

At Enfield Safety, we take IT Security seriously to ensure that there are no data breaches and business continuity. To enable this, we have got various systems in place:

- **Emails** - All incoming and outgoing emails are checked for viruses and if suspicious they are held on a cloud platform for our review.
- **Servers** - The main data servers are held in a restricted access area and they are all password protected. They have a program continually running to detect and isolate malware or suspicious files.
- **Remote Access** – To safely allow remote access, employees working from alternative locations can login through a 2 factor authentication process to access their workspace and prevent hacking.
- **ERP System** – Our system runs a backup starting at 6.30pm every evening. This runs onto a hard drive that is then swapped over the next day to ensure we always have an offline copy. An Enfield Safety Employee has the task of taking it home during non-working hours as a safeguard against fire / flood. Backups are also made ahead of any ERP system maintenance.
- **User Specific Data** – This is backed up onto a cloud platform in 30 minute intervals. A separate hard drive backup is also made of this data to enable a quicker restore time if a large amount of data needs to be recovered. This hard copy is also taken off site by the same employee during non-working hours.