# Network Security Policy

**vStream Digital Media**

**Last updated 03/02/25**

## 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 |
| **VPC** | Virtual Private Cloud - isolated network environment within Google Cloud Platform |
| **Firewall** | Network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules |
| **TLS** | Transport Layer Security - cryptographic protocol for secure communications over networks |
| **DDoS** | Distributed Denial of Service - cyberattack attempting to disrupt normal traffic by overwhelming target with flood of internet traffic |
| **IDS/IPS** | Intrusion Detection System / Intrusion Prevention System - security technologies that monitor network traffic for malicious activity |
| **Network Segmentation** | Practice of dividing a network into multiple segments or subnets to improve security and performance |

| Term | Definition |
|---|---|
| **Private IP** | IP address used for internal network communication, not directly accessible from public internet |

# 1. POLICY STATEMENT

vStream Digital Media operates a cloud-native infrastructure with all systems hosted on Google Cloud Platform. This Network Security Policy establishes requirements and controls to protect the confidentiality, integrity, and availability of data transmitted across networks used by the Company and ShineVR applications.

The Company leverages Google Cloud Platform's robust network security capabilities whilst implementing additional controls specific to our business requirements. All network communications are encrypted, monitored, and controlled through defence-in-depth security measures.

**Critical Context:** vStream operates a cloud-first model with **no customer or production data hosted at Company premises**. All network security for production systems is managed through Google Cloud Platform infrastructure in European data centres.

# 2. PURPOSE

The purpose of this policy is to:

- Define network security requirements for Company and ShineVR systems
- Protect data confidentiality, integrity, and availability during transmission
- Prevent unauthorised network access and data interception
- Ensure secure connectivity for employees, applications, and services
- Establish network segmentation and isolation requirements
- Enable detection and prevention of network-based attacks
- Ensure compliance with GDPR, ISO 27001, and healthcare security requirements
- Document network security controls for audit and compliance purposes

# 3. SCOPE

This policy applies to:

- Google Cloud Platform networks in europe-west4-a (Eemshaven, Netherlands) and europe-west1-b (St. Ghislain, Belgium)
- Company office wireless network at 37 Leeson Close, Dublin 2, Ireland
- Remote access connections to Company systems
- ShineVR application network communications

- Development, staging, and production network environments
- Third-party network connections and integrations
- Employee home networks used for remote work (see BYOD Policy)
- All employees, contractors, and third parties accessing Company networks

# 4. GOOGLE CLOUD NETWORK ARCHITECTURE

## 4.1 Virtual Private Cloud (VPC)

**VPC Configuration:**

- Dedicated VPC for Company infrastructure isolation
- Custom subnet design separating development, staging, and production
- Private IP address ranges for internal communications
- VPC peering disabled except where explicitly required for business purposes
- Regional VPC configuration in europe-west4 and europe-west1

**Network Isolation:**

- Production environment isolated from development and staging networks
- Database networks isolated using private IP addressing only
- No direct internet access to backend services (access via Cloud Load Balancer only)
- Service-to-service communication within VPC using private IPs

## 4.2 Firewall Rules and Access Control

**Firewall Configuration Principles:**

- **Deny by default:** All traffic blocked unless explicitly permitted
- **Least privilege:** Firewall rules grant minimum necessary access
- **Documented rules:** All firewall rules documented with business justification
- **Regular review:** Firewall rules reviewed quarterly, unused rules removed

**Mandatory Firewall Controls:**

- Ingress traffic from internet restricted to:
    - HTTPS (443) for ShineVR application access
    - Specific IP ranges where applicable for administrative access
- Egress traffic restricted to:
    - Required external services and APIs
    - Google Cloud services
    - Software update repositories
- Internal traffic between environments controlled:
    - Production cannot be accessed from development
    - Staging accessible only from authorised development IPs

- SSH access (if required) restricted to:
    - Specific authorised IP addresses only
    - Key-based authentication mandatory (no password authentication)
    - MFA required for administrative access

