Incident Response Plan

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
Incident	Any event that could lead to loss of, or disruption to, the organisation's operations, services or functions
Security Incident	Any actual or suspected breach of security that compromises the confidentiality, integrity or availability of information or systems
Data Breach	A security incident that has led to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data
Response Team	The designated team responsible for managing and responding to security incidents

Term	Definition
Business Hours	9:00 AM – 5:30 PM, Monday to Friday, Irish calendar (excluding public holidays)

1. POLICY STATEMENT

vStream Digital Media is committed to maintaining the security and integrity of all Company and ShineVR systems and data. This Incident Response Plan establishes a comprehensive framework for detecting, responding to, and recovering from security incidents in a timely and effective manner.

The plan provides structured procedures to minimise the impact of security incidents on the Company's operations, customers, and stakeholders, whilst ensuring compliance with GDPR and other regulatory requirements.

2. PURPOSE

The purpose of this Incident Response Plan is to:

- Provide a clear, actionable framework for responding to security incidents
- Ensure rapid detection, containment, and resolution of security incidents
- Minimise business disruption and data loss
- Protect the confidentiality, integrity, and availability of Company and ShineVR systems and data
- Ensure compliance with GDPR breach notification requirements (72-hour rule)
- Facilitate continuous improvement through lessons learned from incidents
- Define clear roles, responsibilities, and escalation procedures
- Enable 24/7 response capability for critical incidents

3. SCOPE

This plan applies to:

- All security incidents affecting vStream Digital Media or ShineVR systems
- All data breaches involving personal data processed by the Company
- All employees, contractors, temporary staff, and third-party suppliers
- All Company and ShineVR systems including:
    - Google Cloud Platform infrastructure
    - ShineVR applications and databases
    - Company email and communication systems
    - Development, staging, and production environments

- Third-party services processing Company or ShineVR data

4. INCIDENT CLASSIFICATION AND SEVERITY LEVELS

All incidents are classified according to severity to ensure appropriate response prioritisation and resource allocation.

4.1 Priority 1 (P1) – Critical Incidents

Definition: Major security breach, significant data loss, or complete system outage affecting operations

Examples:

- Complete ShineVR service outage affecting customer access
- Confirmed breach of personal data (PII) or sensitive health data
- Ransomware attack or major malware infection
- Complete loss of access to Google Cloud Platform
- Unauthorised access to production databases
- Large-scale compromise of customer accounts
- Critical vulnerability actively being exploited
- Total loss of encryption keys

Impact:

- Business operations significantly disrupted or halted
- Customer data confidentiality, integrity, or availability compromised
- Regulatory breach notification likely required
- Significant reputational damage likely
- Financial impact significant

Response Requirements:

- Immediate response (within minutes of detection)
- Response team fully activated
- 24/7 response required
- CTO direct involvement mandatory
- Customer notification within 4 hours
- GDPR notification assessment within 24 hours

4.2 Priority 2 (P2) – High Severity Incidents

Definition: Significant service degradation, potential data exposure, or serious security vulnerability

Examples:

- Partial ShineVR service degradation affecting multiple users
- Potential exposure of non-sensitive personal data
- Successful phishing attack against employee account
- Unauthorised access attempt to production systems (unsuccessful but sophisticated)
- Compromise of development or staging environment
- Discovery of critical unpatched vulnerability in production
- Suspected but unconfirmed data breach
- Loss of backup data
- Prolonged performance degradation

Impact:

- Business operations degraded but not halted
- Limited data exposure or system compromise
- Customer experience significantly affected
- Moderate reputational risk
- Potential regulatory notification required

Response Requirements:

- Response within 30 minutes during business hours
- Response within 2 hours outside business hours
- Core response team activated
- CTO notified and involved in decision-making
- Customer notification within 8 hours if customer-facing
- GDPR notification assessment within 48 hours

4.3 Priority 3 (P3) – Low Severity Incidents

Definition: Minor incidents, policy violations, or informational security events

Examples:

- Single user account compromise
- Minor policy violation (e.g., weak password)
- Failed login attempts (automated scanning)

- Discovery of low-severity vulnerability
- Minor configuration issue detected
- Suspicious but non-malicious activity
- Loss of non-sensitive data
- Brief, isolated service degradation

Impact:

