jrhsupport

PROTECTIVE MONITORING POLICY

PROTETIVE MONITORING POLICY

Introduction
At JRH Support, we are committed to providing high-quality, safe, and secure social care services. This commitment extends to protecting the confidentiality, integrity, and availability of all information and systems we use, particularly those containing sensitive service user and staff data.

This Protective Monitoring Policy outlines our approach to monitoring our IT systems, networks, and activities to detect, prevent, and respond to potential security incidents, unauthorised access, or misuse of resources. It aims to safeguard our data, maintain compliance with relevant regulations (e.g., GDPR, CQC requirements), and ensure business continuity.

Scope
This policy applies to all IT systems, networks, devices (company-owned and, where applicable, personal devices used for work purposes), applications, and data owned or managed by JRH Support. It applies to all employees, contractors, and anyone else who accesses or uses our IT resources.

Policy Objectives
The objectives of protective monitoring at JRH Support are to:

- **Detect Security Incidents:** Identify suspicious or malicious activities that could indicate a data breach, system compromise, or unauthorised access.
- **Prevent Misuse:** Deter and identify unauthorized use of company IT resources or violations of company policies.
- **Ensure Compliance:** Support compliance with data protection regulations (e.g., GDPR), CQC fundamental standards, and other relevant legal and contractual obligations.
- **Aid Investigation:** Provide essential data for forensic analysis and investigation in the event of a security incident.
- **Maintain System Performance:** Monitor system health and performance to ensure reliable and efficient service delivery.

Principles of Protective Monitoring
- **Purpose-Driven:** Monitoring will be conducted for legitimate security and operational purposes only.
- **Proportionate:** Monitoring activities will be proportionate to the risks identified and the sensitivity of the data involved.
- **Transparent:** Where legally permissible and practically feasible, staff will be informed about the nature and purpose of monitoring.
- **Secure:** Monitoring data will be collected, stored, and processed securely to prevent unauthorised access or tampering.
- **Confidential:** Access to monitoring data will be restricted to authorised personnel only.
- **Regular Review:** Monitoring systems and procedures will be regularly reviewed and updated.

Areas of Monitoring
JRH Support will implement protective monitoring in the following key areas:

1. **System & Application Logs:**

- **What:** Collection of logs from critical servers, firewalls, anti-virus software, and key applications (e.g., care management system).
- **Focus:** Login attempts (success/failure), administrative actions, access to sensitive data, system errors, software installations/changes.
- **Retention:** Logs will be retained for a minimum of 60 days to support investigations.

2. **Network Activity (where feasible and necessary):**

- **What:** Monitoring firewall logs.
- **Focus:** External access attempts, unusual outbound connections, high volumes of data transfer.
- **Tools:** Firewall logs.

3. **User Activity (Auditing):**

- **What:** Monitoring of user actions on critical systems and applications.
- **Focus:** Access to service user records, modification of sensitive data, attempts to access restricted areas, login times and locations.
- **Rationale:** To detect unauthorised access, data manipulation, or policy violations. This is particularly important for CQC compliance regarding data access.

4. **Anti-Virus/Anti-Malware:**

- **What:** Centralized monitoring of anti-virus software across all company devices.
- **Focus:** Detection of malware, virus outbreaks, and successful/unsuccessful remediation actions.
- **Alerts:** Immediate alerts for critical threats.

5. **Backup & Recovery Systems:**

- **What:** Monitoring of backup job successes and failures.
- **Focus:** Ensuring data is regularly and successfully backed up and that recovery processes are viable.

Monitoring Technologies & Tools

For a small social care company like JRH Support, sophisticated Security Information and Event Management (SIEM) systems are an overkill. We will leverage more accessible and proportionate tools:

- **Built-in System Logging:** Utilising native logging features of Windows Servers, network devices, and applications.
- **Cloud Service Logs:** When using cloud-based care management systems or other critical software, we will review their built-in audit logs and monitoring features.
- **Managed Firewall/Router Logs:** Reviewing logs from our internet gateway device.
- **Anti-Virus Console:** Centralized management and reporting from our anti-virus solution.

Data Handling and Retention

- **Access:** Access to monitoring data will be strictly limited to authorized personnel ([e.g., Senior Management, with a valid need-to-know]).
- **Security:** Monitoring data will be stored securely, protected from unauthorised access, modification, or deletion.

- **Retention:** Logs and monitoring data will be retained for a period of 60 days unless required for an ongoing investigation or legal hold. After this period, data will be securely disposed of.

Alerting and Incident Response

- **Alerts:** Critical security events (e.g., multiple failed login attempts on a sensitive system, detection of critical malware) should be communicated to the General Manager.
- **Response:** Upon detection of a suspicious activity or alert, the incident response will consist of investigation, containment, eradication, recovery, and post-incident review.
- **Reporting:** All significant security incidents detected through monitoring will be documented and reported to the General Manaer.

Staff Awareness and Training

All staff will receive training on:

- The importance of data security and their role in it.
- The fact that protective monitoring is in place and its purpose.
- Their responsibilities regarding the acceptable use of IT resources.

Policy Review

This Protective Monitoring Policy will be reviewed at least annually, or more frequently if there are significant changes to our IT infrastructure, services, or regulatory requirements.

Paul Battershall
General Manager