**Firewall Rule Management:**

- All firewall changes require CTO approval
- Changes documented in change control system
- Emergency firewall changes follow Incident Response Plan procedures
- Firewall configuration stored in Infrastructure-as-Code repository
- Changes tracked in version control with code review

## 4.3 Private IP Addressing

**Database Network Security:**

- Cloud SQL databases accessible only via private IP addresses
- No public IP addresses assigned to database instances
- Database connections require:
    - TLS encryption mandatory
    - Authentication via Cloud SQL Auth Proxy or IAM
    - Network path through VPC only

**Internal Service Communication:**

- Internal services communicate via private IPs within VPC
- No internet exposure for internal APIs or services
- Service-to-service authentication required
- Mutual TLS (mTLS) for sensitive internal communications where appropriate

## 4.4 Network Segmentation

**Environment Segregation:**

- **Production Network:** Isolated network segment for production systems
    - Separate VPC subnet
    - Restricted access from other environments
    - Enhanced monitoring and logging
    - Change control restrictions enforced at network level
- **Staging Network:** Pre-production testing environment
    - Isolated from production network
    - Mirrors production network configuration

    - Accessible from authorised development sources

- **Development Network:** Active development environment

    - Separated from production and staging
    - More permissive access for development activities
    - No production data permitted in development network

**Benefits of Segmentation:**

- Limits blast radius of security incidents
- Prevents lateral movement by attackers
- Separates sensitive production data from development activities
- Enables environment-specific security controls

# 5. CLOUD LOAD BALANCING AND DDOS PROTECTION

## 5.1 Google Cloud Load Balancer

**Load Balancer Configuration:**

- All public-facing ShineVR traffic routed through Cloud Load Balancer
- HTTPS load balancing with automatic TLS certificate management
- Backend services not directly exposed to internet
- Health checks configured to detect and remove unhealthy instances
- Geographic distribution across European regions for resilience

**DDoS Protection:**

- Built-in DDoS protection at Google Cloud's network edge
- Automatic detection and mitigation of volumetric attacks
- Protection against application-layer attacks
- No additional configuration required (inherent to Google Cloud)

## 5.2 Cloud Armor (Web Application Firewall)

**Cloud Armor Implementation:**

- Web Application Firewall protection for ShineVR application
- Protection against OWASP Top 10 vulnerabilities
- Rate limiting to prevent abuse and brute-force attacks
- Geographic restrictions (if required for compliance)
- Custom security rules for application-specific threats

**Security Rules:**

- Automatic blocking of known malicious IP addresses
- SQL injection and cross-site scripting (XSS) protection
- Protection against protocol attacks
- Custom rules for ShineVR-specific security requirements
- Regular review and tuning of security rules

# 6. WIRELESS NETWORK SECURITY

## 6.1 Company Office Wireless Network

**Encryption Requirements:**

- **WPA2 encryption minimum** for all Company wireless networks
- **WPA3 encryption preferred** where supported by devices
- WEP and open wireless networks strictly prohibited
- Strong Pre-Shared Key (PSK) requirements:
    - Minimum 16 characters
    - Complex passphrase (mix of uppercase, lowercase, numbers, special characters)
    - PSK changed every 6 months
    - PSK change after employee termination (if employee had PSK access)

**Network Configuration:**

- Unique SSID (not broadcasting default router SSID)
- Router admin interface accessible only from internal network
- Router admin password changed from default
- Router firmware kept up to date
- WPS (Wi-Fi Protected Setup) disabled

**Access Control:**

- Company wireless network for employees only
- Guest wireless network (if implemented) segregated from corporate network:
    - No access to internal Company resources
    - Internet access only
    - Guest credentials expire after 24 hours
    - Guest network usage logged

**Important Context:**

- Company wireless network primarily for internet access
- **No customer or production data hosted at Company premises**
- All sensitive data access via encrypted cloud connections (HTTPS, TLS)

