Adapt Consulting Company Limited

DISASTER RECOVERY PLAN

INTRODUCTION

AdaptConsultingCompany is a small business and the summary disaster recovery plan / business continuity plan reflects that fact.

Specifically we have no premises, no employees, no networks, no tangible products. As a consultancy we operate using a laptop and mobile phone.

We operate a strict Data Protection Policy to safeguard the data on the laptop and mobile phone and a strict Information Security Policy to safeguard the devices themselves and information getting in or out.

PLAN STORAGE

The plan is held on a secure, encrypted laptop, with separate secure, encrypted back-up. It is also held on-line so that it can be referenced from any location. It is also kept public for reassurance of our customers and the ICO Office, which requires businesses to have a disaster recovery plan.

PLAN REVIEW

The plan is reviewed annually along-side a review of related policies and procedures including Data Protection Policy and Information Security Policy.

CIRCUMSTANCES

This Plan will be activated in response to an incident causing significant disruption to normal service delivery/business, particularly the delivery of key/critical activities. Examples of circumstances triggering activation of this Plan include:

1. Loss of key staff or skills e.g. above normal levels of absenteeism due to illness
2. Loss of critical systems e.g. ICT failure
3. Denial of access, or damage to, facilities e.g. loss of a building through fire
4. Loss of a key resource e.g. a major supplier vital to the delivery of a key service

Adapt Consulting Company

RESPONSIBILITY FOR ACTIVATION

The disaster recovery plan / business continuity plan owner is Tim Rogers.

INCIDENT MANAGEMENT

1. Purpose of the incident management phase
2. Protect the safety of staff, visitors and the wider community
3. Protect vital assets e.g. equipment, data, reputation etc
4. Ensure necessary communication takes place
5. Support the Business Continuity phase
6. Support the Recovery and Resumption phase

Key actions

1. Evacuate the building if necessary
2. Ensure all staff report to the Assembly Point.
3. Call emergency services (as appropriate)
4. Check that all staff, contractors and any visitors have been evacuated from the building and are present. Consider safety of all staff, contactors and visitors as a priority
5. Ensure log of incident is started and maintained throughout the incident phase
6. Record names and details of any staff, contractors or visitors who may have been injured or distressed in the incident.
7. Forward details of any fatalities or injuries in the incident to HR (depending on scale of incident) and agree action that will be taken.
8. Assess impact of the incident to agree response / next steps

Generally we are located at home or on a client site. When operating on a client site we will generally follow their H&S and disaster recovery procedures (which is usually a contractual requirement)

COMMUNICATION ACTIONS

In the event of an incident and this plan being activated, the following people should be contacted. Nature of contact will depend on the incident type and time it has occurred.

1. ICO and "Data-Subjects" – if a disaster recovery / business continuity issue constitutes a data breach.
2. Customers – if a disaster recovery / business continuity issue affects them.

3. Insurance Company – AdaptConsultingCompany has insurance for such events

Generally the communication will cover
1. Incident is taking place
2. Action being taken
3. Impact on the service
4. Indication of any press interest
5. Areas they can support service

DATA BREACH

Where there is a data breach communication will cover the actions required by GDPR, as outlined below.

https://gdpr-info.eu/art-33-gdpr/

In the case of a personal data breach, AdaptConsultingCompany (the controller) shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

AdaptConsultingCompany shall
1. describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
2. communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
3. describe the likely consequences of the personal data breach;
4. describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

Adapt Consulting Company

ACTIONS TO SUPPORT BUSINESS CONTINUITY

Key actions

1. Recover vital assets/equipment to enable delivery of critical activities
2. Assess the key priorities for the remainder of the working day and take relevant action
3. Inform staff what is required of them
4. Publicise the interim arrangements for delivery of critical activities

ACTIONS TO SUPPORT RECOVERY AND RESUMPTION

Key actions

1. Take any salvage/asset recovery actions that are appropriate
2. Continue to log all expenditure incurred as a result of the incident
3. Seek specific advice/ inform your Insurance Company

PURPOSE OF THE BUSINESS CONTINUITY PHASE

The purpose of the business continuity phase of response is to ensure that critical activities are resumed as quickly as possible and/or continue to be delivered during the disruption.

The Business Impact Analysis (BIA) for AdaptConsultingCompany sets out details of critical activities and the resources required to deliver them both in 'business as usual' and in crisis situations. The Business Continuity Team will refer to the BIA to help inform the business continuity response that is required.

EVALUATE INCIDENT

Key actions

1. Identify any other staff required to be involved in the BC response
2. Evaluate the impact of the incident
3. Plan how critical activities will be maintained.
4. Log all decisions and actions, including what you decide not to do and include rationale
5. Log all financial expenditure incurred
6. Allocate specific roles as necessary

7. Secure resources to enable critical activities to continue/be recovered
8. Deliver appropriate communication actions as required

CRITICAL ACTIVITIES

Key actions (depends on output from incident evaluation)

1. Replace hardware and software
2. Restore data from encrypted backups

NON-CRITICAL ACTIVITIES

Key actions (depends on output from incident evaluation)

- Restore library of books, texts etc.

RECOVERY AND RESUMPTION ACTIONS

This is a point where we are no longer in disaster recovery plan / business continuity plan, but now business-as-usual

This requires some form of hand-over or transition process

1. Agree and plan the actions required to enable recovery and resumption of normal working practises
2. Continue to log all expenditure incurred as a result of the incident
3. Respond to any long terms support needs of staff
4. Carry out a 'debrief' of the incident and complete an Incident Report to document opportunities for improvement and any lessons identified
5. Review this Continuity Plan in light of lessons learned from incident and the response to it
6. Publicise that there is now 'business as usual'