Vendor Management Policy

vStream Digital Media / ShineVR

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
Vendor	Any third-party supplier, service provider, contractor, or partner providing goods or services to the Company
Critical Vendor	Vendor with access to sensitive data, critical systems, or whose failure would significantly impact business operations
Data Processor	Vendor who processes personal data on behalf of the Company as Data Controller
Risk Classification	Assessment of vendor risk level (Low, Medium, High, Critical) based on data access and service criticality
Data Processing Agreement (DPA)	Contractual agreement defining data protection responsibilities between Company and vendor

1. POLICY STATEMENT

vStream Digital Media recognises that third-party vendors are essential to business operations but also represent potential security, privacy, and operational risks. This Vendor Management Policy establishes a comprehensive framework for assessing, selecting, contracting with, and monitoring vendors to ensure they meet the Company's security, privacy, and operational requirements.

All vendors must be evaluated for security posture, data protection practices, and business continuity capabilities before engagement. Ongoing monitoring ensures vendors continue to meet requirements throughout the relationship lifecycle.

2. PURPOSE

The purpose of this policy is to:

- Establish consistent vendor assessment and selection criteria
- Ensure vendors meet appropriate security and privacy standards
- Protect Company and ShineVR data processed by vendors
- Ensure GDPR compliance for vendors processing personal data
- Define vendor risk classification and management requirements
- Establish ongoing vendor monitoring and review procedures
- Define vendor incident response and termination procedures
- Ensure business continuity through vendor resilience
- Maintain a comprehensive vendor inventory and risk register

3. SCOPE

This policy applies to:

- All third-party vendors providing services or products to the Company
- All vendors with access to Company or ShineVR systems, data, or facilities
- All vendors processing personal data on behalf of the Company
- Cloud service providers (including Google Cloud Platform)
- Software-as-a-Service (SaaS) providers
- Professional services firms
- Contractors and consultants
- Technology suppliers
- Business partners with data sharing arrangements

This policy applies throughout the vendor lifecycle:

- Vendor identification and selection
- Vendor assessment and due diligence
- Contract negotiation and execution
- Ongoing vendor management and monitoring
- Vendor performance review
- Contract renewal or termination
- Vendor offboarding

4. VENDOR RISK CLASSIFICATION

4.1 Risk Classification Criteria

All vendors are classified based on:

- **Data Access:** What type and volume of Company/customer data can vendor access?
- **Service Criticality:** How critical is the vendor's service to business operations?
- **System Access:** What level of access does the vendor have to Company systems?
- **Regulatory Impact:** Does vendor processing affect regulatory compliance?
- **Financial Impact:** What is the financial impact of vendor failure or breach?
- **Reputational Impact:** What reputational damage could a vendor incident cause?

4.2 Risk Classifications

Risk Level	Definition	Examples	Assessment Requirements
Critical	Access to sensitive personal data, critical systems, or service failure causes major business disruption	Google Cloud Platform, primary payment processor, core application vendors	Comprehensive security assessment, penetration testing requirements, executive approval, detailed DPA, annual reassessment, continuous monitoring
High	Access to confidential business data, important systems, or service failure causes significant disruption	Email/collaboration platforms (Google Workspace), customer communication tools (Slack), database vendors	Detailed security assessment, security certifications required, CTO approval, DPA if processing personal data, annual review,

Risk Level	Definition	Examples	Assessment Requirements
			performance monitoring
Medium	Limited data access, moderate system access, or service failure causes moderate disruption	Development tools, project management software, analytics platforms	Standard security assessment, basic security documentation, CTO approval, DPA if processing personal data, bi-annual review
Low	No sensitive data access, minimal system access, service failure has minimal impact	Office supplies, marketing services (no data access), generic tooling	Basic vendor assessment, standard contract terms, manager approval, annual review if multi-year contract

4.3 Risk Classification Review

- Initial risk classification assigned during vendor selection
- Risk classification reviewed annually or when vendor services change
- Vendor may be reclassified if risk profile changes
- Higher risk classification triggers enhanced controls
- Risk classification documented in vendor register

