Background Check Policy

vStream Digital Media

Last updated 03/02/25

1. Definitions

Term	Definition
Background Check	A comprehensive verification process to confirm the identity, qualifications, employment history, and suitability of individuals before granting access to vStream systems, facilities, or sensitive information.
Identity Verification	The process of confirming that an individual is who they claim to be through review of government-issued identification documents and other authoritative sources.
Staged Access	A phased approach to granting system access where new employees initially receive limited access (development and staging environments only) until background checks are completed, after which production access may be granted.
Production Access	The ability to access, modify, or manage live production systems including the ShineVR application, customer data, production databases, and Google Cloud Platform production resources.
Sensitive Data	Information requiring enhanced protection including personal data, healthcare information (such as ShineVR trial data), intellectual property, authentication credentials, and business confidential information.

Right to Work	Legal authorisation to work in Ireland, verified through passport, visa, work permit, or other documentation as required by Irish employment law.

2. Policy Statement

vStream Digital Media is committed to protecting customer data, business assets, and maintaining the trust of healthcare customers. Background checks are a critical security control that helps ensure only trustworthy, verified individuals gain access to sensitive systems and information, particularly production environments hosting the ShineVR healthcare application.

All employees and contractors with access to vStream systems must undergo appropriate background verification before being granted production access. This policy establishes comprehensive requirements for identity verification, reference checks, employment verification, and staged access provisioning to minimise insider threat risks and comply with customer security requirements.

Background checks are conducted in compliance with Irish data protection law, GDPR, and employment regulations. All information collected is handled confidentially and used solely for employment screening and security purposes.

3. Purpose

The purpose of this policy is to:

- Verify the identity and credentials of individuals before granting access to production systems
- Minimise insider threat risks by screening for potential security concerns
- Protect customer data, particularly sensitive healthcare information in ShineVR applications
- Ensure compliance with healthcare customer security requirements
- Confirm right to work in Ireland and employment eligibility
- Verify qualifications and employment history relevant to role requirements
- Demonstrate due diligence in personnel security for regulatory compliance and customer audits

4. Scope

This policy applies to:

- All new permanent employees regardless of role or seniority
- All contractors and consultants requiring access to vStream systems
- Temporary staff with system access or handling sensitive information
- Re-screening when employees change roles requiring elevated access
- Periodic re-verification for employees with production access (every 3 years)

5. Background Check Requirements

5.1 Identity Verification

Comprehensive identity verification is required for all new hires:

- **Government-Issued Photo ID:** Passport, national identity card, or driving licence. Must be current and not expired
- **Proof of Address:** Utility bill, bank statement, or official correspondence dated within last 3 months
- **PPS Number:** Personal Public Service Number for Irish residents, required for employment records
- **Right to Work:** Passport with work visa or EU/EEA citizenship documentation. Verified and photocopied for HR records
- **Document Verification:** Original documents inspected in person (not photocopies). Certified copies retained in employee file
- **Digital Verification:** For remote employees, identity verified via video call with live document inspection plus third-party identity verification service where appropriate

5.2 Employment History Verification

Verification of employment history for the most recent 5 years or 2 previous employers (whichever is greater):

- **Direct Contact:** Contact previous employers directly (not through candidate) to verify employment dates, job title, and responsibilities
- **Employment Gaps:** Gaps exceeding 3 months must be explained and verified where possible
- **Contractor Verification:** For contractors or self-employed individuals, verify through client references or contract documentation
- **Documentation:** Written confirmation from employers or reference letters on company letterhead. Notes from phone verification calls retained

5.3 Professional References

Minimum two professional references required:

- **Reference Sources:** Previous managers, supervisors, or professional colleagues who can attest to work performance and character
- **Recent References:** At least one reference from within the last 2 years
- **Direct Contact:** References contacted directly by vStream (phone or email). Contact details verified independently
- **Reference Questions:** Work performance, reliability, trustworthiness, technical competence, and reason for leaving previous employment
- **Red Flags:** Inability to provide references, negative feedback regarding honesty or security, or contradictions with candidate statements require further investigation

5.4 Education and Qualification Verification

For roles requiring specific qualifications:

- **Degree Verification:** For technical roles (developers, CTO), verify relevant degrees through institutions or diploma supplements
- **Professional Certifications:** Verify relevant technical certifications (e.g., Google Cloud certifications, security certifications) through issuing bodies
- **Original Certificates:** Review original or certified copies of qualifications. Photocopies retained in employee file
- **International Qualifications:** For non-Irish qualifications, verify through appropriate recognition bodies or directly with issuing institutions

5.5 Criminal Record Checks

While not mandatory for all roles, criminal record checks may be conducted:

- **Scope:** Conducted through the Garda National Vetting Bureau for Irish residents or equivalent authority for non-Irish nationals
- **Consent Required:** Written consent obtained from candidate before requesting vetting
- **Risk-Based Approach:** Prioritised for roles with elevated access (SuperAdmin, database admin) or customer requirement
- **Evaluation:** Findings assessed on case-by-case basis considering nature of offence, time elapsed, relevance to role, and rehabilitation
- **Confidentiality:** Vetting results handled with strict confidentiality. Access limited to CTO and hiring manager

6. Staged Access Approach

vStream implements a staged approach to system access as a security control while background checks are in progress:

6.1 Initial Access (Day 1)

New employees receive limited access on their first day:

- **Development Environment:** Full access to development systems and non-production Google Cloud Platform resources
- **Staging Environment:** Access to staging systems for testing and pre-production validation
- **Google Workspace:** Email, calendar, chat, and collaboration tools
- **Documentation:** Access to internal documentation, policies, and training materials
- **Source Code:** Read/write access to code repositories for development work
- **No Production Access:** Explicitly denied access to production systems, live customer data, production databases, and ShineVR production application

6.2 Production Access (After Verification)

Production access granted only after successful completion of background checks:

- **Verification Complete:** Identity verification, employment history, references, and qualifications all confirmed
- **CTO Approval:** CTO reviews background check results and approves production access
- **Typical Timeline:** 2-4 weeks from start date depending on reference response times
- **Role-Based Access:** Production access granted based on job role (User, Manager, Admin, or SuperAdmin)
- **Audit Trail:** Production access grants logged with date, approver, and justification

6.3 Rationale for Staged Access

The staged access approach provides multiple security benefits:

- **Risk Mitigation:** Prevents unverified individuals from accessing sensitive customer data and production systems
- **Insider Threat Protection:** Reduces risk window for potential insider threats during verification period
- **Healthcare Compliance:** Meets healthcare customer requirements for personnel screening before accessing patient data
- **Productivity Balance:** Allows new employees to be productive in development and staging while verification progresses
- **Defence in Depth:** Adds additional security layer beyond technical access controls

7. Background Check Process and Timeline

7.1 Pre-Employment Phase

Background check process initiated during recruitment:

- **Job Offer Stage:** Conditional offer made subject to satisfactory background checks
- **Candidate Notification:** Candidate informed of background check requirements and process
- **Consent Forms:** Candidate completes consent forms for reference checks, employment verification, and vetting if applicable
- **Document Collection:** Candidate provides required identification documents, qualification certificates, and reference contact information
- **Right to Work:** Legal right to work in Ireland verified before employment commencement

7.2 Post-Employment Phase

Verification continues after employee starts:

- **Week 1:** Identity documents verified in person, employment verification requests sent to previous employers, reference checks initiated
- **Weeks 2-3:** Follow up on outstanding verifications, chase delayed reference responses, review and evaluate all collected information
- **Week 4:** CTO reviews complete background check file and approves production access if all checks satisfactory
- **Delays:** If verification delayed beyond 4 weeks due to slow reference responses, employee continues with development/staging access only until verification complete

7.3 Documentation and Record Keeping

- **Employee File:** Confidential employee file maintained with all background check documentation
- **File Contents:** Copies of identification documents, reference check notes, employment verification confirmations, qualification certificates, consent forms, and CTO approval for production access
- **Access Restrictions:** Employee files accessible only to CTO and HR personnel with legitimate business need
- **Retention:** Background check records retained for duration of employment plus 7 years after termination for audit and legal purposes
- **GDPR Compliance:** All personal data collected during background checks processed in accordance with GDPR and Irish Data Protection Act

8. Handling Adverse Findings

If background checks reveal concerning information:

