DekkoSecure

Is the way your agency stores and shares sensitive data 100% secure and compliant?

Use Cases

Government agencies handle a wide range of highly confidential and PROTECTED-level information that must be shared securely and efficiently between teams, departments, and external stakeholders. These include:

- Operational briefs
- Digital evidence
- Highly sensitive MOUs
- Briefs of evidence
- eDiscovery/disclosure information
- Affidavits
- Subpoenas
- Operational reporting
- Sensitive supply chain documentation
- Vendor agreements
- Technology contracts

8 vital data security questions to ask your team

1. How comfortable are you with the total security of our data sharing practices (e.g., email, messaging, USBs, hard drives and video conferencing)?
2. Who (which team member agency) is hosting the data on their server(s)?
3. Who controls access to the hosting server(s)?
4. Are there adequate internal and external controls (e.g., physical security) in place for the hosting servers?
5. Does the server or database administrator have access to sensitive and confidential data?
6. Are there controls in place to limit unauthorised disclosure of certain data to cross-functional team members due to privacy regulations?
7. Do we have the ability to view a comprehensive audit trail on every piece of data uploaded and shared by the team?
8. Do our current information sharing practices satisfy Data Sovereignty?

If you are concerned about any of the answers to the above questions, your data may not be as safe as you need it to be.

DekkoSecure's end-to-end encrypted solution addresses all eight of the above security concerns with no hardware or software to purchase or download and minimal IT administration required.

Contact us to learn more:

help@dekkosecure.com

DekkoSecure