Access Management process/procedure

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
Access Control	Security mechanisms that regulate who can view or use resources in a computing environment
Identity and Access Management (IAM)	Framework of policies and technologies ensuring the right individuals access the right resources at the right times for the right reasons
Principle of Least Privilege (POLP)	Security principle whereby users are granted only the minimum access rights necessary to perform their job functions
Role-Based Access Control (RBAC)	Method of restricting access based on the roles of individual users within an organisation
Multi-Factor Authentication (MFA)	Authentication method requiring two or more verification factors to gain access to a resource
Privileged Access	Special access or abilities beyond those of ordinary users, typically administrative access
Service Account	Special account used by applications and services (not human users) to interact with systems

1. POLICY STATEMENT

vStream Digital Media is committed to protecting Company and ShineVR systems and data through comprehensive access control measures. All access to systems and data is granted based on legitimate business needs, the principle of least privilege, and appropriate role-based controls.

This policy establishes requirements for managing the complete lifecycle of access rights—from initial provisioning through ongoing monitoring to ultimate revocation—to ensure that only authorised individuals and services can access Company resources. All access is logged, monitored, and regularly reviewed to prevent unauthorised access and ensure compliance with data protection requirements.

2. PURPOSE

The purpose of this policy is to:

- Ensure only authorised individuals and services have access to Company and ShineVR systems and data
- Implement the Principle of Least Privilege across all systems
- Define clear roles and responsibilities for access management
- Establish consistent procedures for granting, modifying, and revoking access
- Ensure proper authentication and authorisation mechanisms are implemented
- Require regular review and re-certification of access rights
- Protect personal data through appropriate access controls per GDPR requirements
- Enable audit and compliance through comprehensive access logging
- Prevent unauthorised access, data breaches, and insider threats

3. SCOPE

This policy applies to:

- **All users:**

  - Employees (permanent, temporary, contractors)
  - Third-party suppliers and service providers
  - Partners and collaborators
  - External auditors and consultants

- **All systems and resources:**

  - Google Cloud Platform infrastructure and services
  - ShineVR production, staging, and development environments
  - Cloud SQL databases
  - Cloud Storage buckets
  - Google Workspace (email, Drive, Calendar)
  - Source code repositories (GitHub/BitBucket)
  - Communication platforms (Slack)
  - Development and deployment tools
  - Administrative interfaces and consoles

- **All data:**
    - Customer data and personal information
    - ShineVR application data
    - Business confidential information
    - Employee personal data
    - System configurations and credentials

This policy covers the entire access lifecycle:

- Account creation and provisioning
- Authentication and authorisation
- Access modification and elevation
- Access monitoring and review
- Access suspension and termination

4. PRINCIPLE OF LEAST PRIVILEGE (POLP)

4.1 Core Principle

Mandatory Requirement: All users, applications, and systems are granted only the minimum access rights necessary to perform their legitimate functions.

Application of POLP:

- Users receive access only to systems and data required for their job role
- Access is role-based, not individual-based, where possible
- Temporary elevated access granted only when necessary and time-limited
- Access automatically removed when no longer needed
- Regular reviews ensure access remains appropriate and necessary
- "Default deny" approach: access denied unless explicitly granted

4.2 Need-to-Know Basis

Sensitive Data Access:

- Access to personal data restricted to those with legitimate business need
- Access to production systems limited to authorised operations and support staff
- Developers do not have access to production customer data
- Source code access granted based on project involvement
- Financial data access restricted to finance team and senior management
- Security credentials and encryption keys restricted to CTO and designated personnel

4.3 Separation of Duties

Critical Separations:

- **Development vs. Production:** Developers cannot access production environment directly
- **Code Development vs. Deployment:** Code review and approval required before production deployment

- **Security Administration vs. Business Operations:** Security controls managed separately from business functions
- **Data Entry vs. Approval:** Where applicable, different individuals perform data entry and approval

5. ROLE-BASED ACCESS CONTROL (RBAC)

5.1 Standard Access Roles

The Company implements role-based access control with four standard roles:

5.1.1 User Role

Access Level: Limited, read-only or specific function access

Typical Permissions:

- Access to specific applications or data required for job function
- Read-only access to shared resources
- Ability to modify only own data or assigned records
- No administrative capabilities
- No access to system configurations or sensitive data

Examples:

- Developer accessing development environment
- Employee accessing own Google Workspace data
- Contractor accessing specific project resources

Assignment Criteria:

- Standard employees in non-administrative roles
- External parties requiring limited access
- Service accounts with minimal required permissions

5.1.2 Manager Role

Access Level: Moderate, read/write access to specific resources

Typical Permissions:

- Read/write access to departmental or project resources
- Ability to view reports and analytics
- Access to team management functions
- Approval capabilities for specific workflows
- No system administration capabilities

Examples:

- Product Manager accessing ShineVR application configurations
- Department manager accessing team resources
- Project lead accessing project data and documentation

Assignment Criteria:

- Managers with team or project oversight responsibilities
- Individuals requiring broader data access for decision-making
- Roles requiring approval capabilities

5.1.3 Admin Role

Access Level: High, administrative access to specific systems or projects

Typical Permissions:

- Administrative access within specific Google Cloud projects
- Ability to configure system settings and integrations
- User management within assigned scope
- Access to logs and monitoring data
- Deploy applications to non-production environments
- Manage resources within assigned projects

Examples:

- Backend Developer administering development environment
- Team Lead managing staging environment
- DevOps engineer managing CI/CD pipelines

Assignment Criteria:

- Technical staff requiring administrative capabilities
- Roles responsible for system configuration and management
- Requires CTO approval and technical justification

5.1.4 SuperAdmin Role

Access Level: Full administrative access across all systems and projects

Typical Permissions:

- Full access to all Google Cloud Platform resources
- Ability to create, modify, and delete any resource
- Access to all environments (development, staging, production)
- IAM policy management across all projects
- Security configuration and encryption key management
- Billing and cost management
- Audit log access

Examples:

- CTO (Andrés Pitt)
- Designated backup administrator (if appointed)

Assignment Criteria:

- CTO role automatically assigned SuperAdmin
- Emergency backup SuperAdmin only if absolutely necessary

- Requires CEO approval for any SuperAdmin beyond CTO
- Annual re-certification required

5.2 ShineVR Application Roles

Application-Level RBAC: In addition to infrastructure roles, ShineVR applications implement application-specific roles:

Role	Permissions	Use Case
User	Access own data, view assigned content	End users, trial participants
Manager	Access team data, configure content	Clinical supervisors, team leads
Admin	Configure application, manage users, view all data	Application administrators
SuperAdmin	Full application control, system configuration	CTO, designated application owner

Route-Level Access Control:

- Application routes guarded by role requirements
- Automated testing includes role-based access tests (part of 400+ test suite)
- Access tests verify resources cannot access beyond their assigned role
- Failed access tests block code deployment

5.3 Role Assignment and Approval

Assignment Process:

1. **Request:** User's manager or requester submits access request with business justification
2. **Review:** CTO (or designated approver) reviews request for appropriateness
3. **Approval:**
    - User/Manager roles: Department manager approval
    - Admin roles: CTO approval required
    - SuperAdmin roles: CEO and CTO approval required
4. **Provisioning:** IT/CTO provisions access per approved request
5. **Notification:** User notified of access granted
6. **Documentation:** Access recorded in access register

Required Documentation:

- User name and contact information
- Role requested (User, Manager, Admin, SuperAdmin)
- Systems and resources requiring access
- Business justification
- Duration of access (if temporary)
- Approver name and approval date

- Date access provisioned

6. GOOGLE CLOUD IAM (IDENTITY AND ACCESS MANAGEMENT)

6.1 Google Cloud IAM Framework

Primary Access Control Mechanism: All access to Google Cloud Platform resources controlled via **Google Cloud IAM**

IAM Components:

- **Identity:** Who is making the request (user, service account, Google group)
- **Role:** Collection of permissions (predefined or custom)
- **Policy:** Binding of identities to roles on specific resources

6.2 Google Cloud IAM Policies

Policy Structure:

