Incident Management process / procedure

vStream Digital Media

Last updated 03/02/25

1. Definitions

Term	Definition
Security Incident	Any event that could compromise the confidentiality, integrity, or availability of vStream information assets, including data breaches, unauthorised access, system compromises, malware infections, denial of service attacks, and significant security policy violations.
Data Breach	A security incident resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.
Incident Response Team	The team responsible for managing security incidents, typically including the CTO, CPO, backend developers, and Account Director for customer communication.
Containment	Actions taken to prevent an incident from spreading or causing additional damage while investigation and remediation activities are underway.
Root Cause Analysis	Systematic investigation to identify the fundamental cause of an incident, distinguishing from symptoms or contributing factors.

Post-Incident Review	A structured review conducted after incident resolution to document lessons learned, identify process improvements, and prevent recurrence.

2. Policy Statement

vStream Digital Media is committed to rapid, effective response to security incidents affecting our systems, applications, or customer data. This policy establishes procedures for detecting, reporting, assessing, responding to, and learning from security incidents to minimise impact on business operations, customer services (particularly ShineVR healthcare applications), and data protection obligations.

All employees, contractors, and third parties must immediately report suspected security incidents through established channels. Failure to report incidents or attempts to conceal incidents may result in disciplinary action.

This policy works in conjunction with the comprehensive Incident Response Plan which provides detailed technical procedures, escalation paths, and response playbooks for specific incident types.

3. Purpose

The purpose of this policy is to:

- Establish clear incident classification and response timeframes
- Enable rapid detection and response to security incidents
- Minimise impact on business operations and customer services
- Protect customer data, particularly sensitive healthcare information in ShineVR
- Ensure compliance with GDPR breach notification requirements
- Document incidents for regulatory reporting and compliance audits
- Facilitate continuous improvement through post-incident reviews

4. Scope

This policy applies to security incidents affecting:

- Google Cloud Platform infrastructure (europe-west4-a Netherlands, europe-west1-b Belgium)
- ShineVR application and associated healthcare services
- Cloud Run containers and container orchestration
- Cloud SQL databases and data storage systems
- Customer data including anonymised trial data
- Business systems including Google Workspace, source code repositories, and CI/CD pipelines
- Third-party services that process vStream or customer data

5. Incident Severity Classification

All security incidents are classified into three priority levels based on impact and urgency:

5.1 P1 - Critical Incidents

Definition: Incidents with severe impact requiring immediate action.

Initial Response Time: 15 minutes

Examples:

- Active data breach or unauthorised access to production systems
- ShineVR production service complete outage affecting customers
- Ransomware or destructive malware affecting production infrastructure
- Confirmed exfiltration of customer data or personal information
- Compromise of privileged accounts (SuperAdmin, database admin, GCP project owner)
- Critical vulnerability actively being exploited in production

5.2 P2 - High Priority Incidents

Definition: Incidents with significant impact requiring urgent attention.

Initial Response Time: 2 hours

Examples:

- Suspected unauthorised access or suspicious activity in production
- ShineVR partial service degradation affecting customer experience
- Malware detection on development or staging systems
- Successful phishing attack targeting employee accounts
- High-severity vulnerability discovered in production systems
- Compromise of standard user accounts with production access
- Significant Security Command Centre findings indicating policy violations

5.3 P3 - Low Priority Incidents

Definition: Incidents with limited impact requiring standard response.

Initial Response Time: 24 hours (next business day)

Examples:

- Policy violations not involving data compromise
- Low-severity vulnerabilities in non-production systems
- Suspicious activity in development or staging environments
- Failed phishing attempts with no account compromise
- Minor security misconfigurations not affecting production
- Security test failures in pre-production environments

6. Incident Response Procedure

6.1 Detection and Reporting

Security incidents may be detected through:

- **Automated Monitoring:** Security Command Centre alerts, Google Cloud Logging anomalies, failed automated tests
- **Employee Reports:** Suspicious emails, unusual system behaviour, access attempts, or security concerns
- **Customer Reports:** Service issues, suspected data breaches, or security concerns from customers
- **External Notifications:** Security researchers, law enforcement, or regulatory authorities

