Metier Integration Services

Incident Response Plan

1. Purpose and Scope

This plan covers Data Breaches, Ransomware Attacks, Insider Threats and Accidental disclosure of both Metier data and data relating to customer installation.

The purpose of this plan is to ensure:

- The impact of such incidents are minimised,
- The protection of sensitive data
- Maintaining business continuity

In addition when incidents occur then processes are reviewed and improved on.

2. Roles and Responsibilities

Those dealing with any reported or identified breaches or potential breaches shall include (see contact information)

- Metier Internal Management – Responsible for co-ordinating the response and making key decisions during any incident.
- The Clinical Safety Officer (employed through 8 Fold Governance) – to advise on any aspects affecting Patient Safety.
- Our CISSP Accredited consultant who provides annual IT and Security Training and support
- Hiscox with whom we have Business Insurance, £10M Professional Indemnity Insurance, Cyber Security and Data Insurance (£100,000 cover) and Crisis Containment Cover.

3. Incident Classification and Prioritization

Any incident will be assessed and classified (e.g., Informational, Low, Medium, High, Critical) based on factors such as data sensitivity, how many individuals affected, systems compromised and potential damage.

Severity	Description
Critical	A critical severity vulnerability is defined as one that leads to the full immediate compromise of the system or critically sensitive data.
High	A high severity vulnerability is defined as one that can cause major disruption on a network or target which may lead to the target or sensitive data being compromised.
Medium	A medium severity vulnerability is defined as one that may disclose further information that could lead to an attack or may decrease the overall security of the network or target.
Low	A low severity vulnerability is defined as one that may not be an immediate threat to the company. However, the company should review the information and determine the correct course of action.
Informational	An informational severity vulnerability is defined as one that has no direct security impact but is recommended to be remediated.

Incident responses will be prioritised based on the classification and taking into account business impact, data criticality, and urgency and the potential availability of remediation.

4. Incident Detection and Reporting

Incidents may be identified either though an observed issue internally – please see staff code of conduct document outlining responsibilities to report any potential issues immediately – or by being alerted from an external party - see recommended methods of reporting

Reporting - initially this should be to the two named Metier Directors

James Collins 07800 913330

Tony Hill 07740018824

Email -ig@metier.it or 03450 690000

After a notification has been received this will be triaged in accordance with section 3 to determine a classification and prioritised next actions..

5. Incident Response Phases

Preparation: We have established policies and 100% of staff have completed annual IT and Cybersecurity training and we have this policy for responding to incidents.

Identification: Once reported, we will investigate if an incident has actually occurred including gathering evidence, analysing data and determining the type and scope of the incident.

Containment: This includes a range of strategies for short-term and long-term containment to limit damage.

Eradication: Taking the required steps to remove the root cause of the incident.

Recovery: Implementing procedures to restore affected systems and return to normal operations. .

Post-Incident Activity: Conduct a post-mortem analysis to identify lessons learned and improve security measures.

6. Communication Plan

Internal Communication: All members of staff will be alerted once an incident has been confirmed - along with any assigned tasks - after post incident analysis has been conducted then feedback will be issued with any changes to procedures and any further training as required.

Where email has been compromised then more appropriate communications will taken place either by phone, SMS or WhatsApp

External Communication: We will contact third parties as appropriate for advice and assistance including notifying customers where necessary.

7. Documentation and Reporting

We will maintain a log of all reported incidents - where confirmed we will maintain detailed records of all actions taken during an incident, including timelines, affected systems, and remediation steps.

We will issue a report post incident summarising the incident's impact, response actions, and lessons learned. As above these will be shared with relevant stakeholders for review and compliance purposes.

8. Testing & Review

As part of our Business Continuity testing, we use the National Cybersecurity Centre "Exercise in a box" and conduct simulated incident response exercises to test the plan's effectiveness and the response team's readiness.

We regularly review and revise plans to reflect changes in the organisation, technology, or regulatory landscape. We also keep a business incident risk log.

Incidents are very rare, but we always look to incorporate feedback from post-incident reviews and testing to refine the plan and strengthen our security posture.

9. Contact Information:

Metier responsible Directors

James Collins 07800 913330 james.collins@metier.it

Tony Hill 07740018824 email tony.hill@metier.it

8 Fold Governance - providing Clinical Safety Officer asaService – Tel 01273 569172 email **info@8foldgovernance.com**

Information Commissioners Office(ICO) : Telephone helpline on 0303 123 1113 Make a complaint | ICO. website

Hiscox Policies under Policy number: PL-PSC10003230822/01

Claims - Tel 0800 280 0351 8:30am – 5:30pm Monday to Friday or email claims@hiscox.co.uk

Hiscox Customer Relations Telephone: 0800 1164 627 Address: The Hiscox Building Peasholme Green York YO1 7PR UK Email: customer.relations@hiscox.com