- IAM policies defined at project, folder, or organisation level
- Policies bind identities (users, service accounts) to roles
- Roles grant specific permissions to resources
- Policies inherited hierarchically (organisation → folder → project → resource)

Policy Management:

- All IAM policies defined in Infrastructure-as-Code
- Policy changes require code review and approval
- Production policies modifiable only by CTO
- Automated testing of IAM policies before deployment
- Policies audited quarterly for compliance

6.3 Google Cloud Roles

Predefined Roles Used:

- **Viewer:** Read-only access to resources
- **Editor:** Read and write access to resources
- **Owner:** Full control including access management
- **Custom Roles:** Tailored permissions for specific needs

Role Assignment Strategy:

- Use predefined roles where possible for simplicity
- Create custom roles only when predefined roles too permissive
- Document all custom roles with justification
- Regular review of custom roles for continued necessity

6.4 Service Account Management

Service Accounts for Automated Access:

- Applications and services use service accounts (not user credentials)
- Each service account assigned minimum required permissions
- Service account keys rotated annually minimum
- Service account keys stored in Google Secret Manager
- Service account activity logged and monitored

Service Account Security:

- Service accounts named descriptively (purpose, application, environment)
- No shared service account keys between applications
- Service account impersonation used where possible instead of key export
- Unused service accounts disabled and deleted
- Service account compromise triggers immediate key rotation and investigation

7. AUTHENTICATION REQUIREMENTS

7.1 User Authentication

Primary Authentication: Google Workspace Accounts

- All employees authenticate via Google Workspace accounts
- Google Workspace provides single sign-on (SSO) for Company services
- Authentication integrated with Google Cloud Platform IAM
- Centralised user lifecycle management

Authentication Standards:

- Strong passwords required (minimum 12 characters, per Password Policy)
- Password expiry every 90 days
- Account lockout after 5 failed attempts
- Session timeouts enforced (12 hours maximum, shorter for privileged access)

7.2 Multi-Factor Authentication (MFA)

Mandatory MFA Requirements:

Must Use MFA:

- **All Google Cloud Platform access (mandatory, no exceptions)**
- **All privileged administrative accounts (mandatory)**
- **Remote access to Company systems (mandatory)**
- **Access to production environments (mandatory)**
- Recommended for all Google Workspace accounts

Approved MFA Methods:

- **Google Authenticator** (time-based one-time password)
- **Hardware security keys** (FIDO U2F/WebAuthn - preferred for high-risk roles)
- **Google Prompts** (push notification to registered device)
- **SMS** (acceptable but less preferred due to security concerns)

MFA Enrollment:

- MFA enrollment required during account creation
- Users cannot access protected systems until MFA enrolled
- MFA backup codes generated and securely stored
- Lost MFA devices reported immediately to CTO for reset

MFA Monitoring:

- MFA compliance monitored via Google Workspace admin console
- Non-compliant accounts identified and remediated
- MFA bypass attempts logged and investigated
- Regular audits of MFA enrollment and usage

7.3 Service Account Authentication

API Keys and Service Credentials:

- Service accounts use API keys or OAuth tokens
- Keys generated via Google Cloud IAM
- Keys stored in Google Secret Manager (never in source code)
- Keys injected at runtime, not stored on disk
- Key compromise triggers immediate rotation

8. ACCESS PROVISIONING

8.1 New User Onboarding

Access Provisioning Process:

Day 1 (Account Creation):

1. Google Workspace account created by CTO or HR
2. Initial password set and communicated securely
3. User forced to change password on first login
4. MFA enrollment required before system access
5. Basic access granted (email, calendar, drive)

Week 1 (Role-Based Access):

1. Manager submits access request for required systems
2. CTO reviews and approves access request
3. Access provisioned based on role assignment
4. User added to appropriate Google Groups for resource access
5. User notified of access granted

Onboarding Documentation:

- New user receives Information Security Policy
- Security awareness training mandatory during first week
- Access responsibilities and acceptable use explained
- Incident reporting procedures communicated

8.2 Role Change or Transfer

Access Modification Process: When employee changes roles:

1. Manager notifies CTO of role change
2. Current access reviewed and documented
3. New access requirements identified
4. Unnecessary access revoked immediately
5. New access provisioned based on new role
6. Access change logged and documented

Systematic Review and Re-Certification:

- Access rights systematically reviewed when internal role changes occur
- Line managers responsible for certifying access appropriateness
- Access re-certified within 5 business days of role change
- Old access not required for new role revoked immediately

8.3 Temporary or Elevated Access

Temporary Access Grants: For time-limited access needs (projects, consulting, audits):

- Clearly defined start and end dates
- Access automatically expires on end date
- Reminder sent to approver before expiry for renewal decision
- Access logged as temporary in access register
- Enhanced monitoring of temporary access usage

Elevated Privilege Access: For tasks requiring temporary elevated privileges:

- "Break glass" procedure for emergencies requiring immediate SuperAdmin access
- Elevated access granted only for specific task duration
- Detailed logging and monitoring of elevated access activities
- Access revoked immediately upon task completion
- All elevated access activities reviewed by CTO

9. ACCESS MONITORING AND LOGGING

9.1 Access Logging

Comprehensive Logging:

- All authentication attempts (successful and failed) logged
- All access to systems and data logged via Google Cloud Audit Logs
- All privileged actions logged
- All IAM policy changes logged
- All service account usage logged
- All data access logged (where applicable)

Log Retention:

- Audit logs retained for minimum 1 year
- Compliance-critical logs retained for 7 years
- Logs stored securely with encryption
- Log access restricted to CTO and authorised security personnel
- Logs protected from modification or deletion

9.2 Access Monitoring

Automated Monitoring:

- Failed authentication attempts trigger alerts (threshold: 3 failed attempts within 5 minutes)
- Unusual access patterns detected and alerted
- Access from unexpected locations flagged
- After-hours access by privileged accounts monitored
- Concurrent sessions from different locations investigated
- Service account key usage monitored for anomalies

Alert Channels:

- Email notifications to CTO
- Slack alerts to security monitoring channel
- Google Cloud Console notifications
- Integration with Google Cloud Security Command Centre

9.3 Automated Access Testing

Continuous Access Control Validation:

- **400+ automated tests** include access control tests
- Tests explicitly verify role-based access restrictions
- Tests confirm resources cannot access beyond assigned permissions
- Failed access control tests block code deployment
- Tests run on every code change (before deployment)
- Test results logged and reviewed

Access Test Examples:

- User role cannot access Admin functions
- Manager role cannot access SuperAdmin functions
- Service accounts cannot access resources outside scope
- Anonymous users cannot access authenticated resources
- Specific routes accessible only by designated roles

10. ACCESS REVIEWS AND RE-CERTIFICATION

10.1 Regular Access Reviews

Quarterly Access Review (Systematic): Conducted by CTO every quarter:

- Review all IAM policies across all Google Cloud projects
- Review all role assignments in ShineVR applications

- Review all service account permissions
- Identify unused or excessive permissions
- Revoke access no longer required
- Document review results and actions taken

Annual Comprehensive Access Audit: Conducted annually:

- Complete inventory of all user accounts
- Complete inventory of all service accounts
- Verification of role assignments against job functions
- Review of access granted vs. access used
- Identification of dormant accounts
- Certification of access appropriateness by managers
- Update access documentation

10.2 Event-Driven Access Reviews

Immediate Review Triggers:

- **Employee departure:** Access reviewed and revoked same day
- **Role change:** Access reviewed within 5 business days
- **Security incident:** All related access reviewed immediately
- **System compromise:** All access to affected systems reviewed
- **Policy violation:** User's access reviewed and potentially restricted
- **Extended absence:** Access suspended after 90 days of inactivity

10.3 Manager Certification

Line Manager Responsibilities:

- Managers certify access appropriateness for their team members
- Certification required:
    - Upon role changes
    - Annually for all team members
    - When access privilege requested or modified
- Managers accountable for access granted to their teams
- Non-responsive managers escalated to senior management

11. ACCESS REVOCATION

11.1 User Departure

Immediate Actions (Same Day):

