
1 Principals
COMM-TECH understand the importance of data protection and have robust procedures in place to ensure our support and maintenance activities prioritise the integrity and security of our clients’ data.

2 Information security management
1. We apply industry standard best practice to our information security practices
2. We maintain a system of continuous security review and patching process appropriate to prevailing cyber threats
3. Our staff are vetted and trained in information security awareness
4. All hosted services are located in secure data centres in the UK
5. We meet the demands of relevant legislation

3 Risk Management
1. Required works to servers are fully risk assessed prior to commencement for liability to data disclosure as well as any danger posed to business continuity
2. Systems vulnerabilities are analysed and risk-assessed security breach.

4 Systems design
COMM-TECH systems have data integrity and security at their core, our systems are designed to:

1. protect the integrity of our clients’ informational assets using reliable hardware, maintained software and robust backup systems.
2. protect our clients’ informational assets from unauthorised access using granular file permissions
3. protect our clients’ informational assets from unauthorised access by using encryption and/or keeping them in a secure computing environment
4. ensure business continuity with minimal possible downtime in the event of software or hardware failure
5. record all server activity to inform forensic examination and patching strategies in the event of a data breach or unexpected downtime
6. be monitored closely to ensure wherever possible that we receive adequate warnings prior to hardware failure
7. fulfil our Service Level Agreements obligations