

Case Study

Mole Valley District Council meet Code of Connection directives with solutions from Becrypt

Based in Dorking, Surrey, Mole Valley District Council provides a full range of services to its citizens. As part of its commitment to provide good value services and flexible working conditions for its staff, Mole Valley has a long established home working policy. Any member of staff that is able to undertake their work from home and wants to, subject to complying with health and safety requirements, is permitted to. When the government announced Code of Connection requirements in order to join the Government Connect Secure Extranet (GCSx) the IT Team at Mole Valley had a challenge. How to comply and yet still provide Council staff with the same flexible working arrangements that they were used to and continue to provide a full range of services to citizens within a limited budget?

Head of IT at Mole Valley Bob Thomas explains, "It would be a huge task to change employment terms and conditions for staff, and we couldn't afford to buy new Council owned equipment for them to work with. So we had to find a way to make our existing system more secure to meet the Code of Connection requirements and allow staff to continue using their own equipment."

Data security requirements

Mole Valley already had a home working solution that enabled staff to connect to the network from their home PCs, but it lacked the level of security required for the new Code of Connection. Added to this was the need to encrypt sensitive data, if transporting it by media such as disks or USB stick to ensure it is protected. In addition, the Council has a fleet of over 60 laptops, and while it is policy never to hold personal data on laptops, all laptops are to be fully encrypted to provide assurance.

Bob Thomas commented, "We looked at a range of solutions, but we are a small

team and did not want to end up with a lots of products from different vendors, with overlaps and tensions between them. We were keen to source as much as possible from one vendor which would ensure that different aspects of the solution would work well together."

Encryption, end-point control and secure remote working

Mole Valley found that Becrypt were able to supply solutions to cover all the elements that they were looking for. The team have selected Becrypt Trusted Client, DISK Protect, Connect Protect and Media Client.

End-point control

As part of the Code of Connection compliance, "Green IT" initiative, to reduce costs and to make IT support arrangements easier, Mole Valley has implemented a policy of thin client desktops. Now most people do not have a PC but a thin client desktop device that provides them with access to all the software and information that they need to do their work. No data can be stored locally, and all USB ports are blocked to prevent data leakage. However as Bob Thomas explains, "While we have ensured that data can not be leaked during the day-to-day usage of the thin client devices, there are occasions when data does need to be sent to third parties or other locations, so we do provide a number of 'walk up' PCs for people to use as and when they need to."

The 'walk up' PCs are all controlled by Becrypt Connect Protect, which enables IT to keep track of exactly who saves what data, where and when. If someone takes a copy of a file and records it to a DVD, CD or USB stick, Connect Protect records this, and provides a prompt asking the user if the data needs to be encrypted. If it does, it uses Becrypt Media Client to encrypt the CD/USB stick.

Becrypt help Mole Valley District Council to:

- Secure data and prevent data loss
- Implement end-point control policy
- Enable staff to work securely from home PCs
- Comply with GCSx Code of Connection

Protecting data in transit

Media Client is a simple and easy way of protecting data whilst it is in transit. Sometimes data needs to be sent or shared with a 3rd party who are outside the physical boundary of the organisation. Media Client allows data to be quickly encrypted and shared therefore reducing the risks of data loss should a CD, DVD or USB storage device be lost or stolen whilst it is in transit. Designed to be easy to use, a file or folder can be quickly encrypted and stored onto a CD for example. A strong pass phrase is created, which is shared with the recipient. Media Client has a zero footprint, allowing the recipient to access the encrypted file or folder without the need to install software, as long as they have the correct passphrase.

Secure remote working

To continue to provide to same levels of remote working the IT Department needed a solution that would allow them to comply with the Code of Connection guidance for remote working and one that would be cost effective. Essentially staff needed to be able to continue to use home equipment to access the network and work effectively from home.

Trusted Client was an ideal solution. Trusted Client is a low cost secure remote access device, or 'bootable media', that solves the problem of secure remote working on unmanaged PCs.

From an Information Assurance perspective there are two key benefits, firstly any malware from the unmanaged host PC's operating system or hard drive can not infect the network, and secondly 'corporate' data can not leak onto the host PC.

Carried on a USB stick, Trusted Client uses ground breaking technology to create a secure environment on the host PC, only the PC memory and processor are used, the hard drive is bypassed.

Users simply boot their home PC from Trusted Client and after secure login are presented with their office desktop, just as if they were in the office. After their work is complete they switch off the PC in the

normal way and no trace of the work session is left on the host PC.

Cost savings

As all home and remote workers have remote access, and using Becrypt Trusted Client will have secure access to their office desktop, the need for Council laptops has reduced significantly. Bob Thomas says, "We still need some laptops for when people need to do external presentations and the like, but the majority we will be decommissioning and not replacing. This policy will reduce our laptop estate by at least 40 devices, which is a big saving, not only in costs, but also in support overheads." All Council laptops will be encrypted using Becrypt DISK Protect. This will ensure that if a laptop is lost, any data held on the device will be inaccessible and therefore safe.

Benefits and business continuity

The Council was already providing home working and remote access arrangements for staff however now, using Becrypt technology they have the means to provide these services securely whilst complying with GCSx Code of Connection. When the current pilot project is finished and the roll out of Trusted Client to all staff is complete there will be only one home/remote working set up for IT to support, where before everyone had something different. Another valuable benefit to the Council is that with secure remote access available to most people, if and when a flu pandemic hits or bad weather disrupts travel, staff will be able to work from home for extended periods without needing to come into the office, ensuring that essential services can still be provided.

When the current pilot projects are completed the Council intends to roll out Becrypt Trusted Client to all around 150 staff who make use of the opportunities to work from home. This will enable Mole Valley to comply with the GSI Code of Connection for GCSx, which details that any mobile, remote and or home working solution must meet the HMG IA policy and guidance. Trusted Client meets all of the criteria stipulated in the compliance guidelines to enable secure home working.

For more information please call 0845 838 2050 or +44 (0) 20 3145 1050, or visit www.becrypt.com

Becrypt Limited, 2nd Floor, North West, 90 Long Acre, London WC2E 9RA. www.becrypt.com info@becrypt.com

Becrypt is a leading supplier of innovative Information Assurance solutions and services with operations in the UK and US. Becrypt provides secure, feature rich, out of the box products suitable for all industry sectors, and is the largest supplier of encryption technology to the UK Government, Ministry of Defence and UK Police.

© Copyright 2009 by Becrypt Limited. All Rights Reserved. The Becrypt logo and trademarks are owned by Becrypt Limited. No material may be reproduced for any purpose, private or commercial, without prior written permission from Becrypt Limited.