- Minimal impact on business operations
- No significant data exposure
- Limited or no customer impact
- Low reputational risk
- No regulatory notification required

Response Requirements:

- Response within 4 hours during business hours
- Next business day response acceptable outside hours
- Can be handled by single responder initially
- CTO notified via daily summary report
- No immediate customer notification required
- Documented and tracked for trend analysis

5. INCIDENT RESPONSE TEAM STRUCTURE

5.1 Core Response Team

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

Role	Name	Responsibility	Contact
Customer Communications Lead (Account Director)	Sabina Boccini	Customer communications, stakeholder management, external relationship coordination	sabina@vstream.ie

5.2 Extended Response Team (Activated as Needed)

- **Backend Developers:** Technical investigation, code analysis, system remediation
- **Product Manager:** Feature impact assessment, product decision support
- **Legal Counsel:** Regulatory compliance advice, contractual obligations (external consultant)
- **External Security Specialists:** Advanced forensics, penetration testing, expert consultation (engaged as needed)

5.3 24/7 Availability

All Core Response Team members maintain 24/7 availability via:

- Direct phone lines (listed above)
- Mobile phones with alerts enabled
- Email with push notifications
- Slack with urgent notification channels

Escalation Order:

1. First contact: CTO (Andrés Pitt) for all P1/P2 incidents
2. If CTO unavailable within 15 minutes (P1) or 30 minutes (P2): Contact CPO
3. If both unavailable: Contact Account Director and continue escalation attempts

6. INCIDENT RESPONSE PHASES

PHASE 1: DETECTION AND ANALYSIS (0-30 minutes)

Objective: Identify, verify, and classify the incident; activate response team

Activities:

6.1 Detection Sources Incidents may be detected through:

- Automated monitoring systems (Google Cloud Security Command Centre)
- Google Cloud alerts (email and Slack channels)
- User reports (employees, customers, partners)
- Automated testing failures (400+ automated tests including security checks)
- Docker vulnerability scans
- External reports (researchers, partners)
- System performance anomalies
- Log analysis and SIEM alerts

6.2 Initial Triage (0-15 minutes) When an incident is detected:

1. **Verify the incident:** Confirm it is a genuine security incident, not a false positive
2. **Document initial details:**
    - Date and time of detection
    - Detection source and method
    - Initial description of incident
    - Systems potentially affected
    - Data potentially impacted
3. **Classify severity:** Assign P1, P2, or P3 classification based on criteria in Section 4
4. **Activate response team:** Contact appropriate team members based on severity

6.3 Response Team Activation (15-30 minutes)

- **P1 incidents:** Full core response team activated immediately via phone
- **P2 incidents:** Core response team notified; CTO and one other member minimum
- **P3 incidents:** Single responder initially; CTO notified via email/Slack

6.4 Preliminary Impact Assessment

- Determine which systems are affected
- Identify what data may be compromised
- Assess number of users/customers impacted
- Estimate business impact and service disruption
- Determine if PII or sensitive personal data involved

6.5 Evidence Preservation

- Do not power off systems unless absolutely necessary
- Preserve log files immediately (may be overwritten)
- Take screenshots of unusual activity
- Document chain of custody for all evidence
- Isolate affected systems if necessary to preserve evidence

6.6 Incident Registration

- Create incident record in Company Data Breach Register
- Assign unique incident number (format: INC-YYYY-MM-DD-XXX)
- Document all actions taken with timestamps
- All subsequent actions logged against this incident number

PHASE 2: CONTAINMENT AND ERADICATION (30 minutes – 4 hours)

Objective: Prevent incident escalation; eliminate threat; limit damage

Activities:

6.7 Immediate Containment Measures (30-90 minutes)

Network-level containment:

- Isolate affected systems from network
- Block malicious IP addresses at firewall/cloud level
- Disable compromised accounts immediately
- Revoke API keys or access tokens if compromised
- Implement network segmentation to protect critical systems

Access restriction:

- Lock compromised user accounts
- Force password resets for potentially affected users
- Revoke session tokens and cookies
- Disable compromised service accounts
- Enable additional authentication for sensitive operations

System isolation:

- Take affected systems offline if necessary
- Redirect traffic away from compromised systems
- Deploy backup/standby systems if available
- Enable read-only mode on databases if data integrity threatened
- Snapshot affected systems for forensic analysis

Communication control:

