

- SAMPLE ONLY -

12th September 2007

Mr A Johnson
Aircraft Plastics Limited
Airfield Way
Southend Airport
Essex SS8 9PQ

Our Ref: KH/dmh
Your Ref:

Dear Alan,

Re: Remote Working Project

First of all, thank you for inviting us in to meet the project team for the remote working initiative. Simon and I enjoyed the tour of the facility, and it certainly was interesting to see the aircraft in such a different light than one does as a passenger.

We have outlined our thoughts for moving the remote working project forward, and we have some general ideas and issues that we think your team will wish to consider.

Requirements

Our understanding is that you are looking for 22 senior managers to be able to access the AP network from their home location. There is also a further requirement for email access for the sales team and the board which comprises a total of nine email accounts. The remote workers all have broadband access at their homes and alternate work locations.

There is also a requirement that a suitable instant messaging solution be implemented for use by all staff and a block be placed upon unsanctioned IM use.

There is also a requirement for a key skills handover to the AP IT team and IT helpdesk support from the Contour support desk on a Monday to Friday 8am to 6pm basis.

Recommendations

VPN Hardware

We recommend that a Fortigate FG800 be installed at the IT centre, Southend with VPN connections to remote locations for effecting homeworkers' access to the network.

The FG800 will also be firewall configured to replace the outdated Neoteris firewall currently installed.

The firewall should be managed on a 24/7 365 basis and patched as required when software updates

- SAMPLE ONLY -

are issued. We recommend that FG60s be installed at each remote worker location for VPN access to the AP network via the FG800. Existing broadband connections at homeworker locations can be retained, or we can arrange for a provider recommendation if centralised control is required.

Email Access

We recommend the installation of Microsoft Outlook to replace the email package currently employed. Given the issues regarding downtime with the existing email server, we further recommend that the email solution be hosted at Contour's hosting centre located at Redbus Interlink, Docklands.

We recommend that the server be managed by Contour as we are able to guarantee email access and server uptime in excess of 99.9% (refer to attached SLA).

Instant Messaging

We recommend that Microsoft Live Communications Server be installed on a HP ProLiant server at the AP network location in Southend. This software will provide instant messaging capability to all staff with network access.

To block unauthorised use of Instant Messaging clients such as Yahoo! and AOL, and to block greynet applications such as Limewire and Kazaa, we recommend that a RealTime Guardian box be installed at the gateway at the AP network centre, Southend. We also recommend that this be remotely controlled by the Contour 24/7 security team at Chelmsford with permissions assigned by AP IT Director, Tony Grimm.

Project Implementation

Project Team resources

The project manager will be Simon Branson who will also oversee AP technical training and knowledge transfer during the project implementation.

Additional Contour staff will be used as required. However, one of the aims of the project implementation phase will be to transfer skills and knowledge to AP's IT team, and to this end, AP staff shall be used wherever possible.

John Lithgow, Senior Security Manager, will handle the firewall configuration and VPN implementation.

The following are approximate timescales for implementation of the project:

FG800 installation and configuration	4 days
FG60 configuration	4 days (note AP staff will handle remote location installation)
VPN Implementation	7 days
MS Outlook implementation	2 days
MS Live Communication server	3 days

- SAMPLE ONLY -

Fraser McDonald
Managing Director

cc: Tony Grimm – AP IT Director

Encs.