OT Group Limited
Part of Paragon Group

BUSINESS CONTINUITY POLICY

Every business and organisation can experience a serious incident that can prevent it from continuing normal operations. This can happen any day at any time. The potential causes are many and varied: they may include but are not limited to flood, fire, explosion, computer malfunction, accident or acts of terrorism.

Each sales office operates its own plan for the loss of local resources. If for any reason the level of disaster dictates that any sales office is put out of action, then the central plan is to move all the work performed by that office to another sales office through the redirection of all lines of telecommunication. This ability is further enhanced by the fact that this workload can also be shared amongst remaining sales offices through our other inter office links, and the ability for our teams to work remotely from home.

The main central warehouse in Smethwick has fire protection, and two separate generators with the ability to operate independently across its three separate chambers. With a fall back site in Croydon with systems established and ready to operate.

Plans are in place to re-house any of OT Group's administrative functions in alternative office accommodation within other sites.

The company operates distributed computer systems using a combination of traditional tier 3+ data centres and cloud compute infrastructure.

All key systems are covered under a Business Continuity contract, with Daisy Corporate Services Trading Ltd. This contract provides for a total loss of a tier 3+ data centre, and the resumption of business at a dedicated Disaster Recovery suite, with all key systems replaced and operational within 8 hours. This includes restoration of backups that are held away from the central site.

Our Wide Area Network provides for all sites to be redirected into any site we designate as the recovery site for OT Group. The network has multiple links to each site, plus additional levels of fall back through different technology, should the main infrastructure fail.

Our E-Commerce servers are hosted at a number of Tier 3 and 4 hosting centres and all have appropriate resilience and protection, ensuring high availability.

Our telecom system is fully redundant with automatic failover between controllers which supports in call failover. All calls are automatically redirected to alternative sites in case of a local issue forcing closure or high call volumes.

OT Group's Primary E-Commerce solution is Smartpad and is hosted in the Azure cloud and is designed using Scale Set technology. The system provides a fully featured, business to-business, stationery-ordering platform to OT Group customers. The system is closely integrated to our back office systems via a comprehensive interface that provides bespoke customer pricing and integrated order placement. This system is administered and supported by a dedicated in-house Digital support team.

Email is hosted by Google (Gmail) which offers multiple layers of resilience and security. Our key systems are either virtualised using VMWare or are clustered to provide high availability using VMotion. All VM data is backed up using snapshot as this can be recovered on demand with RPO and RTO times in minutes. Where physical servers are deployed for legacy software these have warm standby equipment available. Key data is stored on our SAN (Raid5) disk array, with built in disk failover, multiple controllers with multiple fibre connections and is monitored in real time 24/7 as are all key systems.

The local and wide area networks are common to all business areas and have been designed to be resilient and flexible for future requirements.

The local area networks are all Cat5 Ethernet networks based around HP ProCurve for high-speed switches.

Secure wireless networks (WPA2-ENT) are in place at all sites to facilitate RDT devices used in the warehouses and Company owned remote equipment. Guest Wi-Fi requirements are met using a separate and secure SSID and VNet tunnelling.

The main warehouse has built in AP redundancy and can operate with the loss of up to 20% of available AP devices at any site. Each site has cold standby auto configured AP devices that can be deployed in case of failure.

Our Wide Area Network is MPLS. All sites have dual circuits and at our two major RDC units the circuits are fully diverse taking different routes and terminating at different points. Perimeter defense is managed by FortiGate next-generation firewalls, with all sites utilising a single breakout point. All internet traffic is controlled using Websense Triton software ensuring compliance with the Company's 'Use of the Internet' policy. All end points are protected using McAfee antivirus software and networks are protected by IDS/IPS using McAfee ePO orchestration.