- Establish dedicated incident communication channel (private Slack channel)
- Implement communication protocol (who communicates what to whom)

- Brief all responders on current situation and assigned tasks
- Establish regular status update schedule (every 30-60 minutes for P1)

6.8 Root Cause Analysis (1-3 hours) Investigate to determine:

- **How did the incident occur?** (attack vector, vulnerability exploited)
- **When did it occur?** (timeline of events)
- **What was the extent?** (scope of compromise)
- **What systems were affected?** (full inventory)
- **What data was accessed/modified/exfiltrated?** (data breach assessment)
- **Who was responsible?** (internal error, external attacker, system failure)
- **Are there other affected systems not yet identified?**

Investigation methods:

- Review system logs (Google Cloud logs, application logs, access logs)
- Analyse network traffic patterns
- Review authentication and access logs
- Examine database query logs
- Check integrity of critical files (file integrity monitoring)
- Review recent system changes (change control logs)
- Analyse Docker container vulnerabilities scans
- Interview relevant personnel

6.9 Threat Eradication (2-4 hours) Eliminate the threat completely:

- Remove malware or malicious code from systems
- Close security vulnerabilities that were exploited
- Apply security patches and updates
- Replace compromised systems with clean installations if necessary
- Update firewall rules and access controls
- Enhance monitoring on affected systems
- Deploy additional security controls as needed

Verification of eradication:

- Scan all affected systems for malware/vulnerabilities
- Verify no unauthorised access or backdoors remain
- Confirm all compromised credentials have been changed
- Review and test security controls
- Obtain confirmation from external security experts if needed (P1 incidents)

PHASE 3: RECOVERY AND POST-INCIDENT (4-24 hours and ongoing)

Objective: Restore normal operations safely; ensure no recurrence; learn from incident

Activities:

6.10 System Restoration (4-12 hours)

Gradual restoration approach:

- Restore systems incrementally, starting with non-critical systems
- Monitor intensively during restoration (enhanced logging and alerting)
- Verify security controls are functioning properly
- Test functionality before full production restoration
- Validate data integrity after restoration
- Confirm backups are clean before restoring from them

Validation steps:

- Run full security scans on restored systems
- Verify proper authentication and authorisation
- Test encryption is functioning properly
- Confirm monitoring and alerting is operational
- Run automated test suite (400+ tests) to verify functionality
- Conduct manual testing of critical functions

6.11 Enhanced Monitoring (12-24 hours post-restoration) After systems are restored:

- Implement enhanced logging for affected systems
- Deploy additional monitoring for similar attack patterns
- Increase frequency of security scans
- Monitor for any unusual activity indicating persistence
- Continue enhanced monitoring for at least 7 days

6.12 Stakeholder Notification and Status Updates

Internal notifications:

- Update all employees on incident status (if company-wide impact)
- Provide clear guidance on any required actions (password changes, etc.)
- Brief senior management on business impact and recovery

External notifications:

- **Customer notification (if customer-facing incident):**
  - P1: Within 4 hours of incident classification
  - P2: Within 8 hours if customer data potentially affected
  - P3: Only if specifically required
- **Regulatory notification (GDPR):**
  - Assessment within 24 hours (P1) or 48 hours (P2)
  - Notification to Data Protection Commission within 72 hours if required
  - Include: nature of breach, categories/numbers of data subjects affected, likely consequences, measures taken/proposed
- **Partner/supplier notification:**
  - Notify if their systems/data potentially affected
  - Coordinate response if incident involves shared infrastructure
- **Garda Síochána notification:**
  - Notify for criminal activity (e.g., hacking, data theft)
  - Provide evidence for investigation if requested

6.13 Documentation and Reporting Complete detailed incident report including:

- **Incident summary:** What happened, when, how detected
- **Impact assessment:** Systems affected, data compromised, users impacted
- **Timeline of events:** Detailed chronology with timestamps
- **Response actions:** Everything done during response
- **Root cause:** Technical and procedural causes identified
- **Lessons learned:** What went well, what could be improved
- **Recommendations:** Changes to prevent recurrence

Report distribution:

- CTO receives full detailed report
- Board/senior management receives executive summary
- Technical team receives technical details
- Customers receive appropriate notification (if applicable)
- Regulators receive notification (if required)