- Wireless network security important but not critical to data protection
- Production data accessed via Google Cloud Platform with MFA and TLS encryption

### 6.2 Home Network Security (Remote Work)

**Employee Responsibilities:**

- Home Wi-Fi must use WPA2 or WPA3 encryption
- Default router passwords must be changed
- Router firmware kept updated
- Avoid public Wi-Fi for sensitive Company work
- See BYOD Policy for comprehensive home network security requirements

**Company Recommendations:**

- Use separate guest network for IoT devices at home
- Disable remote management on home routers
- Enable router firewall if available
- Consider VPN for public Wi-Fi access (if Company-provided)

## 7. ENCRYPTION IN TRANSIT

### 7.1 TLS Encryption Requirements

**Mandatory TLS Configuration:**

- **TLS 1.2 minimum** for all network connections
- **TLS 1.3 preferred** where supported
- Certificate validation must be enabled
- Self-signed certificates prohibited in production environments
- Strong cipher suites only (no weak or deprecated ciphers)

**Certificate Management:**

- Valid certificates from trusted Certificate Authorities (CAs)
- Automatic certificate renewal via Google Cloud Certificate Manager
- Certificate expiry monitoring and alerting
- Certificates checked during automated testing

### 7.2 ShineVR Application Traffic

**Application-Level Encryption:**

- All ShineVR mobile app to backend communication uses HTTPS with TLS 1.2+
- All API calls encrypted in transit

- WebSocket connections (if used) must use WSS (WebSocket Secure)
- **No sensitive data transmitted over unencrypted HTTP**
- Strict Transport Security (HSTS) headers enforced

**API Security:**

- API endpoints require authentication tokens
- API traffic encrypted with TLS
- API rate limiting to prevent abuse
- API access logged for security monitoring

## 7.3 Google Cloud Internal Traffic

**Automatic Encryption:**

- Traffic between Google Cloud services automatically encrypted by Google
- Includes traffic between:
    - Cloud Run instances
    - Cloud SQL databases
    - Cloud Storage buckets
    - Internal Google Cloud APIs
- Google uses private fiber network with encryption by default
- No additional configuration required from Company

## 7.4 Email Communication Security

**Google Workspace Email Security:**

- Company email enforces TLS for email transmission
- DMARC, DKIM, and SPF configured for email authentication
- Email encryption in transit to external recipients where supported
- Sensitive information shared via encrypted links rather than email attachments (preferred)
- Phishing and malware protection enabled via Google Workspace

## 7.5 Remote Access Encryption

**Secure Remote Access:**

- All remote access to Company systems uses encrypted connections
- Google Cloud Platform access requires HTTPS/TLS encryption
- SSH connections (if used) require encrypted key-based authentication
- MFA mandatory for all remote access (see Access Management Policy)

**VPN (If Implemented):**

- VPN connections (if used) must use strong encryption protocols:
    - IPsec with AES-256 encryption
    - IKEv2 or OpenVPN protocols
    - No PPTP (weak encryption)
- Currently: VPN not required due to cloud-native architecture with built-in encryption

# 8. NETWORK MONITORING AND INTRUSION DETECTION

## 8.1 Google Cloud Security Command Centre

**Continuous Monitoring:**

- Security Command Centre monitors across 19 compliance standards including:
    - ISO 27001
    - CIS Benchmarks
    - HIPAA
    - SOC 2
    - OWASP Top 10
    - PCI DSS
- Weekly review of Security Command Centre findings by CTO
- Automated alerts for high-severity findings
- Integration with incident response procedures

## 8.2 Network-Based Intrusion Detection

**Google Cloud IDS Capabilities:**

- Leverages Google Cloud Platform's built-in network threat detection
- Continuous monitoring for suspicious network activities
- Detection of:
    - Unusual traffic patterns
    - Known attack signatures
    - Port scanning attempts
    - Protocol anomalies
    - Data exfiltration attempts

