Password Policy

vStream Digital Media / ShineVR

Date: 03 February 2025

Owner: Andrés Pitt, CTO

Next Review Date: February 2026

Approved by: Andrés Pitt, CTO

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
User	means any employee, contractor, temporary staff, or authorized third party with access to Company or ShineVR systems

1. POLICY STATEMENT

vStream Digital Media is committed to protecting its information systems and data through strong password security practices. This policy establishes mandatory password requirements for all users accessing Company and ShineVR systems to prevent unauthorised access and protect against brute-force attacks.

All password requirements are enforced through **Google Workspace** centralised password management, ensuring consistent application across all Company and ShineVR systems.

2. PURPOSE

The purpose of this policy is to:

- Establish minimum security standards for password creation and management
- Protect Company and ShineVR systems from unauthorized access
- Reduce the risk of password-based security breaches
- Ensure compliance with data protection regulations and security best practices
- Define clear responsibilities for password security

3. SCOPE

This policy applies to:

- All employees, contractors, and temporary staff of vStream Digital Media
- All third-party suppliers and service providers with access to Company or ShineVR systems
- All user accounts accessing Company email, cloud infrastructure, development systems, production systems, and administrative interfaces
- All systems used for ShineVR product development, deployment, and operations

This policy covers:

- Google Workspace accounts (email, Google Cloud Platform access)
- ShineVR application administrator accounts
- Development, staging, and production environment access
- Any system or service requiring authenticated user access

4. PASSWORD REQUIREMENTS

4.1 Minimum Password Length

- All passwords must be **at least 12 characters** in length
- Longer passwords (15+ characters) are encouraged for accounts with elevated privileges

4.2 Password Complexity

- Passwords must contain a mix of character types to enhance security
- Google Workspace enforces complexity requirements automatically
- Users should avoid using dictionary words, personal information, or predictable patterns

4.3 Password Refresh Cycle

- All users must change their passwords **every 182 days**
- Google Workspace will prompt users to change passwords before expiration
- System administrators may require immediate password changes if a security incident occurs

4.4 Password History and Reuse

- Users are **prohibited from reusing any of their last 5 passwords**
- This prevents users from rotating through a small set of known passwords
- Google Workspace enforces this restriction automatically

4.5 Account Lockout

- User accounts will be **automatically locked after 5 consecutive failed login attempts**
- Locked accounts must be unlocked by the CTO or designated IT administrator
- The lockout mechanism protects against brute-force password attacks
- Users experiencing account lockout should contact andres@vstream.ie

5. PASSWORD STORAGE AND TRANSMISSION

5.1 Password Storage

- Passwords must **never be stored in clear text**
- Google Workspace stores passwords using industry-standard hashing algorithms
- For ShineVR application databases, passwords are hashed before storage
- Encryption keys for password storage are managed via Google Cloud Key Management Service (KMS)

5.2 Password Transmission

- Passwords must only be transmitted over encrypted connections (SSL/TLS)
- Users must never send passwords via unencrypted email
- Initial passwords for new accounts are delivered via Google Workspace secure mechanisms

5.3 Password Sharing

- Users must **never share passwords** with other individuals
- Each user must have their own unique account credentials
- Shared accounts are prohibited except where specifically authorized by the CTO for technical system accounts

6. SPECIAL ACCOUNT TYPES

6.1 Privileged Accounts

- Accounts with administrative access to production systems, Google Cloud Platform, or ShineVR databases require additional security measures
- Multi-Factor Authentication (MFA) is **mandatory** for all privileged accounts
- Privileged account activity is logged and monitored

6.2 Service Accounts

- Service accounts used by ShineVR applications use API keys and tokens rather than passwords
- Service account credentials are stored in Google Cloud Key Management Service

- Service account access is restricted using the Principle of Least Privilege

6.3 Third-Party Supplier Accounts

- Third-party suppliers requiring system access must comply with this password policy
- Third-party accounts are reviewed and re-certified annually
- Accounts are immediately disabled when third-party contracts end

