CommandHub
securing sensitive information

CommandHub Use Case

Government

How To Secure Collaboration on Sensitive Plans, Policies and Technology

USE CASE: Government

How To Secure Collaboration on Sensitive Plans, Policies and Technology

Your Situation

You are the Secretary, Assistant Secretary, Operations Manager or IT Executive of a federal or state government department or entity. Many projects in your area involve advanced technologies, unique policy developments and specific deployment plans. If this sensitive content fell into the wrong hands, it would be embarrassing, costly or even a threat to national security.

For your projects to succeed, collaboration is essential, and your sensitive content must be shared with diverse parties including:

- Ministers, senior public servants and colleagues in other agencies
- External Subject Matter Experts and advisors under contract
- Specific groups and individuals in your department
- Other departments such as regulatory, standards, procurement & supply.

Your Challenge

The sensitive content needs to be shared, discussed, commented on, edited and re-issued, involving multiple steps and users. Therefore, both your content and collaboration process, and opportunities for leakage or theft, must be protected by the highest security.

Your safeguards must be stringent and effective yet not become barriers to collaboration. So, they must be easy to set up and to work with or you'll risk work-arounds and greater exposure. Due to wide use of mobile devices across government, your safeguards must also extend to these devices.

Your Vulnerability

Many of your collaborators don't work in your department and are not accountable to you or your minister. Therefore, you must rely on them following data security rules. You know that up to 50 percent of security breaches result from carelessness, so enforcing the rules could dramatically reduce your department's exposure. The reverse applies too.

Yet, making sure that rules are followed by everyone isn't assured. It's not just system ease of use at play; it's habit too. To get the job done on time, staff can fall back on old habits, like sharing documents as email attachments, using insecure file sharing platforms or media like USB drives. For collaborators outside your department, ensuring that data security rules are followed may be tough.

Your Options

If securing collaboration on sensitive content is critical for your department, there are five main options:

1. **Do Nothing.** This may be tempting if you've had no breaches to date or none reported. You may feel that your rules and processes are adequate and your user education will ensure adherence to them.

   This would be your choice if the data your collaborators share is not highly sensitive and the perceived risk of breach is low.

2. **Choose an Enterprise File Sharing System.** These systems make file-sharing easy and provide some file security but are not designed for collaboration. You'll need to add third party tools which could add cost and complexity and open security gaps.

   This would be your choice if lowering rather than eliminating risk is enough.

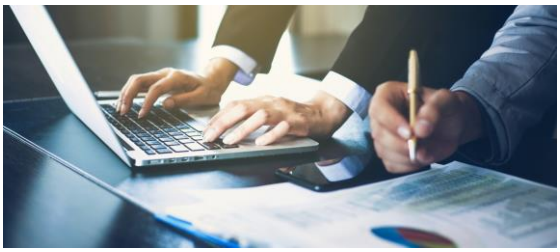
3. **Choose Enterprise Collaboration Tools.** These widely-used tools were designed to facilitate collaboration with security added later. You may find that specified security levels apply to the environment not the tools, and that user configurations require a great deal of IT help. This would be your choice if your content is not critical, mobile device use is not widespread in your department and your IT resources are not stretched.

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.

5. **Choose an End-to-End Secure Collaboration Platform.** This approach, in use for over a decade, creates ultra-secure content compartments to which access is restricted on a 'need to know' basis. It extends protection beyond who accesses your content to how it is used and where it is stored, including on mobile devices.

   This would be your choice if you need complete end-to-end protection of sensitive content, and your risk profile demands a proven solution.



How CommandHub secures your sensitive collaborations

Military Grade Architecture
CommandHub was designed from the ground up for secure collaboration, based on the Military Principle of multiple layered servers. This provides multiple levels of document encryption and infrastructure protection. As well, the hosting environment has been certified to PROTECTED status by the ASD (Australian Signals Directorate).

Patented End-to-End Protection
Providing the highest level of server security is the minimum; CommandHub also provides protection of sensitive content in transit and in use.

With patented HubVault technology, your collaborators can securely access and use your content on mobile devices, via a multi-encrypted tunnel that replaces vulnerable browsing. HubVault also secures content stored on mobile devices, using further encryption and a non-recoverable key, rendering them 'uncrackable' if they're mislaid.

'Need-To-Know' Compartmentation
CommandHub applies the Intelligence Community principle of compartmentation, restricting user access to 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 makes collaboration easy for users while ensuring that your department's business processes are followed. You can set controls for 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 for setup and use without IT skills. After little training, administrators will be able to arrange content logically for the various parties and apply controls to protect it. When projects and or policies vary, administrators can make the changes themselves. For users, the intuitive interface makes collaboration easy without IT support.

Tailored to Your Exact Needs
With over 500 configuration settings, CommandHub can be fully tailored to how your department and collaborators operate. By the simple turning on or off of rules for files, access, use, formats and settings at any level, CommandHub ensures that your sensitive information is fully protected, without impeding how your users work.

Proven In Situations Like Yours
CommandHub has been protecting sensitive content in the most demanding situations for over ten years in Government, Justice, Defence Contracting, Banking, Insurance and Telecommunications, and for Executive Committees elsewhere. Ask us about our case studies.

Contact us about how CommandHub can secure your sensitive collaborations.