

## SmartBackup Data Centre Information

Our servers are locked into the Web in a former NATO nuclear bunker, hidden in a low-risk countryside area. The bunker is situated on 18 acres of land and surrounded by concertina wiring in Kent, England. It is an impregnable fortress, sitting 30 metres below ground. It has concrete walls three metres thick, steel doors weighing over two tons which protect the servers and digital storage units within.



Layered on top of this physical inaccessibility is a 24-hour watch with guard dogs, CCTV and a series of sophisticated access controls that offer the ultimate in protection from a myriad of attacks, including crackers, terrorist attack, electro-magnetic pulse, electronic eavesdropping, HERF weapons and solar flares.

The bunker is designed to keep digital data available to you at all times. There are sufficient underground diesel tanks to keep the plant running for a solid three months without refuelling, and dual UPS systems capable of running the entire server facility for forty hours in the event of a power outage, to ensure there is no interruption to service during switchover.

### SECURITY

- **Physical Security**  
We run our hosting operations from cold war era nuclear bunkers, which are state-of-the-art installations, purpose built with security in mind and originally constructed as an integral part of the UK's strategic communications network.
- **Digital Security**  
The experience of our technical team in providing secure cryptographic solutions, combined with the Bunkers high level of physical security and client identification procedures, offer the ultimate in protection from a myriad of attacks.
- **Security Culture**  
We advocate to all our customers a specific set of security procedures and processes, to help ensure the integrity of your systems.

### DATA CENTRE INFRASTRUCTURE

The core principles behind the design of the datacentre are resilience and redundancy, with the aim of removing all single points of failure.

### ELECTRICAL SECURITY

There are two incoming 11,000 volt 3 phase electricity authority supplies with an auto changeover facility. The primary supply is a dedicated supply directly from the national grid and the secondary supply is a shared supply which also feeds the buildings above ground. The datacentre also has, at present, five generators and UPS support.

Upon failure of the primary supply (which has only occurred twice in 19 years) the incoming HV circuit breakers will, after 30 seconds, automatically change to the secondary supply.

### Distribution

Following transformation of the supply to 415V the outputs from the two transformers are brought together at a main switchboard, that in turn feeds three sub-main switchboards. Sub-main 1 supplying the technical load, sub-main 2 the plant and sub-main 3 general power and lighting.

### Emergency Power Generation

There are at present five generators on site, one above ground, diesel set and four underground battery powered units.

At present a project is underway to install a further 500kVA generator, which will be expandable to allow a further two 500kVA generators to be installed with N+1 redundancy. This will be a backup even to the secondary supply. There are five large bulk diesel tanks housed in the bunker extension, which have the capacity to store in excess of a quarter of a million gallons of fuel.

In the unlikely event of failure of both electricity supplies the generator will automatically start within 30 seconds and the electrical load will automatically transfer to it. Upon restoration of electricity supplies and verification of their stability, the load will be transferred back from the generator. There should be no interruption in the power supplies to client equipment during the changeover due to the UPS support.

### Electro Magnetic Pulse Protection

When detonated, a nuclear weapon generates an electromagnetic pulse (EMP). An EMP is an electromagnetic field that changes in intensity at up to 50kV per nanosecond, and can induce high-energy pulses in any conductor subjected to this changing field strength.

Although the high-energy pulse is short, the energy to be dissipated is sufficient to destroy unprotected communications and other electronic equipment. It is possible for a single explosion to induce damaging effects over an area of thousands of square miles in diameter. The bunker has a two-stage approach to protect against the effects of EMP:

**Zone 1** - Areas within the building structure but outside the EMP shield:

Provision of high-energy surge arrestors (voltage dependant resistors) has been made, for all conductors entering or leaving the building.

Screening of cable runs by means of armouring, braiding, conduit or trunking.

**Zone 2** - Areas within the EMP shield:

Shielding by means of a continuously welded 3mm thick, steel shield of all technical equipment areas.

All conductors entering this shield do so via a penetration plate and vault and have VDRs and RFI filters incorporated.

The EMP protection also serves to protect client equipment from mains data sniffing, which is a potential risk on unfiltered mains supplies.

### Earthing

Earthing throughout the building takes the form of a radial or tree system leading back to either the primary or vault penetration plate in zone 1 and zone 2 respectively. Earth electrode systems are installed at both penetration plates and are sized to dissipate satisfactorily the extremely large currents that would result from an EMP.



### Tempest Protection

It is possible for all electronic circuits to generate an electrical disturbance, signal or noise. This may be transmitted by radiation (through the air) or along conductors, cables pipes etc. This noise is known as Radio Frequency Interference (RFI). Generally RFI is only of nuisance value to other electronic equipment nearby. In the case of data processing and communications equipment the consequences could be more serious. It is possible for RFI to be generated by equipment, which can be detected and interpreted using sensitive espionage devices at great distance from the equipment producing such interference.

