Backup and Recovery 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
Backup	A copy of data stored separately from the primary data for recovery purposes
Recovery Time Objective (RTO)	The maximum acceptable time that systems can be offline following a disaster or failure
Recovery Point Objective (RPO)	The maximum acceptable amount of data loss measured in time
Mission-Critical Data	Data essential for core business operations, customer service delivery, or regulatory compliance
Non-Mission-Critical Data	Data that supports operations but is not essential for immediate business continuity
Full Backup	Complete copy of all data

Term	Definition
Incremental Backup	Copy of data that has changed since the last backup
Disaster Recovery	Process of restoring systems and data following a catastrophic event

1. POLICY STATEMENT

vStream Digital Media is committed to protecting all Company and ShineVR data through comprehensive backup and recovery procedures. All critical systems and data are backed up regularly using encrypted, geographically redundant backup storage to ensure business continuity and data protection.

The Company leverages Google Cloud Platform's managed backup services to ensure reliable, secure, and compliant data backup and recovery capabilities. Regular testing of backup restoration procedures ensures the Company can recover from data loss or system failures within acceptable timeframes.

2. PURPOSE

The purpose of this policy is to:

- Protect Company and ShineVR data from loss due to hardware failure, human error, cyberattacks, or disasters
- Ensure business continuity by enabling rapid recovery from data loss or system failures
- Define backup frequency, retention periods, and storage requirements
- Establish Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)
- Ensure compliance with GDPR and data retention requirements
- Define roles, responsibilities, and procedures for backup and recovery operations
- Establish regular testing procedures to verify backup integrity and recoverability
- Protect backup data with appropriate security controls (encryption, access control)

3. SCOPE

This policy applies to:

- All Company and ShineVR data including:
    - Production databases (Cloud SQL)
    - Application data and configuration

        - Source code repositories
        - Business documents and records
        - Employee data
        - Customer data
        - System configurations
        - Encryption keys and credentials (via Google Cloud KMS)

- All systems hosting Company or ShineVR data:

    - Google Cloud Platform production environments
    - Google Cloud Platform staging environments
    - Google Workspace (email, documents, calendars)
    - Development environments (source code)

- All employees, contractors, and third parties responsible for managing backups

This policy covers:

- Backup scheduling and retention
- Backup storage and protection
- Recovery procedures and testing
- Roles and responsibilities
- Monitoring and reporting

4. BACKUP ARCHITECTURE

4.1 Google Cloud Platform Managed Backups

Primary Backup Infrastructure:

- All Company and ShineVR production data hosted on Google Cloud Platform
- Backups managed by **Google Cloud services** including:
    - Cloud SQL automated backups for databases
    - Cloud Storage versioning and lifecycle management for object storage
    - Persistent disk snapshots for any VM storage (if applicable)

Geographic Distribution:

- **Primary data location:** europe-west4-a (Eemshaven, Netherlands) OR europe-west1-b (St. Ghislain, Belgium)
- **Backup storage location:** Alternate European region for geo-redundancy
    - Production data in europe-west4 does to Backups in europe-west1

    - Production data in europe-west1 goes to Backups in europe-west4
- All backup data remains within EU
- Compliant with GDPR data residency requirements

4.2 Backup Types

Automated Database Backups (Cloud SQL):

- **Full backups:** Daily automated full database backups
- **Transaction logs:** Continuous transaction log backups enabling point-in-time recovery
- **Retention:** 7 days for transaction logs, configurable retention for full backups
- **Backup window:** Scheduled during low-usage periods (2:00-4:00 AM Irish time)

Object Storage Backups (Cloud Storage):

- **Versioning:** Object versioning enabled on critical storage buckets
- **Lifecycle management:** Automated deletion of old versions per retention policy
- **Replication:** Geo-redundant storage across multiple European locations

Application and Configuration Backups:

- **Infrastructure-as-Code:** All infrastructure configuration in version control (Git)
- **Container images:** Stored in Google Container Registry with retention
- **Application configuration:** Stored in Google Secret Manager and version controlled