1. **Suspend Google Workspace account** (within 2 hours of departure notification)
2. **Revoke Google Cloud Platform access** (IAM policies)
3. **Disable service accounts** specific to departing user
4. **Rotate credentials** accessed by departing user (if applicable)
5. **Revoke application access** (ShineVR admin accounts, etc.)
6. **Remove from Google Groups** and mailing lists

Within 24 Hours:

1. **Transfer data ownership** to manager (Google Drive, emails)
2. **Document all access revoked** in user departure log
3. **Archive user data** per data retention policy
4. **Collect company equipment** (if applicable)
5. **Exit interview** including return of credentials, keys, badges

Within 7 Days:

1. **Delete Google Workspace account** (after data transferred)
2. **Remove from all external systems** (Slack, GitHub, etc.)
3. **Update documentation** removing user from team lists, contact lists
4. **Final access review** confirming all access revoked

11.2 Contractor or Vendor Access Termination

End of Contract/Engagement:

- Access revoked on contract end date (or earlier if work completed)
- Vendor access removed within 24 hours of contract termination
- Temporary accounts deleted after 30-day grace period
- All vendor-generated credentials rotated
- Vendor access termination logged and verified

11.3 Emergency Access Suspension

Immediate Suspension Scenarios:

- Security incident involving user account
- Suspected account compromise
- Policy violation or malicious activity
- Legal or HR investigation requiring access restriction
- Lost or stolen device containing credentials

Emergency Suspension Process:

1. **Immediate:** Suspend Google Workspace account (within minutes)
2. **Within 1 hour:** Revoke all system access
3. **Within 4 hours:** Notify user and HR/management
4. **Within 24 hours:** Document incident and rationale
5. **Ongoing:** Review decision daily until investigation complete

12. DORMANT AND INACTIVE ACCOUNTS

12.1 Dormant Account Detection

Monitoring for Inactive Accounts:

- Google Workspace admin console tracks last login dates
- Google Cloud IAM tracks last activity for service accounts
- Automated reports of accounts inactive for 60+ days
- Monthly review of dormant accounts

12.2 Dormant Account Management

Dormant Account Process:

- **60 days inactive:** User contacted to confirm continued need
- **90 days inactive:** Account suspended (access disabled)
- **120 days inactive:** Account scheduled for deletion
- **180 days inactive:** Account deleted (data archived per retention policy)

Exceptions:

- Accounts for seasonal workers (documented and approved)
- Accounts for employees on extended leave (maternity, medical)
- Service accounts for scheduled/batch processes (minimal activity expected)

Reactivation:

- Suspended accounts reactivated upon user request and manager confirmation
- Reactivation requires business justification
- Access reviewed and right-sized before reactivation

13. PRIVILEGED ACCESS MANAGEMENT

13.1 Privileged Account Security

Enhanced Security for Privileged Accounts:

- **Mandatory MFA:** No exceptions for privileged accounts
- **Hardware security keys** preferred for SuperAdmin accounts
- **Separate accounts:** Consider separate admin accounts for privileged activities
- **Session recording:** Privileged sessions logged in detail
- **Just-in-time access:** Temporary elevation instead of permanent privileged access where possible

13.2 Privileged Access Monitoring

Enhanced Monitoring:

- All privileged actions logged and reviewed
- Privileged account activity monitored in real-time
- Unusual privileged activity triggers immediate alerts
- Weekly review of privileged account usage
- Privileged access audit trail maintained indefinitely

13.3 Emergency "Break Glass" Access

Emergency Access Procedures: For emergencies requiring immediate SuperAdmin access when CTO unavailable:

1. **Break glass account** (emergency SuperAdmin) kept disabled
2. **Activation:** Requires physical security key and CTO notification

3. **Logging:** All break glass account activity logged separately
4. **Review:** All break glass usage reviewed within 24 hours
5. **Deactivation:** Account disabled immediately after emergency resolved

14. WIRELESS NETWORK ACCESS

14.1 Company Wireless Network Security

Wireless Security Standards:

- Company wireless network uses **WPA2** encryption (minimum)
- **WPA3** preferred where supported by devices
- Strong pre-shared key (PSK) - minimum 16 characters
- PSK changed every 6 months
- Guest network separated from corporate network (if implemented)

