



Meeting Your Information Security Obligations

A plain English guide to FSA Compliance

Octree Computers, The Lloyds Building, Birds Hill, Letchworth, Herts. SG6 1JE

T: 08456 171819

W: <http://www.octree.co.uk>

e: security@octree.co.uk

Foreward

In April 2008 the FSA published a report titled *“Data Security in Financial Services - Firms’ controls to prevent data loss by their employees and third-party suppliers”*. This was in the form of a 104 page document describing how financial services firms in the UK are addressing the risk that their customer data may be lost or stolen and then used to commit fraud or other financial crime. It sets out the findings of their recent review of industry practice and standards in managing the risk of data loss or theft by employees and third-party suppliers. I have reviewed this report and drafted the following fourteen point “Best Practices” guide to help the principals of any firm conduct its business in accordance with the FSA’s Principles for Business – ‘to conduct its business with due skill, care and diligence’ and ‘to take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems’.

I hope it helps.

**Tony Richardson, Security Consultant
Octree Computers**

“I welcome this report on the protection of customer data within the financial services industry. It includes examples of good practice by some financial institutions which others could usefully learn from. However, I am disappointed – but not altogether surprised – that the FSA has found that financial services firms, in general, could significantly improve their controls to prevent data loss or theft.

The blunt truth is that all organisations need to take the protection of customer data with the utmost seriousness. I have made clear publicly on several occasions over the past year that organisations holding individuals’ data must in particular take steps to ensure that it is adequately protected from loss or theft. There have been several high-profile incidents of data loss in public and private sectors during that time which have highlighted that some organisations could do much better. The coverage of these incidents has also raised public awareness of how lost or stolen data can be used for crimes like identity fraud. Getting data protection wrong can bring commercial, reputational, regulatory and legal penalties. Getting it right brings rewards in terms of customer trust and confidence.

The financial services industry needs to pay close attention to what its regulator is saying here. But this report is also relevant to organisations outside the financial services industry which hold data about private individuals. All organisations handling individuals’ data, in both the public and private sectors, could benefit from the good practice advice it contains.”

Richard Thomas – Information Commissioner

Octree Computers, The Lloyds Building, Birds Hill, Letchworth, Herts. SG6 1JE

T: 08456 171819

W: <http://www.octree.co.uk>

e: security@octree.co.uk

A 14 point plan to achieving compliance

1 Governance

Develop a security policy document that everyone, from senior management to junior members of staff can “buy in to”. Everybody has to be aware of their responsibilities for protecting client information. Make it easy for all members of staff to report on data security concerns - suspicious activity or unusual behavior for example. Do not think that it is just an IT issue and therefore the IT department’s responsibility. It is also important to notify affected clients of any security breach resulting in exposure of their personal information.

2 Training and Awareness

Make everybody aware of the potential financial crime risks arising from poor data security through innovative training programmes, and the legal and regulatory requirements to protect client data. Why is it so important and what can be done to comply with relevant policies put in place. Keep it simple though – it has to be memorable and easily understood. Keep security in mind with posters, screensavers, or whatever is considered to be effective.

3 Servers, Desktops and laptops

If customer data is stored on a Laptop, Desktop, or a File Server you need to have the following security precautions in place to ensure compliance with FSA best practices and ICO (Information Commissioner’s Office) guidelines.

- a. Firewall - To protect your computer or network from external security threats
- b. Antivirus and Antispyware Software - Should be installed to protect your computer from malware such as Key Loggers and Trojans
- c. Full Disk Encryption – will encrypt your whole hard drive using a set of keys and passwords. If the device is lost or stolen it would be rendered useless to any third party as you would need a special code to access the data.

All computers that hold customer data must be encrypted.

Octree Computers, The Lloyds Building, Birds Hill, Letchworth, Herts. SG6 1JE

T: 08456 171819

W: <http://www.octree.co.uk>

e: security@octree.co.uk

- d. Removable Device Encryption - All Floppy Disks, CDs, DVDs and USB flash drives must be encrypted if they hold customer data. They must use a minimum of 128 Bit encryption.
- e. Encrypted Backups - When backing up data whether it is to Tape, Hard Disk or Online the backup media needs to be encrypted.

4 Password protection

Password protection of all computers is essential. You should be asked for a user name and password every time you switch on or logon to your PC. Follow the rules below to make sure you have the most secure password possible.

- a. Your password should be at least 8 characters long
- b. It should include letters, numbers, capitals and other symbols i.e. *P@nD4b34R!*
- c. It should be easy to remember but hard to guess
- d. Avoid any word in the dictionary, personal information such as a child or partner's name or a football team, common names and slang.
- e. Try playing on normal words such as England – 3nG1@Nd!
- f. Do not write passwords down
- g. Do not tell anyone else your passwords
- h. Change your password every 90 days at the very least!

5 Email security

All emails containing customer data must be secure. Encrypting email means that only the sender and intended recipient are able to read it. Some common and free email encryption types are easy to break and are therefore not secure.

Octree Computers, The Lloyds Building, Birds Hill, Letchworth, Herts. SG6 1JE

T: 08456 171819

W: <http://www.octree.co.uk>

e: security@octree.co.uk

6 Physical Security

Physical security is a key factor in securing your client data. Why encrypt and protect your data electronically when someone can break in and walk away with your file server.