5. VENDOR SELECTION AND ASSESSMENT

5.1 Vendor Identification

Prior to Engaging Any Vendor:

- Business need clearly defined and documented
- Alternative solutions evaluated (build vs. buy, multiple vendor options)
- Budget and resource requirements assessed
- Stakeholder requirements gathered
- Compliance and regulatory requirements identified

5.2 Vendor Assessment Process

Step 1: Initial Assessment

Evaluate vendor based on:

- **Prior Knowledge:** Company's previous experience or industry reputation
- **Financial Stability:** Vendor's financial health and business continuity
- **Market Position:** Vendor's market standing and customer base
- **References:** Feedback from other customers
- **Service Fit:** Technical and functional fit with requirements
- **Geographic Location:** Preference for EU-based vendors for data residency
- **Pricing Model:** Avoid "free" products that monetise through data resale

Step 2: Security Assessment

For Medium, High, and Critical risk vendors:

- **Security Documentation Review:**
    - Information security policies and procedures
    - Data protection and privacy policies
    - Incident response procedures
    - Business continuity and disaster recovery plans
    - Security awareness training programmes
    - Vulnerability management processes
    - Access control procedures
- **Security Certifications:**
    - **Required for High/Critical vendors:** SOC 2 Type II, ISO 27001, or equivalent
    - **Preferred certifications:**
        - ISO 27001 (Information Security Management)
        - ISO 27017 (Cloud Security)
        - ISO 27018 (Cloud Privacy)
        - SOC 2 Type II (Security, Availability, Confidentiality)
        - PCI DSS (if processing payment data)
        - CSA STAR (for cloud providers)
    - Certifications must be current (not expired)
    - Certification audit reports reviewed if available
- **Technical Security Controls:**

    - Encryption at rest and in transit
    - Access control and authentication mechanisms
    - Network security and segmentation
    - Vulnerability management and patching
    - Security monitoring and logging
    - Backup and recovery capabilities
    - Physical security of data centres (for infrastructure providers)

Step 3: Data Protection and Privacy Assessment

For vendors processing personal data:

- **Data Processing Practices:**

    - Types of personal data processed
    - Purpose and legal basis for processing
    - Data storage locations and residency
    - Data retention and deletion practices
    - Sub-processor arrangements
    - Cross-border data transfers

- **GDPR Compliance:**

    - GDPR compliance programme
    - Data Protection Officer (DPO) appointed if required
    - Data subject rights support (access, rectification, erasure, portability)
    - Breach notification procedures (within 72 hours)
    - Data protection by design and default
    - Privacy Impact Assessments for high-risk processing

- **Privacy Certifications:**

    - ISO 27701 (Privacy Information Management)
    - EU-US Data Privacy Framework certification (if US-based)
    - Privacy Shield successor mechanisms
    - National privacy certifications

Step 4: Operational Assessment

- **Service Level Agreements (SLAs):**

    - Availability and uptime guarantees

  - Performance metrics
  - Response and resolution times for issues
  - Penalties for SLA breaches
  - Scheduled maintenance windows

- **Business Continuity:**

  - Business continuity and disaster recovery plans
  - Backup and recovery procedures
  - Redundancy and failover capabilities
  - Incident response capabilities
  - Financial stability and viability

- **Support and Maintenance:**

  - Support availability (24/7, business hours, time zones)
  - Support channels (phone, email, portal)
  - Escalation procedures
  - Account management
  - Professional services availability

Step 5: Contract and Legal Review

- **Standard Contract Terms:**

  - Scope of services clearly defined
  - Pricing and payment terms
  - Contract term and renewal provisions
  - Termination clauses and notice periods
  - Liability and indemnification
  - Intellectual property rights
  - Confidentiality obligations