8.1 Assessment Process

- **Individual Review:** Each adverse finding assessed individually considering nature, severity, relevance to role, and time elapsed
- **Candidate Discussion:** Opportunity for candidate to explain circumstances and provide additional context
- **CTO Decision:** CTO makes final determination on suitability for employment or production access
- **Documentation:** Assessment rationale and decision documented in employee file

8.2 Possible Outcomes

- **Employment Continuation:** Minor issues or satisfactorily explained concerns may result in continued employment with production access
- **Limited Access:** Moderate concerns may result in continued employment but restricted to development/staging access permanently
- **Enhanced Monitoring:** Additional oversight or restrictions applied based on nature of concerns
- **Employment Termination:** Serious findings (e.g., falsified credentials, material misrepresentation, relevant criminal convictions) may result in withdrawal of job offer or termination of employment

9. Periodic Re-Verification

Background checks are refreshed periodically for ongoing assurance:

- **3-Year Cycle:** Employees with production access undergo re-verification every 3 years
- **Scope:** Lighter touch than initial checks - identity confirmation, continued right to work, and reference from current supervisor
- **Role Changes:** Additional verification when employees promoted to SuperAdmin or roles with elevated privileges
- **Continuous Monitoring:** Employees expected to self-report changes affecting background check status (e.g., criminal charges, right to work expiry)
- **Customer Requirements:** More frequent re-verification if required by specific customer contracts.

10. Contractor and Third-Party Requirements

Contractors and third parties with system access are subject to background check requirements:

- **Same Standards:** Contractors undergo same background verification as employees including identity verification and staged access
- **Contracting Company Verification:** If provided through contracting company, verify that company has conducted appropriate background checks
- **Short-Term Access:** For very short engagements (under 1 month), may grant development/staging access only without production access
- **Contract Terms:** Contractor agreements include background check requirements and right to terminate for adverse findings

11. Data Protection and Privacy

Background check processing complies with GDPR and Irish data protection law:

- **Legal Basis:** Processing necessary for employment purposes and legitimate interests in security and fraud prevention
- **Transparency:** Candidates informed of background check process, data collected, and how it will be used
- **Consent:** Written consent obtained before conducting reference checks, employment verification, and criminal record checks
- **Data Minimisation:** Only information necessary for employment screening purposes collected and retained
- **Confidentiality:** Background check information handled confidentially with access restricted to authorised personnel only
- **Subject Rights:** Candidates have right to access background check information and request corrections if inaccurate

- **Retention Limits:** Background check data retained only as long as necessary for employment purposes and legal requirements

12. Integration with Overall Security Programme

Background checks are part of vStream's comprehensive personnel security:

- **Defence in Depth:** Background checks complement technical security controls (MFA, access controls, monitoring) and policy controls (training, acceptable use)
- **Access Management:** Background check status considered in access provisioning decisions per Access Management Policy
- **Security Training:** All employees receive security awareness training after background checks complete
- **Incident Response:** Background check documentation available to incident response team if insider threat investigation required
- **Continuous Monitoring:** Automated monitoring (Security Command Centre, log analysis) provides ongoing oversight even after background checks complete

13. Roles and Responsibilities

13.1 Chief Technology Officer

- Overall responsibility for background check policy and procedures
- Review and approval of all background check results
- Decision authority on production access based on background check outcomes
- Assessment of adverse findings and employment suitability
- Data Protection Officer responsibilities for background check data processing

13.2 Hiring Managers

- Initiate background check process during recruitment
- Collect required documents and information from candidates
- Conduct reference checks and employment verification
- Maintain confidential employee background check files

13.3 All Employees

- Provide accurate and complete information during background check process
- Cooperate with verification requests and provide required documentation
- Report changes in circumstances affecting background check status (e.g., right to work expiry)

14. Related Policies and Documents

- Information Security Policy
- Access Management Policy
- BYOD Policy
- Acceptable Use Policy

15. Contact Information

Data Protection Officer / Chief Technology Officer:

Andrés Pitt

Email: andres@vstream.ie

Phone: (086) 788 6570

Company Address:

vStream Digital Media
37 Leeson Close
Dublin 2, D02 H344
Ireland
Website: vstream.ie