- a. Your file, database and email servers should all be kept in a locked cabinet within a secure room to prevent casual access.
- b. External Hard Drives that contain customer data should be locked away when not in use.
- c. Ensure that only authorized personnel have access to your offices and buildings.

7 Backups

Full backups of all critical data should be a standard process within your business. The simple rules below should help you to keep your data secure.

- a. Backup media should be locked away securely while not in use.
- b. Only authorized personnel should have access to backup media.
- c. Backup media should be held off site for disaster recovery.
- d. If the media is held off site it should be transported and stored securely i.e. a lock box or safe.
- e. Back up media needs to be encrypted.

8 Access Control

Access control should be an ongoing process. Where users have access to confidential information they should only be given permissions to access the data they need to do their job.

- a. You should review access permissions for every user at regular intervals. Each employee should have their own logon account.
- b. Employee's access should be revoked as soon as they leave the company or are suspended.

Octree Computers, The Lloyds Building, Birds Hill, Letchworth, Herts. SG6 1JE

T: 08456 171819

W: <http://www.octree.co.uk>

e: security@octree.co.uk

- c. Locations where sensitive or confidential information is stored should be audited.

9 Data Transfer

If you need to move customer data outside of your secure environment for example; on CD or USB memory you need to make sure you do the following

- a. Encrypt all portable media using a suitable encryption technique.
- b. Use device control software to control and detect unauthorized access to external media such as CDs and USB devices.
- c. Keep a record of all of these devices and which personnel are allowed to use them and for which purpose.

10 Asset management

Asset management is also a must to stay compliant with current regulations. You need to keep a record of all computers, laptops, USB devices, external hard drives etc. that exist in your business.

If you are going to take customer data outside of the business you should have a record of that data that is copied and the business reason for doing so.

11 Data destruction

Data removal and destruction is an important part of keeping your clients' information secure. Simply deleting the data from a computer does not work as it can still be recovered. Companies that hold personal data should only keep it for a reasonable period of time. When you need to delete the data it should be securely shredded using special techniques to prevent recovery by unauthorized persons. This also applies when disposing of old equipment; hard drives should be disposed of securely ensuring all data is destroyed.

Octree Computers, The Lloyds Building, Birds Hill, Letchworth, Herts. SG6 1JE

T: 08456 171819

W: <http://www.octree.co.uk>

e: security@octree.co.uk

12 Remote access

Remote access to your network needs to be secure. Remote access and VPN software needs to be configured properly for the highest possible security level. If staff are allowed to work from home or remote locations they need to make sure that any wireless network that is used is encrypted to prevent eavesdropping.

13 Staff recruitment

Make sure all necessary and available vetting procedures are followed when recruiting staff, particularly those who may have access to sensitive information, including credit records, criminal records and the CIFAS staff fraud database. Follow up on references given. Assess regularly in staff in higher-risk positions may be susceptible to coercion.

14 Email and internet access

Implement monitoring controls for email and internet activity to identify potential data leakage, and remove inefficiencies through irresponsible browsing and non-work related messaging. Filter access to content that allows web based communication such as webmail (Hotmail, Gmail, Yahoo, MSN instant messaging), social networking sites like Facebook and Myspace, and file sharing sites.

About the Author

Tony Richardson has been involved in information technology for 21 years. Originally trained as a Management Accountant he has developed a broadline knowledge of technology within numerous industry sectors. He founded an IT solutions provider – Octree Computers - in 1990, and continues to provide expert technology solutions to the Small Medium Business community (organisations up to 500 employees who have little or no in-house expertise) with a specific focus on Information Assurance in the professional services sectors – financial, accounting, legal, and architectural.

Tony has achieved CISSP (Certified Information Systems Security Professional) certification, the first credential in the field of information security accredited by the ANSI (American National Standards Institute) to ISO (International Standards Organization) Standard 17024:2003. CISSP certification is not only an objective measure of excellence, but a globally recognised standard of achievement, and is presently held by less than 70,000 professionals worldwide.

Tony holds a Certificate in Microsoft Technologies gained at Lancaster University, and is a member of the Microsoft Partner Research Panel, a Microsoft Certified Professional, and a consultant for the Reuters Insight Community of Experts. He actively pursues a program of continuing professional development through vendor specific, and vendor neutral training and accreditation.

Tony can be contacted by email at tony.richardson@octree.co.uk

For more advice or to arrange a consultation email security@octree.co.uk

Octree Computers, The Lloyds Building, Birds Hill, Letchworth, Herts. SG6 1JE

T: 08456 171819

W: <http://www.octree.co.uk>

e: security@octree.co.uk

Appendix

Principles of the Data Protection Act 1998

The eight principles require that personal information:

- Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met;
- Shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes;
- Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
- Shall be accurate and, where necessary, kept up to date;
- Shall not be kept for longer than is necessary for the specified purpose(s);
- Shall be processed in accordance with the rights of data subjects under the Act;
- Should be subject to appropriate technical and organisational measures to prevent the unauthorised or unlawful processing of personal data, or the accidental loss, destruction, or damage to personal data;
- Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Octree Computers, The Lloyds Building, Birds Hill, Letchworth, Herts. SG6 1JE

T: 08456 171819

W: <http://www.octree.co.uk>

e: security@octree.co.uk