**Intrusion Prevention:**

- Automatic blocking of known malicious IP addresses
- Cloud Armor rules prevent common network attacks
- Firewall rules block unauthorized access attempts
- Rate limiting prevents brute-force attacks

## 8.3 Network Traffic Logging

**VPC Flow Logs:**

- VPC Flow Logs enabled for network traffic visibility
- Logs capture:
    - Source and destination IP addresses
    - Ports and protocols
    - Traffic volume
    - Accept/reject decisions
- Flow logs retained per Log Management Policy retention periods
- Flow logs analyzed for security anomalies

**Firewall Logs:**

- All firewall rule matches logged
- Blocked connection attempts logged and monitored
- Unusual patterns trigger security alerts
- Regular review of firewall logs for security incidents

## 8.4 Alerting and Response

**Automated Alerting:**

- Real-time alerts for security events:
    - Firewall rule violations
    - Unusual traffic patterns
    - Failed authentication attempts
    - Suspicious network connections
- Alerts sent to CTO and security team via email and Slack
- Critical alerts trigger immediate incident response

**Response Procedures:**

- Network security incidents follow Incident Management Policy
- P1 incidents: 15-minute initial response time
- Automatic isolation capabilities for compromised instances
- Runbooks for common network security incidents

# 9. NETWORK REDUNDANCY AND RESILIENCE

## 9.1 Multi-Region Architecture

**Geographic Distribution:**

- Primary data centre: europe-west4-a (Eemshaven, Netherlands)

- Secondary data centre: europe-west1-b (St. Ghislain, Belgium)
- Multi-region deployment for high availability
- Automatic failover between regions (where configured)

**Google Cloud SLAs:**

- Network uptime guarantees per Google Cloud SLAs
- 99.95%+ availability for Cloud Load Balancing
- 99.95% availability for VPC networking
- 99.99% availability for Cloud SQL (regional configuration)

## 9.2 High Availability Design

**Redundancy Principles:**

- No single points of failure in network architecture
- Multiple availability zones within regions
- Redundant network paths
- Load balancing across multiple instances
- Automatic health checks and failover

**Network Resilience Testing:**

- Quarterly disaster recovery exercises include network failover
- Monthly testing of network redundancy
- Simulated network outage scenarios
- Documentation of network recovery procedures

# 10. REMOTE ACCESS AND VPN

## 10.1 Cloud-Native Remote Access

**No Traditional VPN Required:**

- Cloud-native architecture eliminates need for traditional VPN
- All remote access via Google Workspace accounts with MFA
- Google Cloud Platform access via HTTPS web console
- Encrypted connections (TLS) for all remote communications
- Zero-trust security model (no implicit trust based on network location)

**Remote Access Requirements:**

- MFA mandatory for all remote access (no exceptions)
- Google Workspace account required for Company resource access
- Strong password requirements (see Password Policy)

- Access via authenticated, encrypted connections only
- Remote access security covered comprehensively in Access Management Policy

### 10.2 VPN (If Future Implementation)

**If VPN Implemented in Future:**

- VPN server hosted in Google Cloud Platform
- Strong encryption protocols only (IPsec with AES-256, IKEv2, OpenVPN)
- Certificate-based authentication preferred
- MFA required in addition to VPN credentials
- Split tunneling disabled (all traffic through VPN)
- VPN logs monitored for security incidents
- Regular VPN access reviews

## 11. THIRD-PARTY NETWORK ACCESS

### 11.1 Third-Party Access Policy

**General Prohibition:**

- Third parties do not have direct network access to production environments
- Exceptions only for essential services (see below)

**Permitted Third-Party Network Access:**

- **Google Cloud support:** Via secure support ticket system
- **External auditors:** Time-limited, supervised, logged access
- **Security consultants:** Emergency incident response only, CTO-approved
- **Specific vendors:** Only if absolutely necessary, limited scope, time-limited

