|  |
| --- |
| Apogee Property and Utility Consultants |
| Website Disaster Recovery Plan (DRP) |
|  |
| **Michael Minton** |
| **Published – 11/11/2021** |

**Revised – 17/11/2021**

|  |
| --- |
| *This Disaster Recovery Plan covers the website built by Shropshire ITC Limited, which went live in November 2021. Includes data, remote or locally stored.* |

# **Introduction**

This document details the policies and procedures for Apogee Property and Utility Consultants in the event of a disruption to critical services or damage to the public website, as developed and published by Shropshire ITC Limited. These processes will ensure that those services are recoverable to the right level and within the right timeframe to deliver a return to normal operations, with minimal impact on the business.

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

# **Policy statement**

Corporate management has approved the following policy statement:

* The company shall implement relevant continuity and recovery planning.
* All continuity and recovery plans should cover essential and critical infrastructure elements, systems, and networks, in accordance with key business activities.
* The plans should be periodically tested in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed.
* All staff must be made aware of the plans and their own respective roles.
* The continuity and recovery plans are to be kept up to date to consider changing circumstances.

# **Definitions**

* All times stated are chronological, assuming 24 hours in any one day.

**Business Impact Analysis**

This section is about identifying important services needed for the website including the business impact if interrupted.

|  |  |  |
| --- | --- | --- |
| **Website/Service/Delivery** | **Supporting Service** | **Impact when interrupted, incl time when it becomes unacceptable** |
| *Public Website* | *Hosting* | *Accessibility to the website. Unacceptable after 48 hours.* |
|  |  |  |
| *Custom Functions* | *Code* | *Will stop internal, customer and quoting access immediately. Unacceptable after 24 hours.* |
|  |  |  |
| *Customer & Commerce* | *System Data* | *Will stop customer and quoting access immediately. Unacceptable after 4 hours.* |
|  |  |  |
| *Geolocation Functions* | *Map Layer Data* | *Will stop quoting immediately. Unacceptable after 4 hours.* |
|  |  |  |
| *Direct Supplier* | *All Services* | *Loss of Support. Unacceptable after 2 weeks.* |
|  |  |  |
| *Indirect Suppliers* | *All Services* | *No access immediately. Unacceptable after 24 hours.* |

**Business Impact Analysis (cont’d...)**This section helps when identifying the business needs regarding availability, recovery times, backup, data integrity and data confidentiality.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Supporting Service** | **Business need of:** | |  |  |  | | |  |
|  | **Availability** | **RTO** | | **RPO** | | **Data Integrity** | **Data Confidentiality** | |
| *Hosting* | *99,5%* | *48 h* | | *1 h* | | *Medium* | *Low* | |
| *Code* | *99,1%* | *4 h* | | *24 h* | | *Medium* | *Medium* | |
| *System Data* | *99,9%* | *4 h* | | *1 h* | | *Very high* | *Very high* | |
| *Map Layer Data* | *99,9%* | *4 h* | | *1 h* | | *Very high* | *Very high* | |
| *All Services - Direct* | *99,9%* | 2 w | | 2 w | | *Low* | *Low* | |
| *All Services - Indirect* | *99,9%* | 24 h | | 48 h | | *Low* | *Low* | |

The Recovery Time Objective (RTO) is the time frame agreed upon to get the business process/delivery operational again after an interruption (including all recovery actions).

The Recovery Point Objective (RPO) is the acceptable amount of time you can lose in an incident without being able to recover/restore it or to recover to a previous “point in time”.   
(This sets the demands on backup/restore/replication solutions.)

Data integrity is the demand that information/services stays intact and isn’t changed intentionally or unintentionally.

Data confidentiality is the demand that ensures that information is not made available or disclosed (intentionally or unintentionally) to others.

**Key Contacts**

| **Name,** Service | **Contact Information** | |
| --- | --- | --- |
| **Aden Lord** | Supplier | Shropshire ITC Limited |
| Hosting | Telephone | 01743 562200 |
|  | Website | www.shropshireitc.co.uk |
|  | Email address | supportdesk@shropshireitc.co.uk |
|  |  |  |
| **Michael Minton** | Supplier | Shropshire ITC Limited |
| Code | Telephone | 01743 562200 |
|  | Website | www.shropshireitc.co.uk |
|  | Email address | supportdesk@shropshireitc.co.uk |
|  |  |  |
| **Michael Minton** | Supplier | Shropshire ITC Limited |
| *System Data* | Telephone | 01743 562200 |
|  | Website | www.shropshireitc.co.uk |
|  | Email address | supportdesk@shropshireitc.co.uk |
|  |  |  |
| **Michael Minton** | Supplier | Shropshire ITC Limited |
| *Map Layer Data* | Telephone | 01743 562200 |
|  | Website | www.shropshireitc.co.uk |
|  | Email address | supportdesk@shropshireitc.co.uk |
|  |  |  |
| **Michael Minton** | Supplier | Personal Contact |
| *All Services - Direct* | Telephone | 07792 692322 |
|  | Website |  |
|  | Email address | mikeminton.uk@outlook.com |
|  |  |  |
| **Vince Dovey** | Supplier | Shropshire ITC Limited |
| *All Services - Indirect* | Telephone | 01743 562200 |
|  | Website | www.shropshireitc.co.uk |
|  | Email address | Vince.dovey@shropshireitc.co.uk |