7. MULTI-FACTOR AUTHENTICATION (MFA)

- Multi-Factor Authentication is **mandatory** for:
    - All Google Cloud Platform access
    - All ShineVR production system access
    - All privileged administrative accounts
    - Remote access to Company systems
- MFA provides an additional security layer beyond passwords
- Users must enroll MFA devices during account setup

8. PASSWORD SECURITY BEST PRACTICES

Users must:

- Never write down passwords or store them in unencrypted files
- Never use the same password across multiple systems (work and personal)
- Be alert for phishing attempts requesting password disclosure
- Report suspected password compromise immediately to andres@vstream.ie
- Use password managers for personal accounts (recommended but not required)
- Log out of systems when leaving workstations unattended
- Lock screens (not just log out) when briefly stepping away

Users must not:

- Share passwords with colleagues, family, or third parties
- Use Company passwords for personal accounts
- Store passwords in browsers on shared computers
- Email passwords or send via unencrypted messaging
- Reuse old passwords
- Use easily guessable passwords (e.g., "Password123", company name, birthdates)

9. PASSWORD COMPROMISE AND INCIDENT RESPONSE

9.1 Suspected Compromise

If a user suspects their password has been compromised, they must:

1. Immediately change their password
2. Report the incident to the CTO (andres@vstream.ie)
3. Review recent account activity for unauthorised access

9.2 Confirmed Compromise

If password compromise is confirmed:

- The CTO will immediately disable the affected account
- A security incident will be logged in the Company's incident register
- Affected systems will be reviewed for unauthorized access
- The user will be issued new credentials after security review
- Additional security measures may be implemented

9.3 Monitoring for Compromised Credentials

- Google Cloud services monitor for compromised passwords or keys on Company VMs
- Security alerts for compromised credentials are sent via email and Slack
- The CTO reviews all compromise alerts and takes immediate action

10. ENFORCEMENT

10.1 Google Workspace Enforcement

All password requirements are technically enforced through Google Workspace settings:

- Minimum length enforcement
- Complexity requirements
- Password expiration (182 days)
- Password history (last 5 passwords)
- Account lockout (5 failed attempts)

10.2 Compliance Monitoring

- The CTO monitors password policy compliance through Google Workspace admin console
- Non-compliant accounts are identified and remediated
- Password policy effectiveness is reviewed annually

10.3 Policy Violations

- Failure to comply with this password policy may result in disciplinary action
- Repeated violations may result in termination of employment or contract
- Security incidents resulting from password policy violations will be investigated

11. EXCEPTIONS

Any exception to this policy must:

- Be requested in writing to the CTO
- Include business justification for the exception
- Be approved by the CTO in writing
- Be documented and reviewed at least annually

- Include compensating security controls where applicable

12. POLICY REVIEW

- This policy will be reviewed **annually** by the CTO
- Updates will be made to reflect:
    - Changes in security threats
    - New technological capabilities
    - Regulatory requirement changes
    - Lessons learned from security incidents
- All users will be notified of policy updates

13. RESPONSIBILITIES

Role	Responsibilities
CTO (Responsible Person)	Overall policy ownership; Google Workspace configuration; incident response; policy review; exception approval
All Users	Comply with password requirements; protect credentials; report compromised passwords; complete security awareness training
Line Managers	Ensure team members understand policy; monitor compliance; report violations
IT Administrators	Configure password enforcement; unlock accounts; monitor alerts; maintain audit logs

14. RELATED POLICIES

This policy should be read in conjunction with:

- Information Security Policy
- Access Management Process/Procedure
- Incident Management Policy and Procedure
- BYOD Policy (for personal device password requirements)

15. TRAINING AND AWARENESS

- All new employees receive password security training during induction
- Training covers this policy and password security best practices
- Annual refresher training is mandatory for all users
- Training completion is tracked and verified

16. CONTACT INFORMATION

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

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