

**CHILTERN TRANSPORT
HEALTH, SAFETY & ENVIRONMENTAL POLICY**

1.10

IT – PROTECTION AND MANAGEMENT OF DATA POLICY

Our company recognises the importance of protecting and securing the integrity of our data.

Our local area network is protected by a router firewall. We regularly review our internet security with rigorous vulnerability profiling which includes file sharing and port probing. All firewall rules are created exclusively in-house by our own IT department to avoid the creation of unauthorised or malicious rules by third parties.

Each PC on our LAN also has its own firewall and antivirus software. Windows Defender is also installed on those computers running Windows XP or Vista.

All computers are set to automatically download both critical and recommended system and security software updates, both for operating system and installed software.

All computers are scanned for viruses and spyware on a weekly basis. Additional installed software components also protect continuously, scanning all files opened, saved, copied, and protecting the system areas of each pc. Any threat activation is blocked and the threat removed.

All incoming e-mails and attachments are also scanned for viruses. Any malicious content or potentially harmful files are quarantined and removed.

Any critical data is backed up by authorised members of staff. Several of these are completed every day to ensure against data loss or system failure.

A back up of data is taken every day and a copy is removed from our premises and held overnight by a Director.

Signed



Keith Croker - Director
Chiltern Transport & Warehousing Limited
Chiltern Transport (Northern) Limited

Date: 25 Nov 2014