Incident planning

Version: v1.1
Author: Clive Simpson
Date: 06/11/2015

Version: v1.2
Author: John Walder
Date: 01/04/2018

Reviewed
Author: Clive Simpson
Date: 04/09/2023

To prevent any kind of an incident affecting the way Redtitan supports its customers and to ensure the continuation of the business the following plan is in place.

Contingency

To prevent issues affecting the head office or any of the satellite offices the following precautions have been taken. All RedTitan employees have the ability to work from home and some do as part of our normal business. In the event of employees being unable to attend the head office they are instructed to work from home. This includes during times of pandemic employees would work from home to avoid unnecessary contact. In the event of a disruption to any employees home office they can work at the head office or if more convenient at another employees home office which are spread across the south east of England. All offices have high speed internet access and access to the in-house server. RedTitan headquarters are based in a Regus managed office, this allows Redtitan employees to access any Regus virtual office and work from there.

Disaster recovery

The In-house server located at the head office contains all the source code for all Redtitan software products. Copies of this code are also taken weekly and are removed from site. The entire server is backed up onto an independent NAS drive and twice a year a mirror of the server disk is taken. In addition each programmer keeps backups of their work at their home office.

The in-house server also keeps a backup copy of the licences we issue which are held on the virtual server in the cloud, see below and we keep customer files where we have permission to retain them for the purposes of diagnosing faults with the software. The in-house server is only accessible via a secure VPN connection and access to most areas is restricted on a need to know basis.

In addition there is an annual backup of all source code and compiled objects at NCC which is accessible to customers who sign up to an escrow agreement with NCC.

Our sales server is hosted on a Microsoft Azure VM and is geo-located. In addition the server is backed up by the Microsoft Azure backup vault. As well as a second backup being located in the RedTitan head office. This contains our web server, email server and our licensing system. No customer information is stored on this server other than the information required by the licensing system which does not include any bank details or other financial information.

RedTitan does not provide any ongoing in-house services to customers other than to provide permission to use the software in the event that the customer changes the hardware. As the licensing server is on the cloud and geo-located this system is always available.

Incident management

In the event of an incident that affects one or more of our customers then the primary contact of that company would be contacted by whatever means was available to alert them to the incident.