Source Code Backups:

- **Primary repository:** GitHub/GitLab with automatic backups
- **Frequency:** Continuous (every code commit)
- **Retention:** Indefinite retention in version control history

4.3 Whole-of-Database Backup Strategy

Implementation:

- Company operates a "whole-of-database" backup system
- Comprehensive backup includes both trial data and non-trial data
- **ShineVR trial data ringfenced and easily selected for deletion** when contract ends
- Backup system allows selective restoration of specific datasets
- Enables compliance with data retention obligations and customer data deletion requests

5. BACKUP FREQUENCY AND SCHEDULING

5.1 Production Systems

Data Type	Backup Frequency	Backup Method	Retention Period
Production Databases (Cloud SQL)	Daily full backup Continuous transaction logs	Automated Cloud SQL backups	Transaction logs: 7 days Full backups: 6 months for non-mission-critical data Longer for mission-critical or compliance-required data
Cloud Storage (Application data)	Continuous (versioning)	Cloud Storage versioning	6 months for non-mission-critical data Longer for mission-critical data
Application Configuration	On every change	Git version control Google Secret Manager	Indefinite (version history)
Infrastructure Configuration	On every change	Git version control	Indefinite (version history)
Source Code	On every commit	Git repository	Indefinite (version history)
Container Images	On every build	Google Container Registry	90 days for development images Indefinite for production releases

5.2 Non-Production Systems

Environment	Backup Frequency	Retention Period
Staging Environment	Daily	30 days
Development Environment	Weekly (if applicable)	14 days
Test Environment	No backup (synthetic data, recreatable)	N/A

5.3 Google Workspace Data

Data Type	Backup Approach	Notes
Gmail	Google Workspace retention policies	30 days deleted item retention Litigation hold available if needed
Google Drive	Native versioning and trash	30 days trash retention Version history per file settings
Google Calendar	No additional backup	Recreatable, not critical for recovery

6. BACKUP RETENTION PERIODS

6.1 Retention Policy

Mission-Critical Data:

- **Production databases (customer-facing):** Retained for **1 year** minimum
- **Compliance-required data:** Retained per regulatory requirements (typically 7 years for financial/audit data)
- **Source code and infrastructure:** Retained **indefinitely** in version control

Non-Mission-Critical Data:

- **General application data:** Retained for **6 months**

- **Development/testing data:** Retained for **30 days** or less
- **Temporary data:** Deleted after **7 days**

ShineVR Trial Data:

- Trial data ringfenced and easily selectable for deletion
- Trial data retained per contract requirements
- **At contract end:** Trial data deleted per agreed schedule
- Non-mission-critical trial data deleted after **6 months**

6.2 Retention Period Compliance

Alignment with Data Retention Policy:

- Backup retention aligns with Company's Media Retention and Disposal Policy
- Personal data not retained longer than necessary per GDPR requirements
- Data retention schedules documented and enforced via automated lifecycle policies
- Exceptions to standard retention documented with business/legal justification

Automated Retention Enforcement:

- Google Cloud Storage lifecycle policies automatically delete old backups
- Cloud SQL backup retention configured per policy requirements
- Alerts triggered if retention policies misconfigured
- Manual intervention required only for exceptions

6.3 Data Deletion and Disposal

Secure Deletion:

- Data deleted such that it is **irrecoverable**
- Google Cloud performs cryptographic erasure or physical destruction
- Encryption keys destroyed to render encrypted data unreadable
- Compliance with Company's Media Retention and Disposal Policy

Deletion Verification:

- Automated lifecycle policies provide deletion confirmation
- Backup deletion logged in audit trails
- Quarterly review of backup inventories to verify policy compliance

7. RECOVERY TIME AND RECOVERY POINT OBJECTIVES

7.1 Application Layer (ShineVR Applications)

Recovery Time Objective (RTO):

