CommandHub
securing sensitive information

CommandHub Use Case

Justice

How to Secure Collaboration on Sensitive Documents

Use Case: Justice

How to Secure Collaboration on Sensitive Documents

Your Situation

You are the Security Officer or Administration Manager for a State or Federal Justice Department or similar entity.

Your organisation handles highly sensitive information such as offender records, current sentencing and historical data, witness and Subject Matter Expert statements.

Your organisation also works with external professionals, such as police officers, parole officers, medical and mental health specialists, subject matter experts, government representatives and employees.
They need to collaborate closely on issues from sentencing and parole conditions to judges' sentencing comments and medical or mental health assessments.

Your Challenge

Collaboration in this environment involves diverse parties, a large volume of sensitive records and a complex process. The sharing of records occurs primarily via hard copy and courier or via email and attachments, which is cumbersome, risky or both.

An extra challenge is to share information on a 'need-to-know' basis, so that collaborators only see the information they need for their roles. Considering the diversity of parties involved and the environment, this is almost impossible.

Should any of these documents be leaked, the public's confidence in the justice system would be shaken, encouraged by media entities and opposition parties keen to fuel embarrassment.

Your Vulnerability

By its nature, data relating to offenders is extremely sensitive. Maintaining the public's faith in the justice system while safeguarding offenders' civil rights is a delicate balancing act. The data has to be protected from other criminals too, as they could use it to their advantage or to do harm.

The increasing use of mobile devices by professionals adds another layer of risk. Securing information on tablets and smartphones is more difficult and these devices are more easily mislaid or stolen. To fully secure sensitive offender data, you need to extend protection to mobile devices, without placing barriers to collaboration that encourage risky work-arounds.

Your Options

If securing collaboration on sensitive data is critical for your organisation, there are 5 main options:

1. **Do Nothing.** This may be defensible if you've experienced no breaches to date, if you're confident that your rules and processes offer adequate protection and that your user education ensures adherence to them. This would be your choice if the perceived risk of breach is low, and the consequences not serious.

2. **Choose an Enterprise File Sharing System.** These systems are designed for easy file-sharing and provide some basic security functions but aren't designed for secure collaboration. You'll need to add third party tools which might add costs and complexity. This would be an option if your objective is to lower rather than eliminate risk.

3. **Choose Enterprise Collaboration Tools.** These tools were designed for collaboration, and security features were added later. The stated security levels tend to apply to the environment not the tools, and user configurations need IT support. This might be a choice if your

content is not critical, use of mobile devices is not widespread and you have ample IT resources.

3. **Choose Secure Collaboration Tools.** These recent developments, designed for closed networks, promise to secure sensitive content by checking the alignment between user, content and context. They may restrict users' access but won't control how they use content, especially on mobile devices. This would be your choice if restricting access is enough, you have a controlled network and mobile device use is limited.

4. **Choose an End-to-End Secure Collaboration Platform.** In use for over 10 years, this approach creates ultra-secure content compartments to which access is restricted on a 'need to know' basis. It protects your content and controls how it is used and where it is stored, especially on mobile devices. This would be your choice if you need complete end-to-end protection of your sensitive content, and you want a proven solution.

How CommandHub secures your sensitive collaborations

Ultra-secure Military Grade Architecture
CommandHub was designed from the ground up for secure collaboration, based on the Military Principle of multiple layered servers. The CommandHub solution is IRAP certified to the Australian Signals Directorate (February 2020) ISM PROTECTED standard. All data is wholly hosted and managed in Australia under the Sovereign Cloud Principles for Critical Infrastructure.

Patented End-to-End Protection
Protecting information at the server level is just the start. CommandHub also protects your sensitive information in transit and in use, including on mobile devices. HubVault technology features a multi-encrypted file transfer tunnel that replaces the need to browse. In addition, HubVault secures that data stored on mobile devices, using further encryption and a non-recoverable key, rendering the devices 'uncrackable' if mislaid.

Need-To-Know' Compartmentation
CommandHub applies the Intelligence Community principle of compartmentation, restricting user access on a 'need to know' basis. This means that even personnel with seniority or high security clearance will only be granted access to specific compartments if they 'need to know' the contents to fulfil their roles. This negates the risk of a 'Chelsea Manning' type breach.

Logical Business Controls
CommandHub lets you set controls for how internal and external parties can use sensitive content – such as who can see, edit or save a file, who may move it to where, how approvals and rejections apply, the exact sequence of these steps as well as version control, watermarking, file-locking and more.

Ease of Setup, Use & Control
CommandHub was designed to be used by business users without special IT skills. After little training, your administrators will be comfortable setting up file structures and applying controls to them. When trials, parameters or legislation change, they can adapt the settings themselves.

Tailored to Your Organisation's Needs
CommandHub is easily tailored to individual needs, with over 500 configuration settings. Your administrators can simply turn rules on or off for files, access, use, formats at any level.

Proven In Situations Like Yours
CommandHub has been protecting sensitive content for over ten years – in Justice, Government, Defence Contracting, Finance and Telecommunications, and by Executive Committees. Ask us about our case studies.

Contact us about how CommandHub can secure your sensitive collaborations.