www.aptlimited.co.uk

Crisis Management

The Mews | 6 Putney Common | London | SW15 1HL | United Kingdom
+44 (0)20 8246 4050 | enquiries.global@aptlimited.co.uk

APT is a Quality Assured Firm, ISO Certificate Number **ATCISO2150**.

Version:	**V3.0**		
Originator:	Andrew Clementson	Director of Operations	**February** 2022
Approved:	Charles Jamieson	Managing Director	**February** 2022

Transtelex Ltd

create translate go global

Crisis Management

APT Transtelex has in place key personnel who are responsible for restoring operations critical to the resumption of business. Primarily this incorporates strategically enabling access to data (client and project data, hardware & software), communications (incoming and outgoing), workspace, and other business needs after a natural or human-induced disaster.

Disaster recovery planning and implementation has been reviewed and coordinated by the Managing and Operations Directors of APT over the past twenty years and has been tested several times during this period.

We have sampled hypothetical and actual scenarios such as unexpected and sudden loss of communications and key personnel and have alternative working sites and backup data systems that enable the company to continue to function in such an event.

With the advances in information technology and todays reliance on business-critical information the importance of protecting irreplaceable data has become a commercial priority in recent years.

APT's Communications Server data is subject to backup up onto secure media on and off site. Data Restore of the information in the case of an event is monitored externally and in most cases the recovery can be undertaken very swiftly.

All current year client information relating to translation projects is backed up on additional hard drives. Any member of the Operations Team can access this immediately upon secure connection to these drives.

IT infrastructure is available remotely under the supervision of APT's Directors and the DR Planner can determine the most suitable recovery strategy for each system in the event of failure or crisis.

The following is a list of the most used strategies for data safeguarding.

- Backups on and off site
- Accessibility of backup communications and hardware systems, which keep both the data, and system replicated off-site, enabling continuous access to systems and data

In addition to preparing for the need to recover systems, APT also implements precautionary measures with the objective of preventing a disaster situation in the first place. These include:

- Local mirrors of systems and/or data and use of disk protection technology such as RAID
- Surge Protectors — to minimize the effect of power surges on delicate electronic equipment
- Multiple Uninterruptible Power Supply (UPS) to keep systems going in the event of a power failure
- Fire Prevention — Rigorously checked Fire and Burglar alarms
- Server and local ESET Anti-virus software and additional beskoe security measures
- Risk Assessment reporting