- **Business hours (9 AM - 5:30 PM Irish time):** 8 hours maximum
- **After hours:** Best effort, target 12-24 hours
- Critical P1 incidents may require faster recovery

Recovery Point Objective (RPO):

- **24 hours** maximum acceptable data loss
- Daily backups ensure compliance with RPO
- Continuous transaction logs enable point-in-time recovery to minimize actual data loss

Implementation:

- RTO/RPO objectives achieved through automated backup systems
- Google Cloud managed services provide rapid recovery capabilities
- Container-based architecture enables fast redeployment
- Infrastructure-as-Code enables rapid infrastructure rebuild

7.2 Infrastructure Layer (Google Cloud Platform)

Google Cloud SLAs:

- Company relies on Google Cloud's Service Level Agreements for infrastructure
- **Cloud Run:** 99.95% monthly uptime
- **Cloud SQL:** 99.95% monthly uptime (regional instances)
- **Cloud Storage:** 99.95% monthly uptime
- Google responsible for infrastructure-level backup and recovery

Company Responsibilities:

- Application-level backup and recovery
- Data backup and restoration
- Application configuration backup
- Testing backup recovery procedures

8. BACKUP SECURITY

8.1 Encryption

Encryption at Rest:

- All backup data encrypted using **AES-256**
- Encryption automatic via Google Cloud services
- Encryption keys managed via **Google Cloud Key Management Service (KMS)**
- Keys stored in hardware security modules (HSMs) in European data centres

Encryption in Transit:

- Backup data encrypted during transfer using **TLS 1.2+**
- All communication with Google Cloud services uses HTTPS
- Internal Google Cloud traffic automatically encrypted

Key Management:

- Encryption keys never stored on disk inside servers
- Keys injected at runtime via Google Cloud KMS
- Key rotation managed automatically by Google Cloud
- Key access audited and logged

8.2 Access Control

Backup Access Restrictions:

- Backup access restricted to **CTO and authorised personnel** only
- Least privilege principle applied to backup access
- Google Cloud IAM policies enforce access control
- Multi-factor authentication required for backup access
- Service accounts used for automated backup operations

Audit Logging:

- All backup access logged via Google Cloud Audit Logs
- Backup creation, restoration, and deletion logged
- Logs reviewed for unauthorised access attempts
- Suspicious activity triggers security alerts

8.3 Physical Security

Data Centre Security:

- Backup data stored in Google Cloud data centres
- Physical security managed by Google Cloud:
    - 24/7 surveillance and monitoring
    - Biometric access controls
    - Security personnel
    - Environmental controls (fire suppression, climate control)
- Google Cloud maintains comprehensive physical security certifications

No On-Premise Backup Storage:

- Company does not maintain on-premise backup infrastructure
- All backups stored in Google Cloud's secure data centres
- Eliminates risks of local hardware failure, theft, or disaster

9. BACKUP TESTING AND VALIDATION

9.1 Regular Testing Schedule

Mandatory Testing Requirements:

Monthly Backup Restoration Testing:

- At least one backup restored monthly to verify recoverability
- Alternating database and application data testing
- Test restoration to non-production environment
- Verify data integrity and completeness after restoration
- Document test results and any issues

Quarterly Disaster Recovery Simulation:

- Full disaster recovery scenario tested
- Simulate complete system failure
- Restore production environment from backups
- Validate all systems and data functional
- Measure actual RTO and RPO achieved
- Document lessons learned

Annual Comprehensive DR Exercise:

- Full-scale disaster recovery exercise
- All critical systems and data restored
- All response team members participate
- External stakeholders notified (simulated)
- Complete documentation and after-action review
- Update disaster recovery procedures based on findings

9.2 Continuous Testing Through Operations

"Release Early, Release Often" Practice:

- Company follows agile deployment practices with frequent releases
- **System reset, build, deploy, and restore operations occur very frequently**
- This continuous cycle inherently tests recovery procedures
- Recovery is "not an exceptional event" but routine practice
- Provides ongoing validation of backup and recovery capabilities

