Executive Summary

If you are working with Defence you may need to be Defence Industry Security Program (DISP) accredited. If the project deals with any of the elements below then it is compulsory to be enrolled in the DISP program and meet accreditation requirements:

- Work on classified information or assets.

- Store or transport weapons or explosive ordinance.

- Provide security services for Defence bases and facilities; and/or

- If there is a Defence business requirement for DISP membership in the contract.

One of the key considerations of DISP is how to manage and secure information. The Information and Cyber Security category is critical, requiring the IT systems used by a business to meet a number of security criteria. However, the security criteria, security controls, and system documentation required for IT systems can be complex and challenging to create and maintain.

Kojensi is a proven and accredited platform for classified information collaboration and file sharing that enables productivity, while managing the level of compliance and security of information required by DISP. It provides a simple and secure cloud-based collaboration space and store for files and documents up to and including Australian Government PROTECTED information.

KOJENSI PROVIDES DISP READY INFORMATION AND CYBER SECURITY

Kojensi can help you comply with core DISP controls as follows:

Facilities Security

Physical premise security is a multi-layered process from the front door right through to the server room. Kojensi is hosted from within an accredited Australian facility, to provide a ready to use platform that meets ISM standards for physical data centre accreditation.

Personnel Security

Changes to your existing policies, procedures, plus the training, monitoring and reporting on personnel for DISP are time consuming, complex and sometimes difficult to implement and maintain. The archTIS team that manages the Kojensi SaaS platform are all certified specialist professionals. This reduces your requirement to have specialist personnel on your team to manage the underlying platform – allowing you and your team to focus on the processes and governance elements that are key to growth in your business.

Information Security

The level of compartmentalised access and sharing controls required by DISP for the management of sensitive/classified information can be costly and difficult to achieve. Kojensi provides a simple and secure cloud-based collaboration space and store for files and documents - up to and including Australian Government PROTECTED information. Kojensi's Attribute Based Access Controls (ABAC) enforce access policies in real-time to:

- Share sensitive files, co-edit content and collaborate securely.

- Invite internal or external parties into your workspaces while ensuring information remains secure and compartmentalised using ABAC policies.

- Apply DISP specific data governance to regulated content – without changing your existing infrastructure governance policies.

- Get a full audit trail of all interactions within Kojensi.

- Reduce the hidden costs associated with the housing and up-keep of cyber assets to the highest patch levels.

Security Governance

Governance is critical to DISP accreditation, however, enforcing these guidelines is another matter. Built into the core of Kojensi is a policy engine that applies your information security and governance requirements to all users of and files stored within Kojensi. Enforcing compliance and transparency in this way assists with reporting elements required for DISP.

KOJENSI IS A PROVEN AND ACCREDITED PLATFORM FOR COMPARTMENTALISED CLASSIFIED INFORMATION COLLABORATION
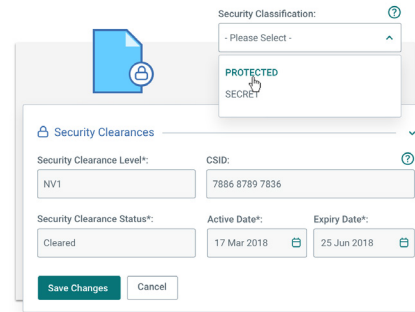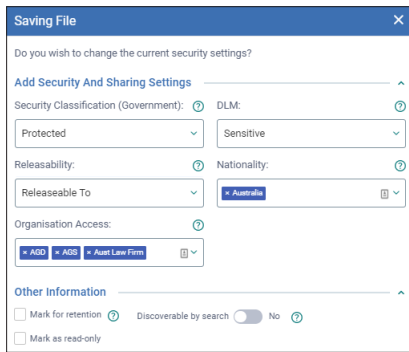

Designed for Defence

Kojensi has been designed from the ground up to meet the specific needs of Government, Defence, Defence Industry and those that engage in Defence business. It has been accredited to store up to and including Australian Government PROTECTED information.

Get Multi-Level Security with Ease

With Kojensi, Defence Industry can collaborate with each other and Defence to securely share any number of files that may have multiple different classifications within a single repository for ease of management via customer-defined ABAC policies. This assists you in meeting compliance and security requirements of the DISP program.
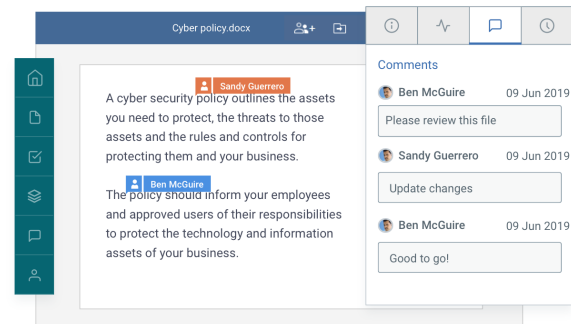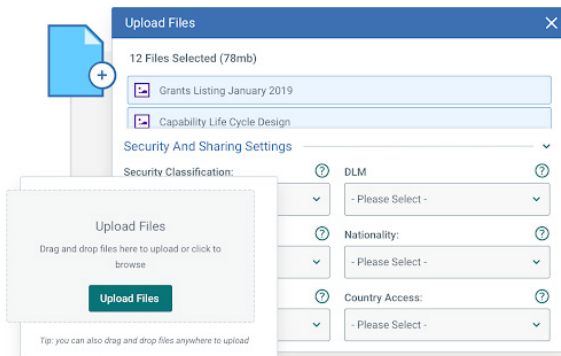
Control how information is accessed and used

Kojensi enables information owners to set and enforce strict control over information access and sharing, using Attribute Based Access Control (ABAC). Access is only granted once a user meets the requirements to release a file to them based on based on key attributes including: a user's organisation, nationality, clearance, and compartmentalisation of information.

Increase productivity with collaboration tools

Kojensi has a secure collaboration suite embedded within the platform, that allows for the creation and co-editing of common document and the capability of making interactive comments about the work that you are performing with others. Share and collaborate on sensitive files using a simple and secure interface, providing the right access to the right people, to help to prevent data loss or misuse.

THE ATTRIBUTE-BASED ACCESS CONTROL (ABAC) ADVANTAGE

Attribute Based Access Control (ABAC) is a zero trust security model that allows individuals to define rules to control who accesses information and under what conditions. This enables the right people to access the right information at the right time. ABAC allows government, defence, and industry to safely share and collaborate on information and ensure that the conditions they set on access and sharing will be enforced.

archTIS

archTIS.com | info@archtis.com   Australia | United States | United Kingdom