Reporting Channels:

- **Email:** andres@vstream.ie (CTO)
- **Phone (24/7):** (086) 788 6570 (CTO direct line for P1 incidents)

- **Google Workspace Chat:** Direct message to CTO or designated incident response team member

6.2 Initial Assessment

Upon receiving an incident report, the CTO or designated responder performs initial assessment:

- **Verify Incident:** Confirm the incident is genuine and not a false positive
- **Classify Severity:** Assign P1, P2, or P3 classification based on impact and urgency
- **Identify Scope:** Determine affected systems, data, and customers
- **Document Details:** Record initial findings including time of detection, symptoms, and potential impact
- **Activate Response:** Notify incident response team and initiate appropriate response procedures

6.3 Containment

Immediate actions to prevent incident escalation:

- **Isolate Affected Systems:** Disconnect compromised containers, revoke access tokens, or disable affected services
- **Preserve Evidence:** Capture logs, memory dumps, and system state before remediation
- **Block Attack Vectors:** Update firewall rules, revoke compromised credentials, patch vulnerabilities
- **Prevent Data Loss:** Stop data exfiltration, block unauthorised exports, isolate affected databases
- **Maintain Service:** Balance security containment with maintaining critical services for customers

6.4 Investigation

Detailed analysis to understand incident scope and root cause:

- **Log Analysis:** Review Cloud Audit Logs, application logs, and Security Command Centre findings
- **Timeline Reconstruction:** Build chronological timeline of events from initial compromise to detection
- **Impact Assessment:** Identify affected data, systems, and customers. For ShineVR, determine if customer data was accessed
- **Attack Vector Identification:** Determine how attacker gained access and what techniques were used
- **Root Cause Analysis:** Identify underlying vulnerabilities or weaknesses that enabled the incident

6.5 Eradication

Remove the threat and address vulnerabilities:

- **Remove Malware:** Clean infected systems, rebuild compromised containers from known-good images
- **Close Vulnerabilities:** Apply security patches, update configurations, strengthen access controls
- **Reset Credentials:** Force password resets, rotate API keys, regenerate service account tokens

- **Verify Clean State:** Confirm no backdoors, persistence mechanisms, or residual threats remain

6.6 Recovery

Restore systems to normal operations:

- **Restore Services:** Bring affected systems back online in controlled manner
- **Data Recovery:** Restore from backups if data was corrupted or destroyed (RTO 8 hours, RPO 24 hours)
- **Enhanced Monitoring:** Increase monitoring sensitivity during recovery period
- **Verify Functionality:** Run full test suite (400+ tests) to confirm system integrity
- **Customer Communication:** Update affected customers on resolution and preventive measures

6.7 Post-Incident Review

Mandatory for all P1 and P2 incidents, optional for P3:

- **Review Meeting:** Incident response team meets within 5 business days of resolution
- **Document Lessons:** What happened, what worked well, what could be improved
- **Identify Actions:** Concrete steps to prevent recurrence (policy updates, technical controls, training)
- **Update Procedures:** Refine incident response procedures based on experience
- **Track Improvements:** Assign ownership and deadlines for identified improvements

7. Escalation and Communication

7.1 24/7 Escalation Contacts

For P1 critical incidents requiring immediate response:

Role	Name	Responsibility	Contact
Incident Commander (CTO)	**Andrés Pitt**	**Overall incident leadership, technical decision-making authority, resource allocation, regulatory liaison**	**andres@vstream.ie** **(086) 788 6570**
Business Lead (CPO)	**Andrew Jenkinson**	**Business impact assessment, service continuity decisions, customer experience coordination**	**andrew@vstream.ie** **(087) 948 0090**
Customer Communications Lead (Account Director)	**Sabina Boccini**	**Customer communications, stakeholder management, external relationship coordination**	**sabina@vstream.ie**

Note: These contacts are available 24 hours a day, 7 days a week for P1 incidents. Response times are measured from first contact.

