

## **ANCHOR SECURE SUPPORT PACK TECHNICAL SPECIFICATION**

This document defines exactly what is and is not included in this support pack. An overview of the areas of support provided and technique used is presented followed by a detailed schedule of scope and definitions.

### **THE GOAL OF ANCHOR SECURE SUPPORT**

The Anchor Secure support pack provides you with a server on which the security and reliability is maintained by technical staff with the required skills, without the expense of a fully managed server. It is aimed at individuals and organizations that do not have the ability or the inclination to perform these essential tasks but still require a dedicated hosting environment.

### **AVAILABILITY MONITORING**

A centralised monitoring system automatically checks to see if the nominated services are responding within a designated time. A failure to respond due to either the performance of the application or the availability will trigger an alert.

Alerts are delivered to technical staff both via audible and visual alarms in the NOC and SMS notification when they are offsite.

Any change of state of any service is logged. Historic reports can be generated to show exactly when the availability of a service or server has changed and the total amount of downtime that has occurred on any service.

Availability monitoring is performed at two levels: Network connection monitoring and application layer monitoring via network.

The information available at each level varies respectively. A breakdown of monitoring points is provided in the schedule.

### **PATCHING AND UPDATES**

Anchor monitors the patches and updates released by the operating system vendor for the installed applications.

The most recent vendor supplied security patches are applied as soon as practical.

Application of patches may be delayed where the application of the update has the capacity to interfere with business requirements.

### **FAULT RECTIFICATION**

If any of the monitored services fail, multiple Anchor staff are notified immediately by Email, Instant messaging, and SMS. Notifications continue and are escalated until the problem is acknowledged.

Basic diagnosis is then performed to allow the affected service to be restored.

### **MANAGED HARDWARE**

In the event that monitoring systems detect a disruption to a service which Anchor investigates and finds to be a hardware fault, Anchor will replace the failed components.

A full inventory of spare components is maintained onsite to permit rapid replacement of failed components.

### **SUPPORT SYSTEMS**

During business hours (8am to 6pm) support is provided via telephone and email. All email requests are tracked via an automated ticketing system to ensure appropriate escalation and response.

All requests and changes are documented internally by Anchor.

Anchor monitoring and response is provided on a 24 x 7 basis.

After hours emergency support is provided 24 x 7 via telephone only. Support after hours is provided for the purpose of resolving problems which cause outages, it is not provided for general configuration changes, provisioning or advice.

Support may be further limited in scope where client side activities result in recurring failure of supported services.

## SCHEDULE OF ANCHOR SECURE SUPPORT SCOPE AND DEFINITIONS

<b>Server hardware</b>	
Component testing	Memory is tested for 48 hours using Memtest before deployment. Motherboard, CPU and disc drives are tested for 5 days using the Cerberus Test Control System before deployment.
Spares inventory	An inventory of spare components of same or compatible specification is maintained onsite for all deployed servers.
<b>Operating Systems supported</b>	
Linux	Red Hat Enterprise Linux, Fedora, Debian
Windows	Windows Server 2003 Web edition, STD, Enterprise Edition
<b>Software installation</b>	
Operating system supplied packages	Installed by Anchor as requested by the client at the time of server deployment.
Third party packaged and non-packaged applications	Installation provided under Anchor Custom Support.
<b>Configuration management</b>	
Initial software configuration during the server build.	As part of the deployment of your server Anchor will configure a single virtual host on your server. Configuration is limited to a maximum of 3 hours duration using only the following supported applications: <ul style="list-style-type: none"> <li>• Web servers: Apache, IIS</li> <li>• Mail servers: Sendmail, Postfix, IIS</li> <li>• FTP: VsFTPd, ProFTP, IIS</li> <li>• SSH: OpenSSH</li> <li>• DNS: BIND, Microsoft DNS</li> <li>• Misc: SVN, CVS, Terminal Services</li> </ul> Anchor Custom Support is available for configuration of other applications and server builds that exceed 3 hours in duration.
Configuration management	After the initial server build all ongoing configuration is provided under Anchor Custom Support.
Security management	Anchor maintains a host based firewall and access control systems.
<b>Performance management</b>	
Application performance research and analysis, client requested application performance changes, diagnosis of hardware limitations.	Provided under Anchor Custom Support.
<b>Patching and updates</b>	
Software updates	Critical security updates to critical applications are applied outside of business hours. Target time for application is 24 hours from receipt.  Critical and non-critical security updates to non-critical applications are applied during business hours as soon as possible. Target time for application is 24 hours from receipt.  Critical applications are those deemed as having a high level of dependence on the end user application or where the risk of service instability resulting from the application of the update is high.
Kernel updates	Kernel updates are scheduled to occur with advance notification outside of business hours. Target time for

	application is 3-7 days from receipt.
<b>Monitoring</b>	
Service availability network checks	Ping, Terminal services
Service availability application layer network checks	Up to 5 services nominated from SSH, HTTP, DNS, POP3, IMAP, NTP, FTP, SMTP, Individual websites or other network facing applications as noted by the client.
	Note: Monitoring of some services are specific to the operating system. Actual services monitored vary accordingly.
<b>Fault rectification</b>	
Restarting failed services	If a monitored service fails, Anchor will perform basic diagnostics to allow the service to be restored.
<b>Migration tasks</b>	
Migration of services/data from/to external hosts, between different application, versions or formats.	Provided under Anchor Custom Support