Security Incident Response Policy

v1.0 · Reviewed Jun 2026 · Next review Jun 2027

HALVED LIMITED

SECURITY INCIDENT RESPONSE POLICY

Version: 1.0 Effective Date: 4th June 2026 Last Review: 4th June 2026 Next Review: 4th June 2027

Owner: Andrew James, CEO

1. PURPOSE

This policy defines how Halved Limited responds to security incidents to minimise impact, recover quickly, and prevent future incidents.

2. SCOPE

This policy applies to all security incidents affecting:

- User accounts (email, cloud services, system access)
- Devices (MacBooks, mobile devices)
- Cloud infrastructure (Azure, MongoDB, GitHub, etc.)
- Organisational data

3. WHAT IS A SECURITY INCIDENT?

A security incident includes:

- Suspected account compromise (unauthorised access)
- Lost or stolen device
- Suspected malware infection

- Phishing attack (clicked link, provided credentials)
- Data breach or unauthorised data access
- Suspicious system behaviour
- Ransomware or attempted ransomware
- Any event that could compromise data confidentiality, integrity, or availability

4. INCIDENT RESPONSE PROCEDURE

Phase 1: IMMEDIATE ACTIONS (Within 15 Minutes)

Step 1: Report the Incident

Who to contact: Andrew James, CEO

How to report:

- Email: aj@halved.io
- Phone: +971 585616250
- WhatsApp: +971 585616250

What to report:

- What happened (brief description)
- When it happened
- Which account/system is affected
- What you've done so far (if anything)

Step 2: Initial Containment

CEO takes immediate action:

If account compromised:

- Force password reset on affected account
- Terminate all active sessions

- Disable account temporarily if necessary

If device lost/stolen:

- Remotely wipe device (if possible via Find My / MDM)
- Disable all accounts accessible from that device
- Change passwords for all accounts

If malware suspected:

- Disconnect device from network immediately
- Do not shut down (preserves evidence)
- Notify CEO for next steps

Phase 2: INVESTIGATION (Within 1 Hour)

Step 3: Assess the Scope

CEO investigates:

- Which accounts were accessed?
- What data was accessed or exposed?
- Was the incident isolated or part of a broader attack?
- Were any changes made to systems or data?

Step 4: Document the Incident

Create incident record documenting:

- Date and time incident discovered
- Date and time incident occurred (if different)
- Affected systems/accounts
- Actions taken
- Timeline of events

Phase 3: REMEDIATION (Within 4 Hours)

Step 5: Remove Threat and Restore Access

For compromised accounts:

- Create new strong password (12+ characters, unique)
- Re-enrol MFA (new device/app)
- Review account settings for unauthorised changes
- Check for forwarding rules (email), API keys, etc.
- Re-enable account for legitimate user

For lost/stolen devices:

- Confirm remote wipe completed
- Issue replacement device
- Restore from backup
- Re-enrol in security systems

For malware:

- Run anti-malware scan
- If infection confirmed, wipe and reinstall OS
- Restore from clean backup
- Re-enrol in security systems

Step 6: Verify System Integrity

- Check for backdoors or persistence mechanisms
- Verify no unauthorised users were created
- Confirm no data was exfiltrated (if possible)
- Review logs for suspicious activity

Phase 4: NOTIFICATION (Within 72 Hours if Required)

Step 7: Determine Notification Requirements

Internal notification:

- Notify all team members if incident affects shared systems
- Brief on what happened and what action they need to take

External notification (if required by law):

- Customer data breach: Notify affected customers within 72 hours (GDPR requirement)
- Regulatory reporting: Notify ICO if required under GDPR
- Partner notification: Notify schools/partners if their data affected

When to notify authorities:

- Ransomware attack: Consider reporting to National Cyber Security Centre (NCSC)
- Financial fraud: Report to Action Fraud
- Critical infrastructure impact: Report to NCSC

Phase 5: POST-INCIDENT REVIEW (Within 1 Week)

Step 8: Lessons Learned

CEO conducts review:

- What was the root cause?
- How was the incident detected?
- What worked well in the response?
- What could be improved?
- What preventive measures should be implemented?

Step 9: Update Policies and Procedures

Based on lessons learned:

- Update this policy if needed

- Update technical controls
- Provide additional training to team
- Document improvements in incident record

Step 10: Close Incident

Mark incident as resolved in incident log when:

- Threat has been eliminated
- Normal operations restored
- Required notifications completed
- Lessons learned documented
- Preventive measures implemented

5. INCIDENT SEVERITY LEVELS

Level 1: CRITICAL

- Customer data breach
- Ransomware attack
- Complete system compromise
- Financial fraud

Response time: Immediate (drop everything)

Level 2: HIGH

- Single account compromise with admin access
- Device lost/stolen
- Suspected malware
- Attempted phishing attack (credentials entered)

Response time: Within 1 hour

Level 3: MEDIUM

- Single standard account compromise
- Failed login attempts
- Suspicious email received (not clicked)
- Minor configuration error

Response time: Within 4 hours

Level 4: LOW

- Spam email
- Suspicious but verified legitimate activity
- General security question

Response time: Next business day

6. ESCALATION CONTACTS

Primary Contact:

Andrew James, CEO

Email: aj@halved.io

Phone: +971 585616250

Regulatory Reporting:

ICO (Data Protection): https://ico.org.uk/make-a-complaint/data-protection-complaints/

NCSC (Cyber Security): https://www.ncsc.gov.uk/section/about-ncsc/report-an-incident

7. INCIDENT LOG

All security incidents are logged in: Halved_Security_Incident_Log.xlsx

Minimum information recorded:

- Incident ID (sequential number)
- Date/time discovered

- Date/time occurred
- Severity level
- Brief description
- Affected systems/accounts
- Actions taken
- Resolution date
- Lessons learned

Retention: Incident logs retained for 7 years (GDPR compliance)

8. TRAINING AND AWARENESS

All team members receive security awareness training:

- On joining: Security incident recognition and reporting procedures
- Annually: Refresher on common threats (phishing, social engineering, etc.)
- After incident: Specific training based on lessons learned

9. POLICY REVIEW

This policy is reviewed:

- Annually: Scheduled review every 12 months
- After major incident: Review within 1 week of any Level 1 or Level 2 incident
- When regulations change: Update to reflect new legal/regulatory requirements

APPROVED BY:

Andrew James, CEO Halved Limited Date: 4th June 2026

Questions about data protection? **dataprivacy@halved.io**

Website **halved.io** · students log in at my.halved.io