FCS for Legal Services

FCS For Legal Services

POWERED BY Asigra.

FCS For Legal Services

IT in the modern legal practice is very different from even a few years ago. Staff mobility, access to large amounts of low cost storage, requirements for data retention, data processing laws and other challenges have all combined to make the management of information difficult and time consuming. There are new, much more complex IT structures in place and more regulation and compliance to adhere to in protecting the data needed to provide the quality service customers demand.

Virtualisation and Cloud computing has brought a great benefits in allowing access to data from anywhere and hybrid solutions have mixed private and public facing solutions to give the right levels of access and control, though there are now further complexities to face.

The old ways of doing things don't provide the flexibility demanded by a modern environment, for example the use of tape backup is now almost exclusively retained for long term archive storage. Recognising the difference between 'storage' and a true restore focussed business continuity and disaster recovery solution is important.

One issue with this environment is that making a workable and restorable backup of the data, wherever it resides, is a difficult one. Additionally, to comply with Principle 7 of the SRA a practice must prove it is 'identifying and monitoring financial, operational and business continuity risks including complaints, credit risks and exposure, claims under legislation relating to matters such as data protection, IT failures and abuses, and damage to offices' – or as the IT world calls it, having 'a Disaster Recovery plan in place that is proven to work and evidence to support this'.

SRA Principle 5 also requires a practice to provide services to clients in a manner which protects their interests in their matter. Not only do we help you keep your systems and data working and available, but, we run dual UK based data centres to ensure your data is also safe in our environment should yours fail. It's important to note the eighth principle of the DPA states that personal data may not be transferred outside the EEA (European Economic Area) unless the provider maintains a 'Safe Harbour' agreement. Though the risk of downtime may be minimal, it is still a risk and as such needs to be mitigated.

One of the main reasons to ensure you have a service behind your data protection is to ensure you can go back in time to a point before an incident occurred. For instance, a malware infection may occur, but, not activate for several weeks. Once activated the data is lost and traditional backup has only retained a copy of the infected file. We can go back several years if needs be.

Being able to quickly and easily access a file, or files, that is deleted (accidentally or maliciously), overwritten with another, malware infected or simply lost due to hardware failure is essential. Principle 7 is not unique to the legal industry, most governance systems have a very similar clause and this means an IT provider can identify, understand and solve most of the issues that you are likely to face while making sure you are covered.

'Most' because not all systems are created equal and 'likely' because you might not face all of them but might present a few unique ones of your own.

FCS operate a service that makes sure whatever you have it is covered. Where ever your data is we can access it and store it. We don't have a single solution to deploy like most providers, we have all of them but the main thing we have is expertise. We have over 25 years of experience in the industry developing and operating such solutions and we are very good at it. In fact we've never lost a single byte of customer data.

In addition to encryption and compression, we take incremental views of the data set. So we only transmit the changes made to a document, rather than the whole thing adding to the security of using public internet as a low cost delivery mechanism.

There are many reasons to consider FCS. Not least that we are here to help you restore the data when you need it and can cover a very wide range of source data, probably in a better way than your existing backup software can. But most of all we provide a daily report that lets you know your 'restore readiness' state and we're available to help you correct any issues that have prevented a recent backup operation completing, these are normally because the target device powered off, had a hardware issue etc.

- By maintaining a restorable copy of data offsite we effectively mitigate issues of Ransomware, building loss, theft, fire etc. (SRA 7.3)
- Client confidentiality (SRA 4.1) is not an issue with FCS, we encrypt and compress all data on your premises before we transmit it to our data centre and you keep the keys, as the data is encrypted at source and incrementally uploaded to our solution – not even we can see it.
- Our system will check the integrity of the data and deliver a daily report outlining the state of the restorable data and we are on hand to assist with remediation if an issue has been highlighted, commonly backup failure due to device being powered off, local data loss etc.
- Flexible and scalable solutions rather than point products allow a unique to you proposition to be built and operated under our standard SLA.
- Agentless – nothing to interfere with the normal operation of your servers, storage etc
- 24x7x365 support as standard with all our solutions connects you with a service representative when you most need it.
- You retain full data control and have the right to get your data back in a usable format and retain full ownership of your data (SRA 4 and 5) .
- Capacity to store virtual machines and invoke a full replica of your DR suite on demand, with your data ready to go.
- FCS are an ISO27001:2005 certified company so we already have standards in place to protect your data, every minute of every day.
- Data Centres are mirrored for additional protection, all data held in the UK only.
- Data Centres are fully secured Tier 3 units so data protection is physical as well as electronic. BS5979 and BS8418 T3 Design and ISO9001.
- Encryption is FIPS-140/2 – almost the defacto standard for NHS, Government and other organisations requiring high confidence in data encryption.
- Data loss hasn't occurred. Ever. We have never lost a single byte of customer data and we intend to keep it that way.
- We can't see your data so we can't leak it and there can be no issues around anyone outside your organisation leaking data to a 3rd party.
- Fully scoped solution that isn't over capacity.

The main focus, and advantage of choosing FCS however is in the event you need to restore the data. Not only are we on hand to help you recover anything you may have lost but we are expert at advising and keeping a cool head when you need it.

Costs are controlled because we understand once size doesn't fit all. Some data you need back in 15 minutes, with some other data it can be a matter of days before you are even ready. We understand this and price our solutions accordingly. You only pay for what you store...

It is, therefore, a safe option to choose FCS for your Disaster Recovery and Backup solution as we help you meet your compliance requirements and actually increase your ability to quickly and cost effectively recover from any disaster, fire, theft, lost file or whatever happens.

We firmly believe we add value to your IT security through enhanced encryption and security and our bespoke service that delivers what you need as you need it keeps costs to a minimum, whatever the scenario.

FCS

Can you afford not to talk to **FCS?**

T: 0333 666 999 1

E: info@fcs-protect.co.uk

To find out how **FCS** can help you get in touch by email
info@fcs-protect.co.uk or call us on **0333 666 9991**