Benefits of Continuous Practice:

- Recovery procedures constantly validated
- Team maintains proficiency in recovery operations
- Issues identified and resolved quickly
- Confidence in ability to recover from real disasters
- Documentation kept current through regular use

9.3 Test Documentation

Required Documentation:

- Test date and time
- Systems and data tested
- Test procedure followed
- Test results (success/failure)
- Data integrity verification results
- Time to complete restoration
- Issues encountered and resolutions
- Recommendations for improvement
- Sign-off by CTO

Test Result Review:

- All test results reviewed by CTO
- Failed tests investigated and corrected immediately

- Successful tests documented for audit purposes
- Trends analysed for continuous improvement
- Test results reported to senior management quarterly

10. DISASTER RECOVERY PROCEDURES

10.1 Disaster Scenarios

Backups enable recovery from various disaster scenarios:

- **Hardware failure:** Server, storage, or network equipment failure
- **Data corruption:** Database corruption or data integrity issues
- **Human error:** Accidental deletion or modification of data
- **Cyberattack:** Ransomware, malware, or malicious data destruction
- **Natural disaster:** Fire, flood, earthquake affecting data centres
- **Service provider outage:** Google Cloud regional outage

10.2 Recovery Procedures

Every system component has support documentation for recovery scenarios:

- Recovery procedures documented and maintained
- Procedures updated as part of System Development Lifecycle (SDLC)
- Support documents include:
    - Pre-requisites and dependencies
    - Step-by-step recovery instructions
    - Expected time to complete each step
    - Validation procedures
    - Troubleshooting guidance
    - Contact information for escalation

Recovery Process:

Step 1: Incident Assessment (0-30 minutes)

- Determine scope and severity of data loss or system failure
- Identify affected systems and data
- Classify as P1, P2, or P3 incident
- Activate incident response team
- Notify stakeholders

Step 2: Recovery Planning (30-60 minutes)

- Review relevant recovery documentation
- Determine recovery approach (full restore vs. partial)
- Identify backup to restore from (date/time)
- Verify backup availability and integrity
- Assign recovery tasks to team members
- Establish recovery timeline

Step 3: System Restoration (1-8 hours)

- Provision new infrastructure if necessary (using Infrastructure-as-Code)
- Restore application configuration from version control
- Restore database from backup (Cloud SQL point-in-time recovery if needed)
- Restore application data from Cloud Storage backups
- Restore container images and deploy applications
- Configure network, security, and monitoring

Step 4: Validation and Testing (2-4 hours)

- Verify all systems operational
- Validate data integrity and completeness
- Test critical application functions
- Verify user access and authentication
- Check integrations with external systems
- Monitor for errors or issues

Step 5: Service Restoration

- Gradually restore service to users
- Monitor closely for any issues
- Enhanced monitoring for 24-48 hours
- Communicate service restoration to stakeholders
- Update incident status

Step 6: Post-Incident Review (within 72 hours)

- Document incident and recovery actions
- Analyse root cause
- Evaluate recovery process effectiveness
- Measure actual RTO and RPO achieved
- Identify lessons learned
- Update procedures as needed

10.3 Recovery Prioritisation

Priority Order for Recovery:

1. **Critical infrastructure:** Cloud SQL databases, authentication services
2. **Core ShineVR application services:** Application servers, APIs
3. **Supporting services:** Monitoring, logging, backup systems
4. **Non-critical services:** Development tools, internal systems

11. BUSINESS CONTINUITY INTEGRATION

11.1 Backup as Core Business Continuity Component

- Backup and recovery is fundamental to business continuity strategy
- Enables continuation of operations following disasters
- Minimises downtime and data loss
- Protects customer service delivery
- Ensures regulatory compliance

11.2 Multi-Region Resilience

Geographic Redundancy:

- Data backed up to different European regions
- Protects against regional disasters or outages
- Enables recovery to alternate region if necessary
- Infrastructure-as-Code enables rapid rebuild in new region

