CommandHub
securing sensitive information

CommandHub Use Case

Defence Contractors

How to Secure Collaboration on Sensitive Commercial and Classified Content

USE CASE: Defence Contractors

How to Secure Collaboration on Sensitive Commercial and Classified Content

Your Situation

You are the Bid Manager, Project Manager or Security Manager for a leading Defence Contractor. The complex demands of major defence contracts makes it difficult for one contractor to supply the whole solution, so you often team up with other contractors.

This kind of collaboration raises unique challenges as it usually involves highly sensitive commercial information, and references classified information with national security implications. Managing these bids means working with teams of people through a lengthy, painstaking process of gathering and submitting material from each supplier.

Your Challenge

Managing these bids is a balancing act on several levels. You're working:

- With organisations who are competitors at other times
- With teams who won't or can't share confidential information
- With other contractors' bid teams, subject matter experts, defence advisers and others
- With executives and experts from your head office
- On various levels from technical to political and cultural.

In this environment, close collaboration on highly sensitive information is critical. These bids include vast amounts of highly technical information, that has to be checked and double-checked by specialists on the participating bid teams.

Your Vulnerability

In the process of putting a winning bid together, you must share a lot of sensitive content with many people. Any leakage of content could have dramatic consequences, such as losing the bid and being crossed off the list of preferred government suppliers.

Your fellow contractors must have full confidence in the integrity of your systems and processes, too. They need to know their sensitive information is protected by military-grade security. This is a challenge, since every contractor's material must be tightly compartmented with no blurring of boundaries between compartments.

Your Options

If securing collaboration on sensitive content is critical for your organisation, there are four main options. You could choose:

1. **An Enterprise File Sharing System**. Such systems make file-sharing easy and provide some file security but are not designed for collaboration. They lack the functionality you need for complex, multi-billion dollar, multi-contractor bids. As a minimum, you'll need to add third party collaboration tools which could open security gaps. This would be your choice if you're confident you can secure these gaps.

2. **Enterprise Collaboration Tools.** These tools were designed to enable collaboration in commercial organisations, with security added later. You may find that they offer neither the compartmentation nor the robust security you and your fellow contractors need. This would be your choice where collaboration is the main priority and absolute security is less so.

3. **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. **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. The CommandHub solution is IRAP certified to the Australian Signals Directorate ISM 2020 PROTECTED standard. All data is wholly hosted and managed in Australia under the Sovereign Cloud Principles for Critical Infrastructure.

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, all contractors can securely access and use sensitive content even 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 on a 'need to know' basis. So, 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 fellow contractors while ensuring 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 to be set up and used without IT skills. With little training, your administrators will be able to arrange content logically for your fellow contractors and apply controls to protect it. When bids end or alter, your administrators can make the changes themselves. For contractors, the intuitive interface makes collaboration easy, removing the risk of workarounds.

Tailored to Your Exact Needs
With over 500 configuration settings, CommandHub can be fully tailored to how you and fellow contractors operate. By simply turning on or off rules for files, access, use, formats and business process settings at any level, CommandHub ensures that your sensitive content is fully protected, without impeding how your contractors need to work.

Proven In Situations Like Yours
CommandHub has been protecting sensitive content in the most demanding situations for over 10 years - in Defence Contracting, Government, Justice, Finance and Telecommunications, and for Executive Committees elsewhere.

Contact us about how CommandHub can secure your sensitive collaborations.