CommandHub
securing sensitive information

CommandHub Use Case

Executive Committees

How to Secure Collaboration on Sensitive Strategy and Projects

USE CASE: Executive Committees

How to Secure Collaboration on Sensitive Strategy & Projects

Your Situation

You're a Senior Manager or Security Consultant with special responsibility for administrative systems. Your enterprise has many committees who collaborate on sensitive projects, from strategy development and business reviews to resourcing priorities.

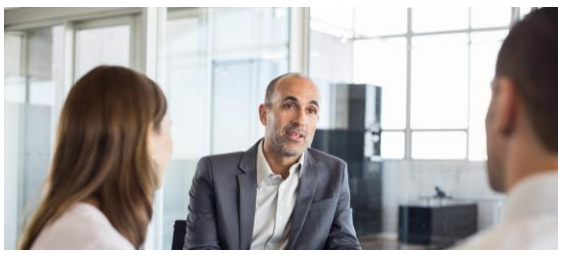
Committee members work from varied locations which makes electronic file sharing and collaboration essential. There are multiple individuals and steps involved in each project, which heightens the risk of accidental or deliberate data leakage. Any breach could damage your organisation's reputation and impact share value and customer confidence.

Your Challenge

Your IT infrastructure provides central facilities for staff to store and access files, but you need greater security for the sensitive data these committees handle. You also want to restrict individual access on a 'need-to-know' basis without raising barriers to collaboration; you don't want to give members reason to look for simpler but riskier workarounds.

IT resources are adequate but not always available; you'd prefer a collaboration platform that could be deployed and maintained by your business units.

Your committee members use mobile devices widely; you're concerned about exposing sensitive content if any devices are mislaid or stolen.



Your Vulnerability

Protecting sensitive data on different devices is one challenge; safeguarding it in transit and final destination is quite another, especially if the end point is a mobile device. The cache will retain data and remote wiping won't work once the device is turned off.

Committee members are not under your control, yet you're responsible for securing the sensitive data. You'd like to control the collaboration process, so you know that committee members are following corporate procedures when working on sensitive documents. You'd also like to restrict senior IT access to executive committee material.

Your Options

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

1. **Do Nothing.** This may appeal 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 only be your choice if the content involved is not highly sensitive and your perceived risk of breach is low.

1. **Strengthen Your Enterprise File Sharing System**. It was probably not designed to provide the type of collaboration and security you need for executive committees. To raise both, 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 to sensitive content is enough.

3. **Choose Enterprise Collaboration Tools.** These widely-used tools were designed to facilitate collaboration and security was 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 the sensitive content is not critical, mobile device use is not widespread and your IT resources are readily available.

4. **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 content protection in transit and in use. With patented HubVault technology, your committee members can securely access and use sensitive 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 virtually '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 for their roles.

Logical Business Controls
CommandHub makes collaboration easy for committee members while ensuring that your business processes are followed. You can set controls for who can see, edit or save a file, who may move it and 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, your administrators will be able to arrange sensitive content logically for committee members and apply controls to protect it.

When projects end or alter, your administrators can make the changes themselves. For committee members, 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 enterprise operates. By simply turning on or off rules for files, access, use, formats and settings at any level, CommandHub ensures that your sensitive data is fully protected, without impeding how your committees work.

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

Contact us about how CommandHub can secure your sensitive collaborations.