

Hosting Service – Security Summary

iplanit is generally offered on a hosted basis with Aspirico's preferred hosting partner, British Telecom. The services can also be set up within the provider/organisation on premise equipment as an alternative option. The following is a summary of the capabilities and services offered with the BT hosting option.

The hosting platform is a blue chip service used to support companies ranging from SME's to FTSE 100 , with data centres across the UK. Trusted by many Blue Chip Financial institutions to manage their internet presence and services, it provides a highly secure service with around the clock support.



The hosting service is a fully managed ISO 27001:2005 accredited hosting package .The service supports 99.95% service uptime, huge capacity and is agile enough to meet your ongoing business needs as the service platform evolves





Hosting Service Summary

- ✓ 100% UK based data centers
- ✓ 24x7x365 monitoring & management
- ✓ 24x7x365 manned operations desk and datacentres
 - ✓ 24x7x365 performance monitoring portal
 - ✓ 100% Internet Bandwidth Uptime
 - ✓ 100% Power availability
 - ✓ 100% Outage Detection
- ✓ 100% Intrusion Prevention Service signature update within 24 hours of release
 - ✓ 99.95% Service Uptime
 - ✓ Asset Management
 - ✓ Change Management
 - ✓ Incident Management
 - ✓ Automated Escalation Process
 - ✓ Gigabit internet connectivity
- ✓ Hosting 24/7 service desk & engineering staff
 - ✓ Hosting engineering staff HMG SC cleared
 - ✓ ISO27001:2000 & ISO9001 accredited
- ✓ PCI DSS compliant. CESG CHECK Infrastructure tested.
 - ✓ Service desk operates to ITIL v3 (ISO 20000).

Technology and Certification

The British Telecom hosting service blends technology, people and processes to provide a high security service.

- ✓ ISO 27001:2005 certified
- ✓ Cisco ASA High Availability Firewalls
- ✓ Intrusion Prevention Services
- ✓ Cisco MARS security reporting
- ✓ Payment Card Industry, Data Security Standard (PCI DSS) compliant.

Security is paramount so several security layers have been included to bolster the platform and minimise risk of compromise. Best of breed components have been included in the design, utilising enterprise class technology. The platform has secure connectivity to the Internet, consisting of a diversely routed internet connection, attached to resilient firewalls. Intrusion Prevention (IPS) modules actively screen all traffic entering the platform from the Internet. Inside the firewall/IPS layer are load balancers available to direct traffic to the appropriate server if load balancing is required.

Our gigabit switching infrastructure is secured by applying access lists so traffic is only allowed to communicate between specified devices on specified ports. Exclusively highly available components have been used and single points of failure have been eliminated. All network and security infrastructure reports into our Monitoring, Analysis and Response System (Cisco Mars), this information is then reviewed by our 24hour support team for appropriate action. Our infrastructure is regularly "penetration tested" by external partners.

Security Management In order to have a well understood and industry recognised approach all security processes are designed and operated according to the ISO 27001 framework – An Internationally recognized Requirement Document for information security management systems and the standard that promotes the adoption of a Scalable, Measurable and Repeatable information security management system.

Physical Environment, Tier 3 Data Centres

Processes and People

Security is enhanced through robust processes and procedures, and delivered by trusted personnel.

- ✓ Server hardened build.
- ✓ Change control – security is considered on all changes, and any risks/mitigation considered.

- ✓ Patch policy – to ensure any new vulnerabilities are countered in a timely fashion
- ✓ Firewall management and policy authorisation .
- ✓ Privileged User Access - access to privileged accounts is restricted and controlled).
- ✓ Backup and Recovery procedure
- ✓ Data centres are solely UK based
- ✓ Security Vetted Staff

Data center - Facilities

- Raised flooring
- Manned 24/7
- Appropriate Heating Ventilation and Cooling (HVAC) systems
- Redundant (N+1) power supplies delivered to rack
- Diverse power supply to separate sub-stations
- Diverse network feeds into the building
- "Onion Layer" security model using access request mechanism, proximity and/or biometric entry systems
- Generator Backup with fuel supply onsite
- Multi Uninterruptible Power Supplies
- Fire detect and suppression systems

Availability and Scalability

Internet Connectivity

The Aspirico hosting service uses burstable high bandwidth internet connectivity of up to a gigabit per second of data transfer capacity. The Internet connectivity can easily accommodate any increases of bandwidth in the future and is capable of dealing with the most demanding requirements, including streaming of media content.

Scalability

- ✓ Scalable high availability across multiple physical servers.
- ✓ VMotion keeps the environment up and running, giving unprecedented flexibility and availability to meet varying demands.
- ✓ Decrease planned and unplanned downtime for improved business continuity.
- ✓ VMware Distributed Resource Scheduler (DRS) continuously monitors utilization across resource pools and intelligently allocates available resources among virtual machines.

Resilience

- ✓ Automatic detection of server failures. Virtual machines with VMware HA provide an easy to use and cost-effective failover solution to protect against server failures.
- ✓ Smart failover of virtual machines (when used with VMware Distributed Resource Scheduler). Automate the optimal placement of virtual machines to servers with best available resources after server failure.
- ✓ Resource checks ensure that capacity is always available in order to restart all virtual machines if there is a node failure.

Monitoring and Management

Standard operating system management activities will be undertaken including system administrative services. The servers and services are proactively monitored to ensure and issues are detected and resolved before they affect service delivery. All levels of infrastructure are comprehensively managed from physical hardware through to operating and server application level.

As well as closely monitoring all components of its infrastructure in house, the Aspirico hosting services support :

- ✓ Web Accessible Portal System
- ✓ Application log monitoring Service
- ✓ Availability Monitoring

Monitoring and Management Managed Data Backup

The service supports a comprehensive data backup service to protect your data from corruption or accidental deletion. The backup services can be tailored to manage database and application backups if required, and backup cycles to be amended in line with your data management needs.

Security Devices

The Cisco ASA 5500 Series provides intelligent threat defense and secure communications services that stop attacks before they impact business continuity. Designed to protect networks of all sizes, the Cisco ASA 5500 Series enables organizations to lower their overall deployment and operations costs while delivering comprehensive multilayer security.

The BT/Aspirico hosting service also utilises a range of third party, industry leading products including enterprise level virus scanning software, event-monitoring

software, patching software, log management software as well as industry standard network level security hardware including firewalls, IDS and IPS. All products are covered by the ISO 27001 documentation for the hosting service.

The hosting service also incorporates:

- Intruder Prevention system built into the Cisco ASA platform
- Riory Anti-DDoS appliances in each of the data centres.