- **Security and Privacy Clauses:**

  - Data Processing Agreement (DPA) for vendors processing personal data
  - Security controls and standards requirements
  - Right to audit vendor security practices
  - Breach notification obligations
  - Data return and deletion upon termination
  - Sub-processor notification and approval requirements

- **Compliance Requirements:**

    - Regulatory compliance obligations
    - Industry standards compliance
    - Legal jurisdiction and governing law (prefer EU/Irish law)
    - Compliance with Company policies

Step 6: Risk Assessment and Approval

- Complete vendor risk assessment documenting:
    - Risk classification (Low, Medium, High, Critical)
    - Key risks identified
    - Mitigating controls
    - Residual risk level
    - Compensating controls if needed
- **Approval Requirements:**
    - **Low risk:** Department manager approval
    - **Medium risk:** CTO approval
    - **High risk:** CTO approval with documented risk assessment
    - **Critical risk:** CTO and CEO approval with comprehensive risk assessment

5.3 Vendor Assessment Documentation

All vendor assessments documented including:

- Vendor name and contact information
- Service description and business purpose
- Risk classification and justification
- Security assessment results
- Compliance verification
- References checked
- Contract review notes
- Risk assessment summary
- Approval signatures and dates
- All documentation retained in vendor management system

6. VENDOR SELECTION PRINCIPLES

6.1 Security-First Approach

Mandatory Principles:

- Security is primary consideration in vendor selection
- Vendors without adequate security controls are rejected regardless of cost savings
- "Free" services are avoided if they monetise user data (e.g., selling data to third parties)
- Security certifications (SOC 2, ISO 27001) strongly preferred for critical vendors

Example Applications:

- Google Analytics not used in ShineVR applications (avoid free products that track user behaviour)
- Paid security tools preferred over free alternatives with data sharing
- Open-source solutions acceptable if security can be verified and maintained

6.2 EU Preference

Data Residency Preference:

- EU-based vendors preferred for services processing personal data
- Non-EU vendors acceptable only if:
    - Adequate data protection mechanisms in place (Standard Contractual Clauses)
    - Data processing occurs in EU data centres
    - GDPR compliance demonstrated
    - No alternatives meeting requirements

Current EU Vendors:

- Primary infrastructure: Google Cloud Platform (EU data centres)
- Email and productivity: Google Workspace
- Internal communication: Slack

6.3 Compatibility and Integration

Technical Compatibility:

- Vendor solutions must integrate with existing systems
- APIs and integration methods assessed
- Data import/export capabilities verified
- Compatibility with Google Cloud Platform preferred

Operational Compatibility:

- Vendor support hours align with Company needs
- Vendor culture and values align with Company
- Communication and language capabilities adequate

6.4 Vendor Reputation and Stability

Reputation Assessment:

- Industry reputation and customer reviews
- Security incident history researched
- Data breach history reviewed
- Customer references checked
- Media coverage and public perception

Financial Stability:

- Financial health assessed for critical vendors
- Business viability for multi-year commitments
- Merger/acquisition risk considered
- Backup vendor identified for critical services

7. CONTRACTUAL REQUIREMENTS

7.1 Data Processing Agreements (DPA)

Mandatory Requirement: All vendors processing personal data must execute a Data Processing Agreement

DPA Must Include:

- Description of processing activities and purposes
- Types of personal data and categories of data subjects
- Duration of processing
- Obligations of data processor (vendor):
    - Process data only on documented instructions
    - Ensure confidentiality of personnel
    - Implement appropriate security measures
    - Engage sub-processors only with prior authorisation
    - Assist with data subject rights requests
    - Notify breaches within 24 hours
    - Delete or return data upon termination
    - Submit to audits and provide information
- Company rights and obligations as data controller
- International data transfer mechanisms (if applicable)
- Liability and indemnification for data breaches

Standard Contractual Clauses (SCCs):

- Required for transfers to vendors outside EEA
- Use EU Commission approved SCCs
- Additional safeguards for transfers to certain countries

7.2 Security Requirements in Contracts

Mandatory Security Clauses:

- Vendor must maintain appropriate technical and organisational security measures
- Specific security controls required (encryption, access control, monitoring, etc.)
- Security standards to be maintained (ISO 27001, SOC 2, etc.)
- Regular security assessments and penetration testing (for critical vendors)
- Vulnerability disclosure and patching timelines
- Security incident notification obligations (within 24 hours)
- Company right to audit vendor security practices
- Security breach liability and indemnification

7.3 Audit Rights

Company Rights to Audit:

- Annual right to audit vendor security and privacy practices
- Right to review vendor security documentation
- Right to request third-party audit reports (SOC 2, ISO 27001)
- Right to conduct on-site audits for critical vendors (with reasonable notice)
- Right to engage third-party auditors
- Vendor must cooperate with audits and provide requested information

7.4 Sub-Processor Management

For vendors who use sub-processors:

- Vendor must notify Company of all sub-processors
- Company right to object to sub-processors
- Sub-processors must meet same security and privacy standards
- Vendor remains liable for sub-processor actions
- List of current sub-processors provided at contract signing
- Changes to sub-processors require advance notification (30 days minimum)

7.5 Termination and Data Return

Contract Termination Provisions:

- Clear termination clauses and notice periods
- Transition assistance during termination period
- Data return or deletion obligations:
    - Vendor must return all Company data in usable format within 30 days
    - Vendor must securely delete all Company data after return
    - Vendor must certify deletion in writing
- Survival clauses (confidentiality, audit rights, liability)

8. VENDOR ONBOARDING

8.1 Onboarding Process

Upon vendor selection and contract execution:

Step 1: Vendor Registration

- Add vendor to vendor register/inventory
- Assign unique vendor ID
- Document vendor details (contact, services, risk level, contract dates)
- Assign vendor owner within Company

Step 2: Access Provisioning

- Provision necessary system access (least privilege principle)
- Create vendor user accounts or service accounts
- Configure access controls and permissions
- Enable multi-factor authentication if applicable
- Document all access granted

Step 3: Security Configuration

- Configure security settings per contract requirements
- Enable logging and monitoring for vendor activity
- Set up security alerts for vendor-related events
- Configure encryption for data shared with vendor
- Test security controls

Step 4: Vendor Orientation

- Provide vendor with relevant Company policies
- Security and privacy requirements review
- Incident reporting procedures

- Communication protocols and contacts
- Support and escalation procedures

Step 5: Initial Performance Baseline

- Establish performance metrics and KPIs
- Configure monitoring and reporting
- Schedule regular review meetings
- Define success criteria

8.2 Vendor Documentation

Maintain comprehensive vendor documentation:

- Vendor contact information and account managers
- Contract and DPA copies
- Security assessment results
- Risk assessment and approval documents
- Access permissions and credentials
- Integration documentation
- Escalation procedures
- Review and audit schedules

9. ONGOING VENDOR MANAGEMENT

9.1 Continuous Monitoring

Automated Monitoring:

- **Security Monitoring:**
    - Keyword monitoring for vendor security incidents (security newsletters, CVE databases)
    - Vendor security posture monitoring via third-party services
    - System availability and performance monitoring
    - Log analysis for unusual vendor activity
- **Performance Monitoring:**
    - Performance dashboards for critical vendors
    - SLA compliance tracking
    - Service availability monitoring
    - Response time and quality metrics

  - Cost and usage tracking

Manual Monitoring:

- Regular review of vendor security news and announcements
- Quarterly review of vendor security status
- Annual review of vendor certifications (renewal, expiration)
- Periodic review of vendor financial stability

9.2 Vendor Performance Reviews

Review Frequency Based on Risk:

- **Critical vendors:** Quarterly reviews
- **High-risk vendors:** Semi-annual reviews
- **Medium-risk vendors:** Annual reviews
- **Low-risk vendors:** Annual reviews (if multi-year contract)

Performance Review Includes:

- SLA compliance and performance metrics
- Security posture and incident history
- Data protection compliance
- Contract compliance
- Communication and support quality
- Cost effectiveness and value
- Business continuity preparedness
- Recommendations for continuation, renegotiation, or termination

Review Documentation:

- Performance review meeting notes
- Metrics and KPIs analysis
- Issues and concerns identified
- Action items and remediation plans
- Decisions on contract renewal or changes

9.3 Vendor Compliance Monitoring

Ongoing Compliance Verification:

- **Security Certifications:**
  - Track certification expiration dates

    - Request updated certificates upon renewal
    - Verify certifications remain current
    - Escalate if certifications lapse

- **Policy and Procedure Updates:**

    - Review updated vendor policies when published
    - Assess impact of vendor policy changes
    - Request clarification on significant changes
    - Update internal documentation as needed

- **SLA and Contract Compliance:**

    - Monitor SLA adherence
    - Track contractual obligations
    - Document and escalate breaches
    - Request remediation for non-compliance

9.4 Vendor Relationship Management

Regular Communication:

- Scheduled review meetings (frequency based on risk level)
- Quarterly business reviews for critical vendors
- Ad-hoc meetings for issues or changes
- Annual strategic planning sessions for key partners

Relationship Optimization:

- Identify opportunities for improved service
- Negotiate better terms or pricing
- Expand or reduce services based on needs
- Provide feedback on vendor performance
- Collaborate on innovation and improvements

Vendor Satisfaction:

- Ensure timely payment of invoices
- Provide clear requirements and feedback
- Maintain professional working relationship
- Recognise and appreciate good performance

10. VENDOR SECURITY INCIDENTS

10.1 Vendor Incident Notification

Vendor Obligations:

- Notify Company of security incidents within 24 hours
- Provide initial incident details:
    - Nature of incident
    - Data potentially affected
    - Number of individuals affected
    - Actions taken by vendor
    - Estimated timeline for resolution
- Provide regular updates during incident response
- Provide final incident report with root cause analysis

Company Response:

- Log incident in Company incident register
- Assess impact on Company operations and data
- Activate incident response plan if necessary
- Coordinate with vendor on response actions
- Notify affected parties if required (customers, regulators)
- Document all communications and actions

10.2 Vendor Incident Assessment

Upon notification of vendor security incident:

Step 1: Initial Assessment (within 2 hours)

- Classify incident severity (P1, P2, P3)
- Determine impact on Company and ShineVR systems
- Identify data potentially compromised
- Assess regulatory notification requirements

Step 2: Containment Actions

- Disable vendor system access if necessary
- Rotate credentials and API keys
- Implement additional monitoring
- Isolate affected systems or data

- Prevent further data access or loss

Step 3: Investigation and Remediation

- Work with vendor to understand root cause
- Verify vendor's remediation actions
- Assess effectiveness of vendor response
- Determine if additional controls needed
- Consider long-term vendor relationship

Step 4: Recovery and Post-Incident

- Restore normal operations when safe
- Enhanced monitoring for 30 days
- Post-incident review with vendor
- Update risk assessment and controls
- Document lessons learned

10.3 Breach Notification Obligations

If vendor incident affects personal data:

- Assess GDPR notification requirements within 24 hours
- Notify Data Protection Commission within 72 hours if required
- Notify affected data subjects if high risk
- Document decisions and rationale
- Maintain detailed records of breach response

Vendor Liability:

- Vendor liable for breaches caused by their actions or negligence
- Indemnification clauses in contract apply
- Financial penalties and damages per contract
- Potential contract termination for serious breaches

11. VENDOR TERMINATION AND OFFBOARDING

11.1 Termination Reasons

Vendor relationships may be terminated due to:

- Contract expiration or non-renewal
- Poor performance or repeated SLA breaches

- Security breaches or non-compliance
- Business requirements change
- Better alternative vendor identified
- Vendor out of business or acquired
- Cost optimization
- Strategic realignment