Network Access Control:

- Corporate wireless network for employees only
- Guest wireless network for visitors (no access to internal resources)
- Guest network credentials expire after 24 hours
- Guest network usage logged

Important Context:

- Company wireless network primarily for internet access
- **No data hosted at Company premises** - all data on Google Cloud
- Wireless network security important but not critical to data protection
- All sensitive data access via encrypted cloud connections (HTTPS, TLS)

15. REMOTE ACCESS AND HOMEWORKING

15.1 Remote Access Security

Remote Work Access:

- All remote access via Google Workspace accounts
- Google Cloud Platform access via web console (HTTPS)
- **MFA mandatory** for remote access
- **Two-factor authentication enabled** on Google Workspace accounts
- VPN not currently required (cloud-native infrastructure)

Remote Work Data Security:

- Files stored in Google Drive (not local devices)
- Access to production systems same as on-premise access
- BYOD policy applies to personal devices used for remote work
- Remote work security covered in BYOD Policy and this policy

15.2 Home Network Security

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 work without VPN
- See BYOD Policy for detailed home network security requirements

16. THIRD-PARTY ACCESS

16.1 Third-Party Access Policy

General Prohibition: Third parties do not have direct access to production environments except as detailed below.

Permitted Third-Party Access:

- **Google Cloud support:** Via support ticket system for troubleshooting
- **External auditors:** Time-limited, supervised access for audit purposes
- **Security consultants:** Emergency incident response only, CTO-approved
- **Vendors:** Only if absolutely necessary, limited scope, time-limited

16.2 Third-Party Access Requirements

All third-party access must:

- Be requested in writing with business justification
- Be approved by CTO
- Be limited to minimum necessary scope
- Be time-limited (typically 24-48 hours, maximum 7 days)
- Use unique third-party accounts (not shared with employees)
- Be fully logged and monitored
- Be supervised where possible
- Be reviewed and deactivated immediately after purpose completed

Third-Party Access Documentation:

- Third-party name and company
- Purpose of access
- Systems/data accessed
- Duration of access
- Approval details
- Supervision arrangements
- Access deactivation confirmation

17. DATA ACCESS CONTROLS

17.1 Data Classification and Access

Access Based on Data Sensitivity:

- Personal data access restricted per GDPR requirements
- Sensitive personal data (health data) requires additional justification
- Customer data access logged and monitored
- Production data inaccessible from development environments

ShineVR Data Access:

- ShineVR uses anonymised data (16-digit random codes)
- ShineVR cannot link codes to identifiable individuals
- Customer maintains data linkage as Data Controller
- Trial data ringfenced for easy deletion at contract end

17.2 Database Access Controls

Cloud SQL Database Access:

- Database access via private IP addresses only (no public access)
- SSL/TLS required for all database connections
- Database users assigned minimum required privileges
- Application databases accessed via service accounts
- Direct database access for troubleshooting requires CTO approval
- All database queries logged

17.3 Storage Access Controls

Cloud Storage Bucket Access:

- Bucket-level IAM policies restrict access
- Object-level access control where required
- Separate buckets for different data classifications
- Public access blocked by default
- Signed URLs for temporary external access
- All access logged via Cloud Audit Logs

18. SEGREGATION OF ENVIRONMENTS

18.1 Environment Separation

Mandatory Separation:

- **Development, Test, Staging, and Production environments completely separated**
- Separate Google Cloud projects for each environment
- Separate databases with different credentials
- Separate IAM policies and access controls

- Separate encryption keys
- Different network configurations

18.2 Environment-Specific Access

Access Restrictions:

- **Developers:** Full access to Development environment only
- **Product Manager & CTO:** Access to Staging environment
- **CTO and designated production staff:** Production environment access only
- **No cross-environment access:** Developers cannot access production data
- Service accounts specific to each environment (no shared credentials)

18.3 Data Segregation

Production Data Protection:

- Production data never copied to development or test environments
- Test data synthetic or anonymised (no real customer PII)
- Sanitisation processes for any production data used in non-production (rare exceptions)
- Data export from production requires CTO approval

