jrhsupport

SECURITY INCIDENT RESPONSE POLICY

SECURITY INCIDENT RESPONSE POLICY

Introduction

At JRH Support, we are committed to providing safe, effective, and person-centred social care services. Protecting the confidentiality, integrity, and availability of sensitive information, particularly the personal data of our service users and staff, is paramount to this commitment.

Despite our best efforts, security incidents can occur. This policy outlines the structured approach we will take to prepare for, identify, respond to, manage, and recover from security incidents. The goal is to minimise damage, restore normal operations quickly, learn from incidents, and maintain public and regulatory trust.

Scope

This policy applies to all employees, contractors, and anyone else who accesses or uses our IT systems, networks, data, and physical premises. It covers all types of security incidents, whether accidental or malicious, that could compromise our information assets or operational capabilities.

Policy Objectives

The objectives of this policy are to:

- **Minimise Impact:** Reduce the financial, operational, reputational, and legal impact of security incidents.
- **Prompt Response:** Ensure a timely and effective response to all detected security incidents.
- **Containment & Eradication:** Limit the spread and eliminate the root cause of the incident.
- **Recovery:** Restore affected systems and data to normal, secure operations as quickly as possible.
- **Learning & Improvement:** Analyse incidents to identify weaknesses and implement preventative measures.
- **Compliance:** Ensure compliance with legal and regulatory obligations, including GDPR and CQC requirements, particularly regarding data breach notification.

Definition of a Security Incident

A security incident is any event that compromises or attempts to compromise the confidentiality, integrity, or availability of information, information systems, or physical assets. This includes, but is not limited to:

- **Data Breach:** Unauthorised access, disclosure, alteration, loss, or destruction of personal data (e.g., lost USB drive with client data, phishing attack leading to account compromise).
- **Malware Infection:** Viruses, ransomware, spyware, or other malicious software.
- **Unauthorised Access:** Successful or attempted access to systems or data by unauthorised individuals.
- **Phishing/Social Engineering:** Attempts to trick staff into revealing sensitive information or performing unauthorised actions.
- **System Outage/Failure:** Unplanned downtime of critical IT systems impacting service delivery.

- **Physical Security Breach:** Unauthorised entry to our premises where sensitive information or IT equipment is stored.
- **Suspicious Activity:** Any unusual or unexplained event that suggests a potential security compromise (e.g., unexpected emails, unusual system behaviour).

Roles and Responsibilities
Effective incident response requires clear allocation of duties:

- **Incident Response Lead (IRL):**
  - General Manager.
  - Overall responsibility for overseeing the incident response process.
  - Authorises actions and decisions during an incident.
  - Liaises with external parties (e.g., police, ICO, CQC, external IT support).
  - Ensures post-incident review and policy updates.
- **Staff Members (All):**
  - Promptly report any suspected or actual security incidents to their Line Manager and/or the General Manager immediately.
  - Follow instructions from the General Manager.
  - Preserve any evidence if safe and instructed to do so (e.g., do not delete suspicious emails).
- **Line Managers:**
  - Act as the first point of contact for staff reporting incidents.
  - Immediately escalate reported incidents to the General Manager.
  - Support their team members during the incident and recovery.

Incident Response Process
The incident response process is divided into six key phases:

Phase 1: Preparation (Ongoing)

- **Training:** Regular security awareness training for all staff.
- **Contact Information:** Maintain up-to-date contact lists for key personnel (internal and external IT support, legal, regulatory bodies, police).
- **Documentation:** Keep this policy, IT asset inventory, system diagrams, and backup procedures readily accessible.
- **Backups:** Ensure regular, tested backups of all critical data.
- **Security Tools:** Maintain up-to-date anti-virus, firewalls, and other security software.
- **Incident Response Kit (Virtual/Physical):** List of tools, contacts, and quick reference guides.

Phase 2: Identification & Reporting

- **Recognize:** Staff identify unusual activity (e.g., pop-ups, slow systems, locked files, strange emails, missing equipment, unauthorized person on premises).
- **Immediate Reporting:**
  - **Action:** Immediately report the incident to your Line Manager and/or the Incident Response Lead.
  - **Information to Provide:** What happened, when, where, who was involved, any visible impact, and any actions already taken.
  - **Do NOT:** Try to fix the problem yourself unless specifically instructed and trained to do so. Do not share details of the incident externally.

Phase 3: Containment

- **Immediate Action:** The Incident Response Team will quickly assess the situation to limit the damage.
- **Isolation:** This may involve disconnecting affected devices from the network, disabling compromised accounts, or shutting down systems.
- **Preservation:** Steps will be taken to preserve evidence for investigation (e.g., by taking screenshots, noting down details, or preventing system reboots if advised).
- **Prioritisation:** Prioritise containment actions based on the potential impact (e.g., stop data exfiltration before restoring a service).

Phase 4: Eradication

- **Identify Root Cause:** Technical investigation to determine how the incident occurred.
- **Remove Threat:** Eliminate the threat (e.g., remove malware, patch vulnerabilities, reset passwords, remove unauthorized access).
- **Clean-up:** Ensure all traces of the malicious activity are removed.

Phase 5: Recovery

- **Restore Operations:** Bring affected systems and services back online. This may involve:
    - Restoring data from backups.
    - Rebuilding systems.
    - Implementing new security controls.
- **Validation:** Verify that systems are fully functional and secure before returning to normal operation.
- **Phased Approach:** Recovery may occur in stages, prioritizing critical services.

Phase 6: Post-Incident Activity & Lessons Learned

- **Documentation:** Fully document the incident, including:
    - Timeline of events.
    - Actions taken during each phase.
    - Impact assessment.
    - Costs incurred.
    - Regulatory notifications made.
- **Analysis:** Conduct a "lessons learned" review meeting with the Incident Response Team and relevant staff to discuss:
    - What worked well?
    - What could be improved?
    - Why did the incident occur?
    - How can we prevent similar incidents in the future?
- **Action Plan:** Develop an action plan based on the lessons learned, including updates to policies, procedures, technology, or training.
- **Policy Review:** Review and update this policy and related security policies as necessary.

Data Breach Notification Procedures

If a security incident involves a data breach (i.e., unauthorised access to, or disclosure, alteration, loss, or destruction of personal data), the Incident Response Lead will follow these steps, guided by GDPR requirements:

1. **Assess Risk:** Determine the likelihood and severity of the risk to the rights and freedoms of individuals.

2. **Notification to ICO (Information Commissioner's Office):** If the breach is likely to result in a risk to individuals, the ICO will be notified within **72 hours** of becoming aware of the breach. This will be done via the ICO's online portal.
3. **Notification to Individuals:** If the breach is likely to result in a *high risk* to individuals' rights and freedoms, the affected individuals will be informed directly without undue delay. This notification will include clear advice on steps they can take to protect themselves.
4. **CQC Notification:** If the breach impacts service users or could affect the delivery of safe care, CQC will be notified according to their guidance (e.g., as a significant event or safeguarding concern if applicable).
5. **Documentation:** All data breaches, regardless of whether notification is required, will be fully documented.

Communication Plan During an Incident

- **Internal Communication:**
  - Regular updates to senior management and affected staff.
  - Clear instructions to staff on actions to take or avoid.
- **External Communication:**
  - **ONLY** the Incident Response Lead (or designated spokesperson) will communicate with external parties (e.g., regulatory bodies, police, media, affected individuals).
  - All external communications will be carefully considered, accurate, and consistent.

Policy Review

This Security Incident Response Policy will be reviewed at least annually, or immediately following any significant security incident or changes to our operations or legal/regulatory landscape.

Paul Battershall
General Manager