CommandHub
securing sensitive information

CommandHub Use Case

Supply Chain Protection

How to Secure Collaboration on Classified Content

USE CASE: Supply Chain Protection

How to Secure Collaboration on Classified Content

Your Situation

You are the Project Manager or Security Manager for a leading defence supplier. The complex demands of major defence contracts mean you have hundreds or even thousands of sub-contractors.

This kind of environment raises unique challenges as it usually involves classified information with national security implications as well as sensitive commercial information.

It means working with teams of people through a lengthy, painstaking process of interacting with each supplier, many of whom are quite small and have little appreciation of the security challenges involved.

Your Challenge

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

- With organisations who are competitors at other times
- With teams who are not used to securing their business processes
- With diverse supply officers, subject matter experts, defence advisers and others
- At various levels from technical to political and cultural.

In this environment, close collaboration on the supply chain process is critical. These projects include vast amounts of highly technical information, that has to be checked and double-checked by specialists and with other contractors.

Your Vulnerability

In the process of managing the supply chain, you must share a lot of sensitive content with many people. Any leakage of content could have dramatic consequences, both immediate and reputational.

Your customer and your suppliers must have full confidence in the integrity of your systems and processes. They need to know their classified information is protected by military-grade security. This is a challenge, since every sub-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 projects. 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 they offer neither the compartmentation nor the robust security you and your customer demand. This would be your choice where collaboration is the main priority and process 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, sub-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 are mislaid.

'Need-To-Know' Compartmentation
CommandHub applies the Intelligence Community principle of compartmentation, restricting user access on a 'need to know' basis. So, sub-contractors and 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 suppliers 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 onboard suppliers and arrange content logically and apply controls to protect it. When the supply chain needs to be altered, your administrators can make the changes themselves. For sub-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 your suppliers 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 suppliers need to work.

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

Contact us about how CommandHub can secure your sensitive collaborations.