11.2 Termination Process

Step 1: Termination Decision and Notification

- Document termination reason and approval
- Review contract termination clauses
- Provide required notice per contract (typically 30-90 days)
- Communicate termination to vendor in writing
- Establish termination timeline and milestones

Step 2: Transition Planning

- Identify replacement vendor or alternative solution
- Plan data migration and service transition
- Assign transition responsibilities
- Establish transition timeline
- Test replacement solution

Step 3: Data Return and Deletion

- Request return of all Company data from vendor
- Verify data completeness and integrity
- Import data into replacement system
- Request certified deletion of all Company data
- Obtain written certification of deletion
- Verify deletion if possible (audit vendor's systems)

Step 4: Access Revocation

- Revoke all vendor access to Company systems
- Delete vendor user accounts and service accounts
- Rotate credentials and API keys accessed by vendor
- Remove vendor from authentication systems
- Update firewall rules and network access controls

Step 5: Documentation and Closure

- Final vendor performance review
- Lessons learned documentation
- Update vendor register (mark as terminated)
- Archive all vendor documentation
- Close out financial accounts
- Provide feedback to vendor (if appropriate)

11.3 Emergency Termination

For serious security breaches or emergencies:

- Immediate access revocation without notice
- Rapid data return or deletion
- Accelerated transition to alternative vendor
- Legal consultation for contract disputes
- Regulatory notification if required

12. VENDOR INVENTORY AND REGISTER

12.1 Vendor Register Contents

Comprehensive vendor register maintained including:

- Vendor name and legal entity
- Vendor contact information
- Service description and business purpose
- Risk classification (Low, Medium, High, Critical)
- Contract dates (start, end, renewal dates)
- Contract value
- Data processing role (processor, sub-processor, joint controller)
- Personal data processed (types, categories, volumes)
- System access granted
- Security certifications
- Last assessment date and next review date
- Vendor owner within Company
- Status (active, inactive, terminated)
- Notes and special considerations

12.2 Register Maintenance

- Vendor register reviewed and updated quarterly
- Changes documented with dates and reasons

- Annual comprehensive review and cleanup
- Register accessible to CTO and relevant managers
- Register used for reporting and compliance demonstration

13. SPECIAL VENDOR TYPES

13.1 Critical Infrastructure Vendors

Google Cloud Platform (Primary Infrastructure Provider):

- Comprehensive annual assessment
- Quarterly service review meetings
- Continuous monitoring of Google Cloud Status and security bulletins
- Leveraging Google's certifications (ISO 27001, SOC 2, etc.)
- Regular review of Google Cloud compliance documentation
- Participation in Google Cloud security programmes
- Escalation procedures for critical issues
- Disaster recovery planning for Google Cloud outages

Key Characteristics:

- Single-source dependency for infrastructure
- Critical to all ShineVR operations
- Extensive due diligence required
- Enhanced monitoring and relationship management

13.2 SaaS Application Vendors

Examples: Google Workspace, Slack, GitHub/GitLab

Management Approach:

- Security assessment focused on data protection
- Review of vendor's security and privacy policies
- Verification of security certifications
- User access management and provisioning
- Regular review of user licenses and usage
- Integration security (APIs, SSO)
- Data export and portability planning

13.3 Professional Services Vendors

Examples: External security consultants, auditors, legal advisors

Management Approach:

- Confidentiality agreements required
- Limited-time access to systems or data
- Supervised access where possible
- Background checks for sensitive work
- Work product ownership clearly defined
- Engagement terms and deliverables documented

13.4 Open-Source Software

Approach to Open-Source:

- Open-source acceptable if security can be verified
- Dependency vulnerability scanning required
- Active maintenance and community support verified
- Licensing compatibility assessed
- Commercial support available (preferred for critical components)
- Security response process for vulnerabilities documented

14. VENDOR RISK REGISTER

14.1 Risk Register Maintenance

Comprehensive risk register documenting:

- Vendor name and service
- Risk classification (Low, Medium, High, Critical)
- Specific risks identified (security, operational, financial, compliance)
- Likelihood and impact assessment
- Mitigating controls implemented
- Residual risk level
- Risk owner within Company
- Risk treatment plan
- Review date

14.2 Risk Escalation

Risk escalation triggers:

- Vendor security incident or breach
- Vendor financial difficulty or instability

- Loss of required certifications
- Significant service degradation
- Contract disputes or non-compliance
- Regulatory concerns
- Change in vendor ownership or service

Escalation Process:

- Risk owner notifies CTO immediately
- Enhanced monitoring implemented
- Risk treatment plan updated
- More frequent reviews scheduled
- Alternative vendor evaluation initiated if necessary
- Senior management notified for critical vendors

15. COMPLIANCE AND AUDIT

15.1 Vendor Compliance Requirements

GDPR Compliance:

- All vendors processing personal data must comply with GDPR
- Data Processing Agreements in place
- Data subject rights support procedures defined
- Breach notification procedures established
- International data transfer mechanisms compliant

Industry Standards:

- ISO 27001 compliance preferred for critical vendors
- SOC 2 Type II reports for critical vendors
- Industry-specific certifications (PCI DSS, HIPAA) as applicable

15.2 Vendor Audits

Audit Schedule:

- Critical vendors: Annual audits
- High-risk vendors: Bi-annual audits or upon contract renewal
- Medium-risk vendors: Audit upon contract renewal
- Triggered audits: Following incidents or significant changes

Audit Types:

- **Documentation Review:** Review policies, procedures, certifications
- **Questionnaire:** Comprehensive security and privacy questionnaires **Third-Party Reports:** Review SOC 2, ISO 27001 audit reports
- **On-Site Audit:** Physical inspection of facilities and operations (for critical vendors)
- **Technical Audit:** Penetration testing, vulnerability assessment (for critical vendors)

Audit Documentation:

- Audit plan and scope
- Audit findings and observations
- Vendor responses and remediation plans
- Follow-up actions and timelines
- Audit completion sign-off

15.3 Regulatory Audits

Supporting Customer/Regulatory Audits:

- Vendor documentation available for regulatory audits
- Vendor audit rights exercised to obtain compliance evidence
- Vendor security and compliance reports provided to auditors
- Coordinate with vendors during customer audits
- Maintain audit trail of vendor management activities

16. ROLES AND RESPONSIBILITIES

Role	Responsibilities
CTO (Responsible Person)	Overall vendor management policy ownership; approve Medium/High/Critical vendor engagements; conduct vendor security assessments; manage critical vendor relationships; vendor incident response; review vendor register quarterly; escalation point for vendor issues
Department Managers	Identify vendor needs; conduct business requirements assessment; approve Low-risk vendors; manage vendor day-to-day relationships; monitor vendor performance; report vendor issues; ensure contract compliance

Role	**Responsibilities**
Finance/Procurement	Contract negotiation and execution; invoice processing; payment management; contract renewal tracking; cost optimization; financial risk assessment
Legal (External Counsel)	Contract review and negotiation; Data Processing Agreement review; legal compliance advice; dispute resolution; regulatory liaison if needed
Product Manager	Vendor technical requirements; vendor integration oversight; vendor performance feedback; feature and functionality assessment
All Employees	Report vendor security concerns; comply with vendor usage policies; protect vendor credentials; follow data sharing procedures; report vendor performance issues

17. TRAINING AND AWARENESS

17.1 Vendor Management Training

Required Training:

- **Managers:** Vendor assessment and selection procedures
- **Technical staff:** Vendor security assessment, integration security
- **All staff:** Acceptable use of vendor services, data protection with vendors

Training Topics:

- Vendor risk classification
- Security assessment procedures
- Contract and DPA requirements
- Ongoing vendor monitoring
- Incident reporting for vendor issues
- Data protection when working with vendors

17.2 Vendor Resources

Available Resources:

- Vendor assessment checklist and templates
- Standard Data Processing Agreement template
- Security questionnaire templates
- Contract security requirements checklist
- Vendor incident reporting procedures
- Vendor register and documentation repository

18. EXCEPTIONS

18.1 Exception Process

Exceptions to vendor management requirements may be requested for:

- Emergency situations requiring immediate vendor engagement
- Unique vendor services with no alternatives
- Cost constraints requiring compromise on requirements
- Technical limitations of available vendors

All exceptions must:

- Be requested in writing to CTO with detailed justification
- Document compensating controls to mitigate risks
- Be approved in writing by CTO (and CEO for critical vendors)
- Be time-limited and reviewed quarterly
- Be documented in vendor register with risk assessment

18.2 Legacy Vendors

Vendors engaged before this policy implementation:

- Retrospective assessment conducted within 12 months
- Bring into compliance with policy requirements
- Update contracts and DPAs to meet requirements
- Terminate if cannot meet minimum requirements

19. POLICY REVIEW AND UPDATES

19.1 Review Schedule

This policy will be reviewed:

- **Annually:** Comprehensive review by CTO
- **After vendor incidents:** Update based on lessons learned
- **Regulatory changes:** Updates for GDPR or other regulatory changes
- **Significant vendor changes:** Major vendor acquisitions, service changes
- **After audits:** Update based on audit findings

19.2 Continuous Improvement

- Monitor vendor management best practices
- Incorporate lessons learned from vendor incidents
- Update vendor assessment criteria based on evolving threats
- Enhance monitoring and automation
- Streamline processes for efficiency

20. RELATED POLICIES

This policy should be read in conjunction with:

- Information Security Policy
- Data Protection Policy
- Cloud Security Policy
- Encryption Policy
- Access Management Process/Procedure
- Incident Response Plan
- Change Control Policy
- Procurement Policy (if applicable)

21. CONTACT INFORMATION

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

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

END OF POLICY

APPENDIX A: VENDOR ASSESSMENT CHECKLIST

Vendor Information:

- □ Vendor name and legal entity
- □ Contact information and account manager
- □ Service description and business purpose
- □ Geographic locations of operations

Initial Assessment:

- □ Business need clearly defined
- □ Alternative vendors evaluated
- □ Budget approved
- □ Preliminary technical fit assessed

Security Assessment:

- □ Security policies and procedures reviewed
- □ Security certifications verified (SOC 2, ISO 27001, etc.)
- □ Encryption at rest and in transit confirmed
- □ Access control mechanisms reviewed
- □ Incident response procedures documented
- □ Vulnerability management process assessed
- □ Security awareness training for vendor staff confirmed

Data Protection Assessment (if processing personal data):

- □ Data processing activities documented
- □ Data types and categories identified
- □ Data storage locations and residency confirmed
- □ GDPR compliance verified
- □ Data subject rights procedures confirmed
- □ Breach notification procedures documented
- □ Sub-processor list obtained
- □ International data transfer mechanisms compliant

Operational Assessment:

- □ SLAs reviewed and acceptable
- □ Availability and uptime guarantees documented
- □ Business continuity and disaster recovery plans reviewed
- □ Support availability and channels confirmed
- □ Financial stability assessed
- □ References checked

Contract Review:

- □ Scope of services clearly defined
- □ Pricing and payment terms acceptable
- □ Termination clauses and notice periods reviewed
- □ Liability and indemnification provisions acceptable
- □ Data Processing Agreement executed (if processing personal data)
- □ Security requirements included in contract
- □ Audit rights included
- □ Sub-processor notification requirements included

Risk Assessment:

- □ Risk classification assigned (Low, Medium, High, Critical)
- □ Key risks identified and documented
- □ Mitigating controls identified
- □ Residual risk assessed
- □ Compensating controls documented if needed

Approval:

- □ Appropriate approval obtained based on risk level
- □ Documentation complete and archived
- □ Vendor added to vendor register