### 11.2 Third-Party Network Requirements

**All third-party network access must:**

- Be requested in writing with business justification
- Be approved by CTO
- Be limited to minimum necessary network segments
- Be time-limited (typically 24-48 hours, maximum 7 days)
- Use unique accounts (not shared with employees)
- Be fully logged and monitored
- Require MFA where technically feasible
- Be reviewed and revoked immediately after purpose completed

**Network Access Documentation:**

- Third-party name and company
- Purpose of network access
- Network segments/systems accessed
- Duration of access
- Approval details
- Deactivation confirmation

**See Vendor Management Policy for comprehensive third-party requirements.**

# 12. NETWORK SECURITY FOR DEVELOPMENT

## 12.1 Development Environment Network Security

**Development Network Controls:**

- Separated from production network (network segmentation)
- Less restrictive firewall rules (to facilitate development)
- Synthetic test data only (no production data)
- Developers have broader network access in development environment
- Development environment infrastructure defined in Infrastructure-as-Code

**Development Network Requirements:**

- TLS encryption still required for development database connections
- Strong authentication required for development resource access
- Development environment access logged
- Regular security scans of development infrastructure
- Development firewall rules documented and reviewed

## 12.2 CI/CD Pipeline Network Security

**Pipeline Network Architecture:**

- CI/CD pipeline runs in isolated network segment
- Pipeline authenticates to Google Cloud using service accounts
- Pipeline has minimum necessary network access (least privilege)
- Pipeline network access audited and logged
- Pipeline cannot directly access production databases (deployment via approved change control only)

**Pipeline Security Controls:**

- Secrets never hardcoded in pipeline configuration
- Encryption keys managed via Google Cloud KMS

- Pipeline logs monitored for security issues
- Vulnerability scanning in pipeline before deployment
- Network access tests in automated test suite

# 13. COMPLIANCE AND REGULATORY REQUIREMENTS

## 13.1 GDPR Network Security

**GDPR Article 32 - Security of Processing:**

- Encryption of personal data in transit (TLS 1.2+)
- Network segmentation to protect personal data
- Network monitoring to detect data breaches
- Regular testing and evaluation of network security measures

**Data Residency:**

- All networks hosting customer data located in EU (Netherlands and Belgium)
- No international data transfers via network connections
- Network traffic logs containing personal data retained per Log Management Policy

## 13.2 ISO 27001 Alignment

**Network Security Controls:**

- A.13.1 Network Security Management
- A.13.2 Information Transfer
- Compliance monitored via Google Cloud Security Command Centre
- Network security controls documented and auditable

## 13.3 Healthcare Security Requirements

**Customer Requirements:**

- Network security controls meet healthcare customer security requirements
- Network segmentation protects healthcare trial data
- Encryption in transit protects patient information
- Network logs available for customer security audits

# 14. ROLES AND RESPONSIBILITIES

| Role | Responsibilities |
|---|---|
| **CTO (Responsible Person)** | Overall network security policy ownership; Google Cloud network configuration; firewall rule approval; Security Command Centre review; network security incident response; policy review and updates |
| **Backend Developers** | Implement secure network configurations; configure Infrastructure-as-Code for network resources; assist with network security incident investigation; network security testing |
| **Product Manager** | Network security requirements for ShineVR features; customer network security requirement coordination |
| **All Employees** | Comply with wireless network security requirements; protect Company network credentials; report network security incidents; follow home network security guidelines (BYOD Policy) |

# 15. NETWORK SECURITY TESTING

## 15.1 Regular Security Testing

**Automated Testing:**

- Network security tests in CI/CD pipeline
- Vulnerability scanning of network-facing services
- Automated firewall rule testing
- TLS configuration testing (certificate validity, strong ciphers)

**Manual Testing:**

- Quarterly network security review
- Annual comprehensive network security assessment
- Penetration testing (application level, leveraging Google Cloud network security)
- Firewall rule effectiveness review