**Disaster Recovery Procedures**

**Procedures Index**

Depending on the incident, one or more of the following disaster recovery procedures may be activated:

|  |  |  |  |
| --- | --- | --- | --- |
| Page | Procedure | Page | Procedure |
| 7 | Ransomware detected on one or more computers/servers |  |  |
| 9 | Supplier Key Personnel – Unforeseen absence/loss of Personnel. |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |  |
| --- | --- |
| **Disaster Recovery Procedure:** | |
| Ransomware detected on one or more computers/servers | |
| **Possible Causes:** | Malware |
| **Risk Areas:** | Storage systems and laptops |
| **Impact:** | Lost or corrupted data |

|  |  |
| --- | --- |
| **Prevention** | * Identify potential weaknesses of your network and IT environment. * Implement the use of VPN connections for all mobile employees. * Employees that service critical IT services should have the maximum access required to be able to complete their job. * Implement a backup and recovery plan for all vital data using the 3-2-1 strategy:   + 3 - Retain a minimum of three copies of data.   + 2 - Store data on two different types of media.   + 1 - Secure one copy of your backups offsite. * Test backups regularly to ensure proper configuration, which will limit the impact of a data breach and accelerate the recovery process. * Isolate critical backups from the network (air gap) for maximum protection. * Implement copy-on-write file systems (NetApp WAFL – Linux ZFS) or WORM features in NAS systems or appliances. * Patch critical operating systems, antivirus, security, and backup software as soon as possible. * Establish ongoing cybersecurity training for users and admins to identify phishing emails. |

|  |  |
| --- | --- |
| **Plan of action** | * Disconnect all ransomware-affected systems from the network. * Never pay the ransom! Paying the criminals doesn’t guarantee that you will get your data back. In many cases (and most definitely, if it is a ‘ranscam’ or wiper malware) you will not get your data back, leaving you with no data. * Do not try to decrypt the data by yourself. Contact Ontrack for advice. * Check your backups. Even if your backup is missing after a ransomware attack, you should never rule out the possibility of recovery. Possible solutions depend on the type of media or storage system, and the type of ransomware. * Identify the issue, coordinate initial response. * Seek advice immediately by contacting Ontrack. * Follow the instructions in detail. |

|  |  |
| --- | --- |
| **Disaster Recovery Procedure:** | |
| Supplier Key Personnel – Unforeseen absence/loss of Personnel. | |
| **Possible Causes:** | Illness, Death, Accident, Other |
| **Risk Areas:** | Code & Maintenance |
| **Impact:** | Low |

|  |  |
| --- | --- |
| **Prevention** | * Supplier will have replacement staff for general coding and maintenance issues. * All third-party key suppliers/services must be documented, and these documents must be tested and maintained for the life of the project. * Key personnel that service critical project areas should have the maximum access required to be able to complete their job. * Third party services must have more than one remote login protocol, and when available this should be 2FA. * Implement a backup and recovery plan for all vital data using the 3-2-1 strategy:   + 3 - Retain a minimum of three copies of data.   + 2 - Store data on two different types of media.   + 1 - Secure one copy of your backups offsite. * Test backups regularly to ensure proper configuration and restoration, which will limit the impact of losing key personnel and this will accelerate the recovery process/fix times. |
| **Plan of action** | * Monthly test process for third party suppliers and services documents. * Fortnightly login to remote services using all user accounts and 2FA where available. * Fix any remote access issues if any should occur. * The supplier’s key personnel should have site of the regular backup process, and this should be tested once per quarter. * Print backup keycodes for all 2FA accounts and store onsite and offsite. *Offsite locations:* Mike Minton Home Aden Lord Home *Onsite locations:* Shropshire ITC Limited * In the event that Shropshire ITC cannot resolve any code or site recovery with 24 hours and there is no estimated or reasonable timeframe for a fix. Apogee may refer the situation to Insimbi consulting Stuart Steele in order to attempt to remediate matters. |

**Appendix  
  
Onsite/Offsite Locations:  
  
*Shropshire ITC Limited***  
Unit 5d, Leaton Ind Estate  
Shrewsbury  
Shropshire  
SY3 5AP  
  
  
***Michael Minton (Home)***  
Tinkerbell, Castle Lane  
Bayston Hill  
Shrewsbury  
Shropshire  
SY3 0NJ  
  
***Aden Lord (Home)***  
(Available upon request)

**Backup Locations:  
  
*Website Functional Files***Azure - Shropshire ITC Limited  
Acronis – Cloud Backup  
Local – Mike Minton Development Computer  
USB – Mike Minton Dev  
OneDrive – Development  
  
***Database Files***  
Azure - Shropshire ITC Limited  
Acronis – Cloud Backup  
Local – Mike Minton Development Computer  
USB – Mike Minton Dev  
OneDrive – Development  
  
***Map Data Files:***  
Mongo DB Cloud Platform  
Acronis – Cloud Backup  
Local – Mike Minton Development Computer