19. INCIDENT RESPONSE

19.1 Access-Related Incidents

Incidents Requiring Immediate Action:

- Unauthorised access attempts or breaches
- Account compromise or credential theft
- Privilege escalation attempts
- Unusual access patterns or data exfiltration
- Lost or stolen credentials
- Insider threat indicators

Incident Response:

1. **Immediate:** Suspend affected accounts
2. **Within 1 hour:** Assess scope and impact
3. **Within 4 hours:** Contain incident and prevent further access
4. **Within 24 hours:** Investigate root cause
5. **Within 72 hours:** Remediate and restore normal operations
6. **Within 1 week:** Post-incident review and lessons learned

See **Incident Response Plan** for detailed procedures.

19.2 Compromised Credential Response

If credentials compromised:

1. **Immediate:** Force password reset for affected user
2. **Immediate:** Revoke all active sessions

3. **Within 1 hour:** Rotate service account keys if applicable
4. **Within 4 hours:** Review access logs for unauthorised activity
5. **Within 24 hours:** Assess data exposure and breach notification requirements
6. **Ongoing:** Enhanced monitoring for 30 days

20. COMPLIANCE AND AUDIT

20.1 Access Control Compliance

Regulatory Compliance:

- GDPR Article 32 requires appropriate access control measures
- ISO 27001 requires documented access control policy
- Access controls support data protection by design and default
- Audit trails enable compliance demonstration

20.2 Access Audit Support

Audit Evidence:

- Access register and role assignments
- IAM policies and configurations
- Access review and re-certification records
- Access logs and monitoring reports
- Incident response records for access incidents
- Training records for access management

Audit Procedures:

- Quarterly internal access audits
- Annual comprehensive access review
- External audits supported with documentation
- Audit findings tracked and remediated

21. ROLES AND RESPONSIBILITIES

Role	**Responsibilities**
CTO (Responsible Person)	Overall access management policy ownership; approve Admin/SuperAdmin access; manage Google Cloud IAM; conduct quarterly access reviews; respond to access incidents; monitor privileged access; enforce POLP; audit access controls
Line Managers	Request access for team members; certify access appropriateness; notify CTO of role changes; review team access annually; ensure departing staff access revoked; approve User/Manager access requests

Role	Responsibilities
IT Administrators	Provision and revoke access per approvals; configure IAM policies; monitor access logs; respond to access incidents; maintain access documentation; assist with access reviews
All Users	Protect credentials; report suspected compromise; comply with access policies; use only authorised systems and data; report unusual access activity; complete security training

22. TRAINING AND AWARENESS

22.1 Access Management Training

Required Training:

- **All employees:** Access management awareness during onboarding
- **Managers:** Access request and approval procedures
- **Technical staff:** IAM configuration and access control implementation
- **All users:** Annual security awareness including access responsibilities

Training Topics:

- Access management principles (POLP, RBAC)
- How to request access appropriately
- Password security and MFA usage
- Recognising and reporting access incidents
- Data classification and appropriate access
- Consequences of policy violations

23. EXCEPTIONS

23.1 Exception Process

Exceptions to access management requirements may be requested for:

- Emergency situations requiring immediate access
- Technical limitations preventing standard access controls
- Unique circumstances requiring non-standard access

All exceptions must:

- Be requested in writing to CTO with detailed justification
- Document compensating controls
- Be approved in writing by CTO (CEO approval for SuperAdmin exceptions)
- Be time-limited and reviewed monthly
- Be documented in access exception register

24. POLICY REVIEW AND UPDATES

This policy will be reviewed:

- **Annually:** Comprehensive review by CTO
- **After security incidents:** Update based on lessons learned
- **Technology changes:** New systems or access control capabilities
- **Regulatory changes:** GDPR or compliance requirement updates
- **Organisational changes:** New roles, departments, or business functions

25. RELATED POLICIES

This policy should be read in conjunction with:

- Information Security Policy
- Password Policy
- Cloud Security Policy
- BYOD Policy
- Incident Response Plan
- Data Protection Policy
- Vendor Management Policy

26. CONTACT INFORMATION

For questions regarding this policy or to report access control incidents:

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