D5 – Cyber Incident Response Process

Applicant to detail their cyber incident response process including how customers are notified.

2 page A4 Arial 11 2%

Excellent scores will be awarded where Applicants robustly;

- *Details a well-documented plan and process.*
- *Evidence that the plan and process is managed (reviewed and tested) periodically no less than annually.*
- *Detail when and how they would notify clients, providing an interface for the Company CSIRT (Cyber Security Incident Response Team)*
- *Details when the plan was last tested and describes and evidences any lessons learnt as part of this frequent testing plan.*

Delivering what we promise

We are ISO 27001 certified and have an information security management procedure, a Cyber Security Incident Response (CSIR) Plan and CSIR Playbook in place which are fully embedded into all our IT processes and refer to how our managed service provider will be required to classify reported event. We have a corrective actions procedure which highlights how we investigate reported issues to identify the root cause and develop lessons learned.

There is a CSIR team in place via our Cyber Security Incidence Response Plan to manage incidents. The plans are tested annually.

We also have ISO 22301 certification, and as part of compliance monitoring, we have a schedule of exercising and testing regime in place for that. We further have a log of security incidents and events which we regularly review and create reports on incidents with lessons learned to ensure a recurrence is avoided. We have a fully trained in-house information security team who work alongside our managed service provider in dealing with security incidents.

The policies involved in this process are as follows.

MGS-POL-DP-003 Data Breach Policy

MGS-PRO-IT-005 Cyber Security Incident Response Plan

MGS-PRO-IT-006 MGS CSIR Plan Playbook

MGS-PRO-IT-009 Critical Systems Recovery Plan

An assumed Breach test was managed in July 2023 with the assistance of our BT SOC to test how our CrowdStrike defences coped with an intrusion, and when a full response would be called.

The test proved our defences worked well against Identity appropriation and attempts to traverse the network. Some actions were agreed to resolve in the next builds for the Laptops, the speed of response between SOC and Service desk. When escalations should be enforced.

Clients are informed of a Breach via the guidelines with the Data Breach procedure. Which is up 72 hours where applicable.