6.14 Post-Incident Review (Within 72 hours of resolution) Conduct formal post-incident review meeting with:

- All response team members involved
- Relevant technical staff
- CTO and senior management (for P1/P2 incidents)

Review agenda:

1. Incident summary and timeline review
2. What went well (strengths in response)
3. What could be improved (weaknesses identified)
4. Root cause analysis validation
5. Preventative measures identified
6. Process improvements needed
7. Policy/procedure updates required
8. Training needs identified
9. Action items assigned with owners and deadlines

6.15 Continuous Improvement Based on lessons learned:

- Update this Incident Response Plan as needed
- Update relevant security policies and procedures
- Implement technical security improvements
- Deploy additional monitoring or detection capabilities
- Conduct additional training for staff
- Update incident response training materials
- Share anonymised lessons learned with industry (where appropriate)

7. BUSINESS HOURS vs. AFTER-HOURS RESPONSE

7.1 Business Hours Response (9:00 AM – 5:30 PM, Monday-Friday)

- Standard incident response procedures apply
- Full response team available
- All resources and tools immediately accessible
- Fastest response times achievable

7.2 After-Hours Response (Outside Business Hours)

- **P1 incidents:** Full 24/7 response activated
    - Core response team contacted via phone immediately
    - All team members expected to respond within 30 minutes
    - Remote access to all systems maintained
    - Escalation continues until contact established
- **P2 incidents:**
    - CTO contacted via phone
    - Response within 2 hours
    - Additional team members contacted if needed
    - Can be escalated to P1 if severity increases

- **P3 incidents:**
    - Next business day response acceptable
    - Documented for review in morning
    - Escalated if situation worsens

7.3 24/7 Escalation Contact Methods

All Core Response Team members maintain:

1. **Primary contact:** Mobile phone with ringer enabled 24/7
2. **Secondary contact:** Email with push notifications
3. **Tertiary contact:** Slack with urgent alerts configured
4. **Backup contact:** Alternative phone number (e.g., home phone)

8. COMMUNICATION PROTOCOLS

8.1 Internal Communication

- **Primary channel:** Dedicated private Slack channel for each incident
- **Backup channel:** Email thread with clear subject line (INC-XXXX)
- **Emergency channel:** Direct phone calls
- **Status updates:** Scheduled regular updates (frequency based on severity)

8.2 External Communication

- **Customers:** Account Director manages all customer communications
- **Regulators:** CTO or designated DPO manages regulatory communications
- **Media:** Only authorised spokespersons may speak to media (CEO/CTO)
- **Partners:** CTO or Account Director manages partner communications

8.3 Communication Principles

- **Accuracy:** Only communicate confirmed information
- **Timeliness:** Communicate within timeframes specified above
- **Transparency:** Be honest about what is known and unknown
- **Consistency:** Ensure all parties receive consistent information
- **Confidentiality:** Protect sensitive details while being transparent about impact

9. SPECIAL INCIDENT TYPES

9.1 Ransomware Incidents

Additional considerations:

- **DO NOT** pay ransom without CTO and legal consultation
- Isolate affected systems immediately
- Determine if backups are clean and unaffected
- Assess data exfiltration (modern ransomware often exfiltrates before encrypting)
- Consider law enforcement involvement
- Evaluate backup restoration vs. ransom payment
- Implement additional access controls during recovery

9.2 Data Breach Incidents (GDPR)

Critical requirements:

- Assess within 24 hours whether personal data was compromised
- Document assessment of risk to data subjects' rights and freedoms
- Notify Data Protection Commission within 72 hours if high risk
- Notify affected data subjects if high risk to their rights and freedoms
- Document all decisions regarding notification
- Maintain detailed records of breach in GDPR breach register

Factors for notification assessment:

- Type of data compromised (PII, sensitive personal data, health data)
- Volume of data and number of affected individuals
- Potential consequences for data subjects
- Characteristics of data subjects (children, vulnerable persons)
- Any mitigating factors (encryption, limited access)

9.3 Insider Threat Incidents

Special handling:

- Coordinate with HR and legal counsel before taking action
- Consider evidence preservation for potential legal action
- Implement access revocation carefully to avoid alerting suspect
- Review all systems accessed by suspected insider
- Conduct thorough audit of all actions by insider
- Consider law enforcement referral for criminal activity

9.4 Third-Party Supplier Incidents

When incident involves supplier:

- Contact supplier immediately to coordinate response
- Assess impact on Company and ShineVR systems

- Review contractual obligations and SLAs
- Determine if supplier breach affects Company's GDPR obligations
- Monitor supplier's response and recovery
- Document all supplier communications

9.5 Google Cloud Platform Incidents

If incident involves Google Cloud infrastructure:

- Review Google Cloud Status Dashboard immediately
- Contact Google Cloud support (appropriate priority)
- Assess impact on ShineVR services
- Implement workarounds if possible
- Communicate service impact to customers
- Monitor Google's incident resolution
- Document incident and Google's response

10. TOOLS AND RESOURCES

10.1 Detection and Monitoring Tools

- **Google Cloud Security Command Centre:** Primary security monitoring
- **Google Cloud Logging:** Centralised log management
- **Docker Vulnerability Scanning:** Container security
- **Automated Testing Suite:** 400+ tests including security checks
- **Google Workspace Admin Console:** Email and account monitoring

10.2 Response Tools

- **Google Cloud IAM:** Access control management
- **Google Cloud KMS:** Key management and rotation
- **Slack:** Incident communication and alerting
- **Google Cloud Console:** Infrastructure management
- **Incident Documentation Template:** Standardised incident recording

10.3 External Resources

- **Google Cloud Support:** Technical support and guidance
- **External Security Consultants:** Advanced forensics and investigation
- **Legal Counsel:** Regulatory and contractual advice
- **Data Protection Commission:** Regulatory breach notification
- **Garda Síochána:** Criminal investigation support

11. INCIDENT CATEGORISATION EXAMPLES

Security Incidents (Confidentiality Breach)

- Unauthorised access to systems or data
- Data exfiltration or theft
- Phishing attack successful
- Insider threat or malicious employee activity
- Lost or stolen device containing sensitive data
- Accidental disclosure of confidential information
- Social engineering attack successful

Integrity Incidents (Data Modification)

- Unauthorised modification of data
- Database corruption
- Malware infection modifying files
- Unauthorised system configuration changes
- Tampering with audit logs
- Code injection or SQL injection attack

Availability Incidents (Denial of Service)

- DDoS attack
- Ransomware encryption
- System failure or crash
- Network outage
- Resource exhaustion
- Performance degradation

Compliance Incidents

- GDPR violation or breach
- Failure to meet regulatory requirements
- Breach of customer contract SLAs
- Certification compliance failure
- Policy violation with compliance implications

12. INCIDENT METRICS AND REPORTING

12.1 Incident Tracking Metrics

Track and report on:

- **Number of incidents by severity** (P1, P2, P3)
- **Mean time to detect (MTTD):** Time from incident occurrence to detection
- **Mean time to respond (MTTR):** Time from detection to response initiation
- **Mean time to contain (MTTC):** Time from response to containment
- **Mean time to recover (MTTRec):** Time from containment to full recovery
- **Incident trends:** Are certain types increasing?
- **Root causes:** Most common causes of incidents

12.2 Regular Reporting

- **Weekly:** CTO reviews all incidents from past week
- **Monthly:** Summary report to senior management
- **Quarterly:** Trends analysis and improvement recommendations
- **Annually:** Comprehensive incident review and plan update

12.3 Incident Register

Maintain centralised, secure register documenting:

- Incident ID and classification
- Detection date/time and method
- Description and impact
- Response actions taken
- Resolution date/time and outcome
- Lessons learned and recommendations
- All register entries retained for minimum 7 years

13. TRAINING AND EXERCISES

13.1 Incident Response Training

- **All employees:** Annual security awareness training including incident reporting
- **Response Team:** Quarterly incident response training
- **Technical staff:** Specialised training on forensics and investigation
- **New joiners:** Incident reporting procedures in onboarding

13.2 Tabletop Exercises

Conduct tabletop exercises:

- **Frequency:** At least twice annually
- **Scenarios:** Rotate through different incident types (ransomware, data breach, DDoS, etc.)

