code commits
- Automated testing (400+ tests including security tests)
- Container image vulnerability scanning
- Build artifacts signed and verified
- Deployment requires approval for production

Deployment Process:

- Code review and approval required
- Automated tests must pass
- Vulnerability scans must be clean (no critical/high vulnerabilities)
- Staging deployment and testing before production
- Production deployment requires CTO or Product Manager approval

- Rollback plan prepared for all deployments
- Full audit trail of deployments maintained

16.3 Security Testing

Automated Testing (400+ tests):

- Unit tests for application logic
- Integration tests for service interactions
- **Security tests:**
    - Authentication and authorisation tests (role-based access)
    - Input validation tests
    - SQL injection prevention tests
    - Cross-site scripting (XSS) prevention tests
    - API security tests
- Performance and load tests

Manual Security Testing:

- Code review by senior developer or CTO
- Penetration testing (annually recommended)
- Security architecture review for major changes

17. COST MANAGEMENT AND OPTIMISATION

17.1 Cost Monitoring

Budget Alerts:

- Monthly budget set for Google Cloud spending
- Alerts at 50%, 75%, 90%, and 100% of budget
- Unexpected cost increases investigated promptly
- Cost anomalies may indicate security issues (e.g., cryptomining)

Cost Optimisation:

- Right-sizing of resources based on actual usage
- Automatic scaling to match demand
- Cleanup of unused resources
- Use of committed use discounts where appropriate
- Storage lifecycle policies to move data to cheaper tiers

17.2 Resource Tagging and Management

Tagging Strategy:

- All resources tagged with: environment, project, owner, cost-centre
- Tags enable cost allocation and resource tracking
- Untagged resources identified and tagged or deleted
- Tag compliance monitored monthly

18. ROLES AND RESPONSIBILITIES

Role	Responsibilities
CTO (Responsible Person)	Overall cloud security ownership; Google Cloud administration; IAM policy management; security monitoring; incident response; policy compliance; vendor relationship with Google; approve major changes; weekly Security Command Centre review
Backend Developers	Secure application development; container security; code review; security testing; development environment security; report security issues; follow SDLC security practices
Product Manager	Review and approve staging deployments; review security impact of features; balance security with functionality; customer security requirements
DevOps/Infrastructure (if dedicated role)	Infrastructure-as-Code development; CI/CD pipeline management; monitoring configuration; backup management; coordinate with Google Cloud support
All Employees	Report security incidents; follow access control policies; protect credentials; complete security training

19. TRAINING AND AWARENESS

19.1 Cloud Security Training

Required Training:

- **New employees:** Cloud security awareness training during onboarding
- **Developers:** Secure coding and container security training
- **Cloud administrators:** Google Cloud security best practices training
- **All staff:** Annual security awareness refresher including cloud security topics

Training Topics:

- Google Cloud Platform security features
- IAM and access control principles
- Container and application security
- Secure SDLC practices
- Incident reporting procedures
- Data protection and encryption
- Compliance requirements

19.2 Security Resources

Available Resources:

- Google Cloud security documentation
- Internal security policies and procedures
- Security best practice guides
- Contact information for security support
- Incident reporting procedures

20. CONTINUOUS IMPROVEMENT

20.1 Security Metrics

Tracked Metrics:

- Number of security incidents
- Mean time to detect (MTTD)
- Mean time to respond (MTTR)
- Compliance posture (% passing across frameworks)
- Vulnerability remediation time

- Backup success rate
- Security test coverage

Reporting:

- Weekly metrics reviewed by CTO
- Monthly security dashboard for senior management
- Quarterly trend analysis
- Annual comprehensive security review

20.2 Lessons Learned

Post-Incident Reviews:

- Lessons learned documented after each incident
- Policy and procedure updates implemented
- Security controls enhanced based on incidents
- Training updated to address gaps
- Success stories shared to reinforce good practices

20.3 Security Roadmap

Ongoing Improvements:

- Regular assessment of new Google Cloud security features
- Evaluation of emerging security threats
- Technology refresh and modernisation
- Security automation enhancements
- Compliance framework expansion

21. POLICY REVIEW AND UPDATES

21.1 Review Schedule

This policy will be reviewed:

- **Annually:** Comprehensive review by CTO
- **After major incidents:** Update based on lessons learned
- **After infrastructure changes:** New services, major architecture changes
- **Regulatory changes:** Updates to GDPR, ISO 27001, or other compliance requirements
- **Google Cloud changes:** Major platform updates affecting security

21.2 Version Control

- Current version maintained in Google Drive
- Previous versions archived for reference
- All changes documented with rationale
- Change log maintained
- Stakeholders notified of policy updates

22. EXCEPTIONS

22.1 Exception Process

Exceptions to this policy may be requested for:

- Emergency incident response requiring policy deviation
- Temporary operational requirements
- Technical limitations preventing policy compliance
- Cost constraints requiring alternative controls

All exceptions must:

- Be requested in writing to CTO
- Include detailed justification
- Document compensating controls
- Be approved in writing by CTO
- Be time-limited (reviewed at least quarterly)
- Be documented in exception register

23. RELATED POLICIES

This policy should be read in conjunction with:

- Information Security Policy
- Encryption Policy
- Password Policy
- Access Management Process/Procedure
- Backup Policy
- Incident Response Plan
- Change Control Policy
- Data Protection Policy

24. CONTACT INFORMATION

For questions regarding this policy or to report cloud security incidents:

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

Google Cloud Support: Access via Google Cloud Console Select appropriate priority based on incident severity