Cross-Region Recovery Capability:

- In extreme scenarios, Company can rebuild infrastructure in different Google Cloud region
- Backups stored across regions available for recovery
- Infrastructure-as-Code defines all infrastructure in version control
- Recovery to new region possible within RTO objectives (though extended)

11.3 Vendor Resilience

Google Cloud Provider Resilience:

- Google Cloud maintains 99.95%+ availability SLAs
- Google's infrastructure designed for high availability
- Automatic failover and redundancy at Google's platform level

- Company benefits from Google's disaster recovery capabilities
- Google Cloud Status Dashboard monitored for platform issues

12. BACKUP MONITORING AND REPORTING

12.1 Automated Monitoring

Backup Status Monitoring:

- Automated monitoring of backup job completion
- Alerts triggered for failed backups
- Monitoring of backup storage usage and costs
- Verification of backup retention policy enforcement
- Tracking of backup age (alerts if backups too old)

Alert Channels:

- **Email:** CTO and backend developers
- **Slack:** Dedicated monitoring channel
- **Google Cloud Console:** Visual dashboards

Alert Response:

- Failed backups investigated immediately (within 1 hour)
- Root cause identified and resolved
- Re-run backup if failed
- Escalate if persistent failures
- Document incident and resolution

12.2 Reporting

Weekly Backup Status Report:

- Backup completion status (success/failure rates)
- Backup storage utilisation
- Any backup issues or incidents
- Outstanding remediation actions

Monthly Backup Summary:

- Backup testing results
- Storage costs and optimisation opportunities
- Compliance with retention policies

- Recommendations for improvements

Quarterly Business Continuity Report:

- Disaster recovery testing results
- RTO/RPO compliance
- Recovery capability assessment
- Business continuity risks and mitigations
- Strategic recommendations

13. ROLES AND RESPONSIBILITIES

Role	Responsibilities
CTO (Responsible Person)	Overall backup policy ownership; Google Cloud backup configuration; monitor backup status; respond to backup failures; conduct recovery testing; approve changes to backup procedures; review backup reports; disaster recovery leadership
Backend Developers	Configure application backups; ensure backup requirements in application design; assist with backup testing; participate in disaster recovery exercises; troubleshoot backup issues; implement backup improvements
Product Manager	Define data retention requirements; prioritise recovery testing; participate in disaster recovery planning; communicate with customers during recovery events
DevOps/Infrastructure (if dedicated role)	Implement Infrastructure-as-Code backup procedures; automate backup processes; monitor backup systems; configure Cloud SQL and storage backups; manage backup lifecycle policies
All Employees	Maintain critical work files in Google Drive (automatically backed up); report data loss incidents immediately; follow data retention

Role	Responsibilities
	guidelines; participate in recovery exercises as needed

14. BACKUP COSTS AND OPTIMISATION

14.1 Cost Management

Backup Storage Costs:

- Google Cloud Storage costs for backup data
- Costs based on storage volume and retrieval frequency
- Automated lifecycle policies reduce costs by deleting old backups
- Monthly cost monitoring and budget alerts

Cost Optimisation Strategies:

- Use appropriate storage classes (standard vs. nearline vs. coldline)
- Implement retention policies to delete unnecessary backups
- Compress backup data where possible
- Monitor and eliminate duplicate backups
- Right-size backup retention periods

14.2 Budget and Forecasting

- Backup costs included in monthly Google Cloud budget
- Backup growth projected based on business growth
- Budget alerts at 80% and 100% of backup allocation
- Annual review of backup costs and optimisation opportunities

15. COMPLIANCE AND AUDIT

15.1 Regulatory Compliance

GDPR Compliance:

- Backup retention aligns with GDPR data minimisation principle
- Personal data not retained longer than necessary
- Backup security protects personal data from unauthorised access
- Data subject rights (erasure) supported through selective deletion
- Breach notification procedures include backup restoration if needed

Industry Standards:

- ISO 27001 backup requirements addressed
- SOC 2 backup controls implemented
- Regular testing demonstrates backup reliability

15.2 Audit Support

Audit Evidence:

- Backup configuration documentation
- Backup test results and reports
- Recovery time objective achievement records
- Retention policy compliance evidence
- Access logs for backup systems

Audit Procedures:

- Annual backup audit as part of security review
- Backup procedures reviewed during external audits
- Backup test results provided to auditors
- Compliance documentation maintained for 7 years

16. EXCEPTIONS

16.1 Exception Process

Exceptions to backup policy may be requested for:

- Systems with no recovery requirements (truly temporary data)
- Data that can be easily regenerated or re-obtained
- Cost constraints requiring reduced backup frequency
- Technical limitations preventing standard backups

All exceptions must:

- Be requested in writing to CTO with justification
- Document why backup not required or possible
- Confirm no regulatory or business requirement for backup
- Be approved in writing by CTO
- Be reviewed annually
- Be documented in backup exception register

16.2 Non-Backed-Up Systems

Acceptable Non-Backup Scenarios:

- **Test environments:** Using synthetic data that can be regenerated
- **Development environments:** Local developer machines (code in version control)
- **Temporary processing data:** Intermediate data that can be recreated
- **Publicly available data:** Can be re-downloaded from original source

17. TRAINING AND AWARENESS

17.1 Backup and Recovery Training

Required Training:

- **CTO and backend developers:** Comprehensive backup and recovery procedures training
- **All technical staff:** Basic disaster recovery awareness
- **All employees:** Data protection and backup awareness (using Google Drive)

Training Topics:

- Backup architecture and systems
- Recovery procedures and documentation
- Incident response for data loss events
- Testing procedures and schedules
- Roles and responsibilities during recovery
- Google Cloud backup services usage

17.2 Disaster Recovery Exercises

- All technical staff participate in annual DR exercise
- Tabletop exercises for scenario planning
- Hands-on recovery simulations
- Post-exercise debriefs and lessons learned
- Continuous learning and procedure improvement

18. CONTINUOUS IMPROVEMENT

18.1 Improvement Process

- Lessons learned from backup failures and recovery events

- Feedback from testing and exercises
- New Google Cloud features and capabilities
- Industry best practices and standards
- Emerging threats and vulnerabilities

18.2 Metrics for Success

Key Performance Indicators:

- **Backup success rate:** Target 99.9% successful backups
- **Recovery test success rate:** Target 100% successful tests
- **Actual RTO:** Measure time to recover in tests and real incidents
- **Actual RPO:** Measure data loss in recovery scenarios
- **Mean Time to Recovery (MTTR):** Average time for recovery operations
- **Backup storage efficiency:** Cost per GB of data protected

Reporting and Review:

- Metrics reviewed monthly by CTO
- Trends analysed for improvements
- Targets adjusted based on business needs
- Performance reported to senior management quarterly

19. POLICY REVIEW AND UPDATES

19.1 Review Schedule

This policy will be reviewed:

- **Annually:** Comprehensive review by CTO
- **After major incidents:** Update based on recovery experience
- **After testing failures:** Update based on lessons learned
- **Technology changes:** New backup capabilities or infrastructure changes
- **Regulatory changes:** GDPR or other compliance requirement updates
- **Business changes:** New systems, services, or data types requiring backup

19.2 Version Control

- Current policy maintained in Google Drive
- Previous versions archived for reference
- Changes documented with rationale
- Stakeholders notified of policy updates
- Training materials updated to reflect policy changes

20. RELATED POLICIES

This policy should be read in conjunction with:

- Cloud Security Policy
- Information Security Policy
- Media Retention and Disposal Policy
- Incident Response Plan
- Encryption Policy
- Change Control Policy
- Data Protection Policy

21. CONTACT INFORMATION

For questions regarding this policy or to report backup failures or data loss:

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

For Emergency Data Loss (P1 Incidents): Contact CTO immediately: (086) 788 6570