7.2 Customer Communication

For incidents affecting customer services or data:

- **Initial Notification:** Inform affected customers within 2 hours of confirming customer impact
- **Progress Updates:** Regular status updates every 4 hours during active incident response
- **Resolution Notice:** Final communication when incident is resolved, including root cause summary
- **Transparency:** Clear, honest communication about what happened, what data was affected, and what actions were taken

8. GDPR Data Breach Notification

For incidents involving personal data breaches, vStream complies with GDPR notification requirements:

8.1 Data Protection Commission Notification

- **72-Hour Requirement:** Notify Data Protection Commission within 72 hours of becoming aware of qualifying breach
- **Required Information:** Nature of breach, categories and approximate number of data subjects affected, contact point (DPO), likely consequences, and measures taken
- **Phased Reporting:** If complete information not available within 72 hours, provide initial notification with updates to follow
- **Documentation:** Document all breaches (even if not notified to DPC) for compliance audits

8.2 Data Subject Notification

When breach likely to result in high risk to individuals:

- **Direct Communication:** Notify affected individuals without undue delay
- **Clear Language:** Use clear, plain language explaining nature of breach and recommended actions
- **Trial Context:** For ShineVR trials, vStream cannot directly contact individuals (data is anonymised). Customer as Data Controller handles subject notification if required
- **Support Resources:** Provide contact information for questions and support

8.3 Data Controller Notification

As a Data Processor for customers:

- **Immediate Notification:** Inform Data Controller immediately upon becoming aware of breach
- **Support Controller's Obligations:** Provide information needed for Controller to meet their own GDPR obligations
- **Cooperation:** Cooperate fully with Controller's incident response and notification activities

9. Incident Documentation

All security incidents must be documented with:

- **Incident Identifier:** Unique reference number for tracking
- **Timeline:** Chronological record of detection, response actions, and resolution
- **Classification:** Severity (P1/P2/P3), type, and impact assessment
- **Response Actions:** Containment, investigation, eradication, and recovery steps taken

- **Root Cause:** Underlying vulnerability or weakness that enabled the incident
- **Affected Systems:** GCP resources, containers, databases, and applications impacted
- **Data Impact:** Whether personal data was accessed, modified, or exfiltrated
- **Notifications:** Record of all regulatory, customer, and data subject notifications
- **Lessons Learned:** Post-incident review findings and improvement actions

10. Training and Testing

10.1 Security Awareness Training

- **All Employees:** Annual security awareness training including incident recognition and reporting
- **Incident Response Team:** Specialised training on incident response procedures and tools
- **Phishing Simulations:** Periodic simulated phishing exercises to test and improve detection

10.2 Incident Response Testing

- **Tabletop Exercises:** Annual scenario-based discussion to test incident response procedures
- **Technical Drills:** Quarterly technical exercises testing specific response capabilities (e.g., backup restoration, account lockout)
- **Continuous Testing:** Automated security tests (400+ tests) run on every code commit, providing ongoing validation of security controls

11. Roles and Responsibilities

11.1 Chief Technology Officer / Data Protection Officer

- Overall responsibility for incident response programme
- Incident response team leadership for P1 and P2 incidents
- GDPR data breach notification to Data Protection Commission
- Post-incident review facilitation and improvement tracking
- Annual review and update of incident management procedures

11.2 Backend Developers

- Technical incident investigation and analysis
- Implementation of containment and eradication measures
- System recovery and service restoration
- Technical improvements identified in post-incident reviews

11.3 Account Director

- Customer communication coordination
- Customer liaison for ShineVR trial incidents
- Customer impact assessment and relationship management

11.4 All Employees

- Immediate reporting of suspected security incidents
- Cooperation with incident investigation and response
- Following instructions from incident response team during active incidents

12. Related Policies and Documents

- Information Security Policy
- Incident Response Plan (detailed technical procedures)
- Log Management Policy
- Access Management Policy
- Backup and Recovery Policy
- Cloud Security Policy

13. Contact Information

24/7 Security Incident Hotline:

Andrés Pitt (CTO / DPO)

Phone: (086) 788 6570

Email: andres@vstream.ie

Company Address:

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