



Data Security Made Simple

courtesy of

The PCI guide lines

Every once in a while sanity shines through and a group of organizations with a mutual interest sit down and agree a simple and effective set of self imposed guide lines. The PCI Security Standards Council, founded by American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International, achieved one such success when they compiled the payment card information data security standard (PCI DSS).

So why is that of interest to those responsible for ICT within their own organization if they do not hold payment card information? The answer is simple. By substituting the word 'key' for 'cardholder' in the defined requirements, you gain of a set of effective guidelines for securing an organization's data and communications. Thus with judicious use of these guide lines, those responsible for ICT security can form a coherent security policy which can be implemented and demonstratively tested without out getting lost in a plethora of technical minutia.

That said, it should be noted that it is important to reflect the particular priorities, operation and scale of the organization concerned.

To help meet the financial and social imperatives of your organization's data and communication security requirements, please find below the PCI DSS requirements with the word 'key' added to provide a generic data security check list:

Build and Maintain a Secure Network:

Requirement 1: Install and maintain a firewall configuration to protect cardholder/key data.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

Protect Cardholder/Key Data:

Requirement 3: Protect stored cardholder/key data.

Requirement 4: Encrypt transmission of cardholder/key data across open, public networks.



www.keyfort.co.uk

Tel: 0870 727 3535

information@keyfort.co.uk

Keyfort Limited

21 Oxford road

Bournemouth. BH8 8ET

FOR MORE INFORMATION, CONTACT US NOW



Data Security Made Simple

courtesy of

The PCI guide lines

Maintain a Vulnerability Management Program:

Requirement 5: Use and regularly update anti-virus software.

Requirement 6: Develop and maintain secure systems and applications.

Implement Strong Access Control Measures:

Requirement 7: Restrict access to cardholder/key data by business need-to-know.

Requirement 8: Assign a unique ID to each person with computer access.

Requirement 9: Restrict physical access to cardholder/key data.

Regularly Monitor and Test Networks:

Requirement 10: Track and monitor all access to network resources and cardholder/key data.

Requirement 11: Regularly test security systems and processes.

Maintain an Information Security Policy:

Requirement 12: Maintain a policy that addresses information security.

If you would like to discuss how the above may be applied to your organization's particular security requirements, please do not hesitate to contact Keyfort, we would be happy to help.

FURTHER INFORMATION ON THE PCI DATA SECURITY STANDARDS CAN BE OBTAINED AT: [HTTPS://WWW.PCISECURITYSTANDARDS.ORG/INDEX.HTM](https://www.pcisecuritystandards.org/index.htm)

www.keyfort.co.uk

Tel: 0870 727 3535

information@keyfort.co.uk

Keyfort Limited

21 Oxford road

Bournemouth. BH8 8ET

FOR MORE INFORMATION, CONTACT US NOW