Disaster Recovery Policy

Disaster recovery is the ability to respond to a major incident or disaster by implementing a plan to restore the Company's critical business functions including information system uptime, data integrity and availability, and business continuity are resumed and maintained as soon as possible

Whilst we at Iconis Learning face few potential hazards that could have a detrimental effect on its ability to function, it is important that these to be addressed. Some risks can be anticipated; others cannot. Nevertheless, we must be able to address proactively any emergency situation regardless of its nature or origin.

In the event of an actual emergency situation, modifications to this document may be made to ensure physical safety of our people, our systems, and our data.

Objectives

This policy enables Iconis Learning to develop, implement and monitor arrangements in the event of an emergency to ensure that and business continuity are resumed and maintained as soon as possible, specific focus areas to include:

Pandemic

Associates will be advised to stay at home if they are sick and displaying flu-like signs/symptoms or, as a precaution sent home, at the earliest opportunity should this commence in the workplace to reduce the likelihood of further spread of the disease to the workforce.

In the event that the intended consultant/facilitator is unable to attend (e.g., illness), Iconis will provide a fully briefed and experienced alternative consultant/facilitator from the Iconis Team, or postpone the assignment, whichever the client prefers. However, Iconis accepts no liability for any losses, howsoever incurred by the client as a result of the cancellation of an assignment by either party.

If staff and associates can safely work from home, then this will be identified and encouraged. Opting for video-conferencing or tele-conferencing where possible instead of holding meetings, if in agreement with all

Cyber attack

The following steps have been put into place in the event of any unforeseen malicious or accident cyber attack

Step 1: Prepare for incidents

Malicious and accidental, can occur in many ways therefore it is impractical to develop detailed step-by-step instructions to manage every type of incident, as the list could be endless. We have prepared Iconis Learning for the most common threats and we have developed plans to handle those incidents most likely to occur.

Step 2: Identify what's happening

The first step in dealing effectively with an incident involves identifying it. That is, how can you detect that an incident has occurred (or is still happening)? On the first sign of any Cyber Attack the first contact will be with our IT Consultant James Staples of Fernwood Projects Ltd who will identify the problem and instruct the team accordingly. The systems we use have built in security and will alert us of unauthorised log in attempts.

Step 3: Resolve the incident

James is responsible and with the wider teams support to get our organisation back up-and-running as soon as possible to confirm that everything is functioning normally and fix any problems.

Step 4: Report the incident to wider stakeholders

Once a cyber security incident has been resolved, formal reporting may be required to both internal and external stakeholders e.g. clients, associates or in certain incidents that you're the Information Commissioner's Office (ICO).

IT Systems

Our mission is to ensure information system uptime, data integrity and availability, and business continuity.

Iconis Learning together with James Staples of Fernwood Projects Ltd have designed a robust and secure IT disaster recovery plan. The disaster recovery plan covers all essential and critical infrastructure elements, systems and networks, in accordance with key business activities.

All associates are made aware of the disaster recovery plan and their own respective roles.

Infrastructure

We used cloud-based services with enhanced levels of security, wherever available, such as multifactor authentication and unique passwords and ensure all associates with accounts adhere to our IT Security policies and procedures

Responsibilities

Jan Cowan, Director has overall responsibility for Disaster Recovery planning.

All associates must take normal management action to assess and mitigate risks at all times. This Policy and the accompanying Codes of Practice do not exempt them from this responsibility.

Iconis Learning will maintain an up-to-date central Disaster Recovery Plan and will be prepared for emergencies which will be reviewed annually