- **Participants:** Core response team and relevant technical staff
- **Objectives:** Test procedures, identify gaps, improve coordination
- **Documentation:** Document lessons learned and action items

13.3 Plan Testing

Test specific aspects:

- Contact information accuracy (quarterly review)
- Backup restoration procedures (monthly testing)
- Escalation procedures (annual test)
- Communication channels (quarterly test)
- Tool accessibility and functionality (ongoing)

14. COMPLIANCE AND LEGAL CONSIDERATIONS

14.1 GDPR Breach Notification

This plan ensures compliance with GDPR requirements:

- **Article 33:** Notification to supervisory authority within 72 hours
- **Article 34:** Notification to data subjects without undue delay (if high risk)
- Documented rationale if notification not required
- Records of all data breaches maintained

14.2 Contractual Obligations

This plan addresses contractual requirements:

- Customer SLA breach notification procedures
- Service provider incident notification requirements
- Incident reporting to partners and suppliers
- Insurance claim documentation

14.3 Legal Evidence Preservation

For incidents that may involve legal proceedings:

- Maintain chain of custody for all evidence
- Do not destroy or modify evidence
- Preserve all logs and communications
- Engage legal counsel early if criminal activity suspected
- Coordinate with law enforcement as appropriate

15. PLAN MAINTENANCE

15.1 Regular Review

This plan will be reviewed:

- **Annually:** Comprehensive review by CTO
- **After major incidents:** Update based on lessons learned
- **When organisational changes occur:** New systems, personnel, or processes
- **When threat landscape changes:** New attack types or vulnerabilities
- **When regulations change:** Updated compliance requirements

15.2 Version Control

- Current version maintained in Google Drive
- Previous versions archived for reference
- All changes documented with rationale
- Distribution list updated when plan changes

15.3 Plan Distribution

Ensure plan is accessible to:

- All Core Response Team members (current version)
- All technical staff (relevant sections)
- Senior management (executive summary)
- Stored in multiple secure locations for availability during incidents

16. ROLES AND RESPONSIBILITIES SUMMARY

Role	Responsibilities
CTO (Incident Commander)	Overall incident response leadership; technical decision-making; resource allocation; regulatory liaison; plan maintenance; post-incident review chair
CPO (Business Lead)	Business impact assessment; service continuity decisions; customer experience coordination; communication prioritisation

Role	Responsibilities
Account Director	Customer communications; stakeholder management; external relationships; customer notification execution
Backend Developers	Technical investigation; system forensics; threat eradication; system restoration; security testing
Product Manager	Feature impact assessment; product recovery decisions; customer impact analysis; change prioritisation
All Employees	Detect and report incidents immediately; preserve evidence; follow response team instructions; maintain confidentiality

17. CONTACT INFORMATION

Core Response Team (24/7 Availability)

Incident Commander / CTO: Andrés Pitt Email: andres@vstream.ie Phone: (086) 788 6570

Chief Product Officer: [CPO Name] Email: [CPO Email] Phone: [CPO Phone]

Account Director: [Account Director Name] Email: [Account Director Email] Phone: [Account Director Phone]

External Contacts

Data Protection Commission (Ireland): Email: info@dataprotection.ie Phone: +353 (0)761 104 800 Website: https://www.dataprotection.ie

Google Cloud Support: Access via: Google Cloud Console Priority: Select based on incident severity

Garda Síochána (Computer Crime Investigation Unit): Phone: Garda Station number or 999/112 for emergencies

18. APPENDICES

Appendix A: Incident Report Template

- Incident ID: INC-YYYY-MM-DD-XXX
- Severity: P1 / P2 / P3
- Detection date/time:
- Detection method:
- Initial description:
- Systems affected:
- Data affected:
- Number of users impacted:
- Business impact:
- Response team activated:
- Containment actions:
- Eradication actions:
- Recovery actions:
- Root cause:
- Lessons learned:
- Recommendations:
- Final resolution date/time:

Appendix B: GDPR Breach Notification Decision Tree

1. Was personal data involved? If NO Document as security incident only
2. If YES, Assess risk to individuals' rights and freedoms
3. Is there a likely risk? If NO Document decision not to notify
4. If YES, Notify DPC within 72 hours
5. Is there high risk? If YES Also notify affected individuals without undue delay

Appendix C: Incident Communication Templates

- Internal staff notification email template
- Customer incident notification template
- GDPR breach notification to DPC template
- GDPR breach notification to data subjects template
- Media statement template (if needed)

Appendix D: Quick Reference Cards

- One-page P1 incident response checklist
- Contact list with phone numbers
- Escalation flowchart

- GDPR notification decision flowchart