



David Paine

David is Technical Services Manager for Castle Computer Services Ltd, a leading provider of financial and business systems and IT infrastructure design and support.

✉ david.paine@castle-cs.com

YOUR QUESTION

The nature of our business means we sometimes hire freelance or short-term contract workers. How can I make sure they have access to the data they need, but do not pose any threat to the business?

DAVID'S ANSWER

The security of data is all about reducing risk by applying multiple layers of protection. This is achieved through a combination of user authentication, access privileges, encryption and control over the movement of the data; while also ensuring strict adherence to policies on IT use.

Electronic data must be protected against loss, unwarranted disclosure or introduction of erroneous or harmful content. When granting user access privileges, they must be set at the minimum level necessary to satisfy the business requirement – access should be on a strict need-to-know basis.

The best practice approach for storing sensitive data is full disk encryption. This preserves confidentiality by rendering all files inaccessible to unauthorised users.

Consideration also needs to be given to the transfer of data from file servers to removable media such as memory sticks, MP3 players and DVDs. This can be controlled through port management.

Finally, to prevent the transmission of sensitive data through corporate e-mail systems or via the internet, you need to set up content analysis security at the perimeter of your network. This ensures the transfer of outgoing data meets with acceptable use policies and, therefore, unauthorised data transfer is prevented.