Executive summary

Purpose of this guide and who should read it

The purpose of this guide is to provide a framework for an appropriate Protection Plan for a Data Centre. It is intended for security professionals with responsibility for the protection of Data Centres. It will be of value to senior managers and Risk owners with responsibility for Data Centre protection, and for other specialists who directly implement protection measures.

Scope of this guide

The guide treats the protection of Data Centres holistically, covering the protection principles from initial site selection through to design, build, and operation. It covers all the elements required but does not set an exhaustive standard for protection as individual requirements will vary. Where CPNI provides authoritative subject guidance in other documents or references with Protective Marking these are referenced back to their source i.e. the CPNI extranet.

The protection approach

Data Centre protection should start with a Risk and Threat Assessment, which combines threats, hazards, vulnerability and weaknesses and sets controls proportionate to identified risks. From this an Operational Requirement is developed that is agreed by the business and from which protection is justified.

The Data Centre Guide treats people, processes and technologies as factors combining to deliver the physical security, personnel security and information security controls that will protect the Data Centre and the services it delivers.

Once in place, protection controls should be continually tested and revised to ensure that they remain relevant and responsive to the agreed Risk assessment.

The Data Centre site

The Data Centre requires a reliable, stable electrical power supply (backed up by generators and uninterruptable power supplies), a location that is as free from risk and hazard as possible, and the availability of diverse communications.

The site should provide a layered approach to security. With consideration given to security of the external environment and providing a secure perimeter. The facility should be further separated into appropriate security zones to protect the most critical and sensitive assets. These layers and zones will incorporate appropriate physical protection, detection and monitoring systems to deter, detect and delay any attacker.

Managing the Data Centre

Effective management of the Data Centre will depend upon a Risk Assessment and Protection Plan that is owned by executive management, appropriately managed and followed by all members of staff. Protection goes hand in hand with operational delivery that may also require a business resilience strategy incorporating business continuity and disaster recovery plans to ensure that an individual Data Centre does not become a single point of Corporate business failure.