TEMPEST is a protection measure that prevents electronic eavesdropping by containing all emanations

to the locality of the equipment generating them. It consists of a screened enclosure to contain the radiated RFI by reflection or absorption. Supplies and services both mechanical and electrical are treated to prevent the conduction passage of RFI through the screen. Many parts of the bunker are within a Tempest screen and are therefore protected from this electronic eavesdropping.

#### **Environmental Controls**

The environment within the Bunker is an electro-pneumatic system controlled by microprocessor.

#### **Mechanical Services**

Fresh, filtered air (98%) is introduced to the bunker via a fresh air intake air conditioning system where it is pre-conditioned. There is the ability if needed to supply the air via activated charcoal gas filters, which could remove gasses, biological agents or radioactive material if required.

The introduced fresh air goes into a plenum, which supplies each of the individual air conditioning units, serving all areas within the bunker. Each individual area can be adjusted to create any required environmental condition. However the general operating conditions are 19 degrees centigrade, plus or minus 3 degrees, with a relative humidity of between 43 - 63%.

#### **Chillers**

There are three refrigerated water chillers, each capable of producing 340kW of cooling, giving an installed cooling capacity of 1,020kW. Only two chillers can be run at any one time, resulting in an operating capacity of 680kW with 50% redundancy. Pipes distribute the chilled water throughout the bunker complex via pumps to the various air conditioning and fan coil units used for localised cooling. The chillers are themselves cooled by a condensed water system and open evaporative cooling towers.

#### **Fire Detection and Automatic Fire Suppression**

We are continually upgrading our fire system, as new server rooms are brought on line. Once occupied, each room is upgraded from basic detection to detect and suppress, which complies with BS 6266 and an FM200 fire suppression system. The whole bunker is fitted with a system, which complies with the EN 54 standard.

The fully addressable fire alarm system provides a comprehensive system of automatic and manually initiated detection equipment. Automatic detection, by means of heat and smoke detectors is provided in all areas including below raised floors and above false ceilings. A central control panel also has a repeater panel located remotely within the guardroom.

Upon detection of a fire in server room areas, there will be an automatic initiation of the FM200 gas suppression system to extinguish the fire, only within the area in which the fire was detected. FM200 is a chemical known as heptafluoropropane, which chemically interrupts the chain reaction of a fire. Discharge time is only 10 seconds and the extinction is rapid. At the concentration used in computer rooms, 7.5% volume, it is safe for humans to be present.

#### **PHYSICAL SECURITY**

A 3.5 metre high security fence surrounds the 18-acre site. Entry to the site is via the Guardroom (fitted with bullet-proof glass), which has a vehicular gate with control barrier and electrically operated pedestrian gate. A team of security staff maintains security at the site 365-days of the year. This includes a physical presence in the Guardroom/reception area; regular random patrols of the site together with M.O.D trained guard dogs. Patrols of secure areas take place on a regular basis, together with constant monitoring of the CCTV system. In addition a contract security company makes team, random out of hours mobile patrol visits to the site.

The site operates a security pass system for all visitors and staff. The bunker itself is only accessible to cleared personnel who have the appropriate security clearance and or pass..

#### **Electronic Security Systems**

Monitored infrared CCTV cameras, both above and below ground, cover the site. These are monitored 24 hrs a day by security staff from the guardroom and include a 'last motion picture captured' facility,

with thumbnail archives. Entry to the bunker is via a turnstile, operated by a security card system. All entry to The bunker is monitored and recorded by security staff, both physically and via the CCTV system. Other security mechanisms are in place both on and off site, to enhance the above systems

### PHYSICAL SECURITY

A 3.5 metre high security fence surrounds the 18-acre site. Entry to the site is via the Guardroom (fitted with bullet-proof glass), which has a vehicular gate with control barrier and electrically operated pedestrian gate. A team of security staff maintains security at the site 365-days of the year. This includes a physical presence in the Guardroom/reception area; regular random patrols of the site together with M.O.D trained guard dogs. Patrols of secure areas take place on a regular basis, together with constant monitoring of the CCTV system. In addition a contract security company makes team, random out of hours mobile patrol visits to the site.



The site operates a security pass system for all visitors and staff. The bunker itself is only accessible to cleared personnel who have the appropriate security clearance and or pass.

### Electronic Security Systems

Monitored infrared CCTV cameras, both above and below ground, cover the site. These are monitored 24 hrs a day by security staff from the guardroom and include a 'last motion picture captured' facility, with thumbnail archives. Entry to the bunker is via a turnstile, operated by a security card system. All entry to The bunker is monitored and recorded by security staff, both physically and via the CCTV system. Other security mechanisms are in place both on and off site, to enhance the above systems.