SRA Code of Conduct FAQs.

Choosing a CoC-compliant cloud provider can be a daunting task. Nimbox is fully compliant with the SRA's Code of Conduct, and its guidance on cloud services.

Q: I need to ensure that you are a reputable company. What makes you reputable, and can you supply a reference from a client in the legal sector?

A: Your account manager is able to supply references specific to your profession. We were also featured in a major legal publication recently: http://www.legaltechnology.com/latest-news/comment-safeguarding-data-secure-private-and-accessible/.

Q: Where is my data stored, and are you Safe Harbour compliant?

A: All user data will remain in Sovereign UK territory, and will never be transferred outside of her borders. As a company that is registered, and operates in the UK, we have no need to be registered with the American Safe Harbour scheme.

Q: Will you have access to my data? The SRA says that I must use software to automatically encrypt documents at the law firm's end, using security keys that are not known to the provider.

A: Nimbox cannot access data that is stored in Vault because it is instantly encrypted and decrypted on-the-fly, on the device that is being used at the time. Nimbox uses a widely trusted encryption algorithm called Advanced Encryption Standard (AES) with a 256-bit key. In its CNSSP-15 publication, the Committee on National Security Systems mandates that AES with a 256-bit key is secure enough to encrypt classified data marked up to TOP SECRET.

Q: Can you provide details of any security breaches over the last few years?

A: We have never been the subject of a breach, but in the incredibly unlikely event that user data is disclosed, you would be informed immediately.

Q: What backup arrangements do you have in place if your storage facility suffers from data loss or corruption?

A: Our entire platform is replicated across 3 data centres, in real time. This means that if one location 'goes dark,' our users can rely on the other two. We also employ unlimited file versioning, meaning that files can be 'rolled back' to a previous state.

Q: What security arrangements of you have at your data storage facilities (i.e. monitoring premises and vetting staff). Do you have back-up generators in case of power failures?

A: Our data centres are in geographically-different locations, and are rated as Tier 3+ (the highest rating for DCs in the UK). They all use advanced FM200 Fire Suppression systems, have N+1 power failover, N+1 UPS, and Tier 3+ security such as double-skinned walls, air-gapped racks, man-traps, and perimeter fencing. Each DC also has an onsite, 24x7 Network Operations Centre. They are also ISO27001:2013 accredited.

Q: Do you offer a private cloud, or private area of a hybrid cloud, for client confidential material?

A: Your Vault account is sandboxed from all other accounts on our system, effectively making it a stand-alone 'cloud.' Nobody has access to your data, not even us.

Q: What is your policy on law enforcement requests for user data?

A: We are a law-abiding company, and as such we comply with legal requests that are in the letter and spirit of the law, in the jurisdictions where we must. Presently, this would be those authorised by the Courts of England and Wales. We aim to be fully transparent about those responsibilities.

We have designed our services to hold a minimal amount of information, such that any legal disclosure we must make reveals only a small amount of personal information, as set out in our Privacy Statement. We do not hold the encryption keys to your data, and are unable to decrypt your files under any circumstances. Against this backdrop, we must and will comply with binding legal requests for data.

Q: Can you send me a model agreement that would form the terms and conditions of service? The SRA may request access to our data, so this needs to be part of the agreement.

A: Our Subscriber Agreement is located at https://www.nimbox.co.uk/subscriber-agreement/. As per the requirements of Outcome 7.10 of the Code of Conduct, the SRA will usually request access via the registered practitioner, who must provide access—we have no ability to decrypt user passwords or data, so cannot grant access to anybody (including us). When the practitioner has granted access, the SRA has the ability to view all files and folders held by the practitioner on Vault. A full audit trail will be maintained for both you, and the Authority.