## 15.2 Vulnerability Management

**Network Vulnerability Scanning:**

- Continuous vulnerability scanning via Google Cloud Security Command Centre
- Docker container vulnerability scanning includes network services
- Automated scanning on every code change
- Failed vulnerability scans block deployment

**Remediation:**

- High-severity network vulnerabilities: 7-day remediation target
- Medium-severity: 30-day remediation target
- Low-severity: 90-day remediation target
- Emergency patches for actively exploited vulnerabilities (immediate)

# 16. INCIDENT RESPONSE

## 16.1 Network Security Incidents

**Types of Network Security Incidents:**

- Unauthorized network access attempts
- DDoS attacks
- Network intrusion detected
- Firewall rule violations
- Unusual network traffic patterns
- Network service outages

**Incident Classification:**

- P1 (Critical): Active network breach, production service outage
- P2 (High): Suspected unauthorized access, network anomalies
- P3 (Low): Network policy violations, minor configuration issues

**See Incident Management Policy for comprehensive incident response procedures.**

## 16.2 Network Isolation Procedures

**Incident Containment:**

- Ability to isolate compromised instances from network
- Emergency firewall rules to block malicious traffic
- Network segmentation limits incident spread
- Automated isolation for certain attack types (via Cloud Armor)

**Recovery:**

- Network configuration restored from Infrastructure-as-Code
- Clean instances deployed from known-good container images
- Network connectivity restored after threat eliminated
- Post-incident network security review

# 17. POLICY REVIEW AND MAINTENANCE

**Review Schedule:**

- Annual policy review by CTO
- Review triggered by:
    - Significant network security incidents
    - Changes to Google Cloud network architecture
    - New regulatory requirements
    - Customer security requirement changes
    - Major ShineVR feature releases affecting network architecture

**Policy Updates:**

- All updates require CTO approval
- Changes communicated to all staff within 10 working days
- Updated policy published to Company policy repository
- Policy version history maintained

# 18. TRAINING AND AWARENESS

## 18.1 Network Security Training

**Required Training:**

- All new employees: Network security awareness training during induction
- Annual refresher training for all staff
- Specialized training for backend developers (secure network configuration)
- Training covers:
    - Wireless network security
    - Remote access security
    - Recognizing network security incidents
    - Phishing and social engineering
    - Home network security (for remote workers)

## 18.2 Developer Network Security Training

**Technical Training:**

- Secure network configuration in Google Cloud
- Firewall rule best practices
- Infrastructure-as-Code for network resources
- TLS/SSL certificate management
- Network security testing
- Incident response for network security issues

# 19. EXCEPTIONS

## 19.1 Exception Process

**Requesting Network Security Exceptions:**

- Exceptions requested in writing to CTO
- Business justification required
- Risk assessment documented
- Compensating controls identified
- Time-limited exceptions preferred
- Permanent exceptions require CEO approval

**Approved Exception Documentation:**

- Exception details and justification
- Approved compensating controls
- Review schedule
- Expiry date (if time-limited)
- CTO approval signature

## 19.2 Emergency Exceptions

**Emergency Network Changes:**

- During P1 security incidents, CTO may authorize emergency network changes
- Emergency changes documented within 24 hours
- Emergency firewall rules reviewed within 48 hours
- Temporary emergency changes replaced with permanent solution within 7 days

# 20. RELATED POLICIES AND DOCUMENTS

This policy should be read in conjunction with:

- Information Security Policy
- Cloud Security Policy
- Access Management Policy

- Encryption Policy
- Incident Management Policy
- Log Management Policy
- BYOD Policy
- Physical Security Policy
- Change Control Policy
- Vendor Management Policy

# 21. CONTACT INFORMATION

**Data Protection Officer / Chief Technology Officer:**

Andrés Pitt
Email: andres@vstream.ie
Phone: (086) 788 6570
Available 24/7 for P1 network security incidents

**Company Address:**

vStream Digital Media
37 Leeson Close
Dublin 2, D02 H344
Ireland

Website: vstream.ie