kojensi
SAAS

SECURE FILE SHARING AND COLLABORATION FOR CRITICAL INFRASTRUCTURE

SECURE INFORMATION SHARING FOR CRITICAL INFRASTRUCTURE

The Australian Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (SLACIP Act) which amends the Security of Critical Infrastructure Act 2018 (SOCI Act), and Systems of National Significance (SoNS) regulations are aimed at improving the resilience and risk management practices of Australia's Critical Infrastructure sector and making it easier for organisations and governments to securely share information.

Kojensi allows the Critical Infrastructure Responsible Entity to:

- Securely share files with different clearance levels internally, with partners and government within a single repository.
- Instantly establish a secure workspace to collaborate internally and with third parties for the required Plans, Assessments, and Asset Registers, while ensuring only cleared users can see and access protected information.
- Control access and sharing with granular, zero trust ABAC policies using attributes including security classification, country and organisational releasability.
- Assists in meeting SOCI, SLACIP, SoNS, and other Australian Government Acts and frameworks including DISP, PSPF, ISM, C2M2, CPS234, etc.
- Share files easily and quickly, in a highly secure environment.

Use Case:

CHALLENGE

Responsible Entities deemed as Critical Infrastructure must register their assets; develop, review, report on, and comply with a Risk Management Plan. The Risk Management Plan identifies cybersecurity hazards that include physical, personnel, supply chain, and cyber hazards. Furthermore, those entities deemed a System of National Significance (SoNS), must also comply with the Act's Enhanced Cyber Security Obligations (ECSO). These include Incident Response Plans, Cyber Security Exercises, and Vulnerability Assessments. Additionally, companies and third party's parties that work with, and supply these entities must also have a secure method to share and collaborate on files.

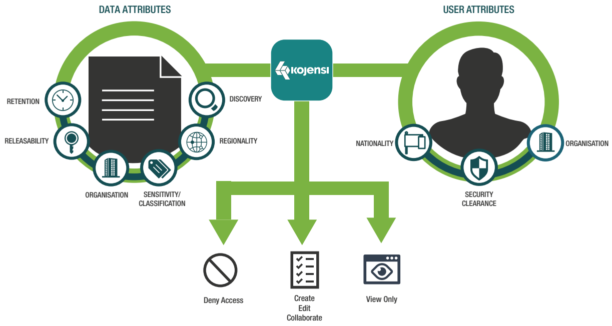
SOLUTION

Risk management and governance are critical to SLACIP and SoNS, however, enforcing these mandates is another matter. The level of compartmentalised access and sharing controls required for the management of sensitive and classified information can be costly and difficult to achieve.

Kojensi provides a turnkey solution with a government-accredited PROTECTED information sharing cloud service and is also available on-premises. Kojensi's industry leading attribute-based access control (ABAC) model makes the platform unique. User and document attributes control the flow of information and facilitate secure sharing to validate access and sharing policies each and every time a file is accessed or shared internally or with industry partners. A full audit trail, version control, and tracking ensure transparency and help meet auditing requirements.

Critical Infrastructure organisations can consume the platform as needed, without the substantial costs of implementing new on-premises secured ICT infrastructure. Within minutes, users can set up a shared workspace and invite internal and external partners in to share and collaborate on the information required to carry out projects, knowing that users will only have access to information they are authorised to.

PROTECT FILES USING KOJENSI'S ABAC POLICIES & CONTROLS



KOJENSI DELIVERS SECURE FILE SHARING & COLLABORATION

Critical Infrastructure information is shared and collaborated on within the secure Kojensi platform, ensuring it is not inappropriately accessed. It provides a cost-effective accredited platform to ensure the security of classified and sensitive information to meet SLACIP, SoNS and other compliance requirements.

Securely share sensitive information with internal and third parties

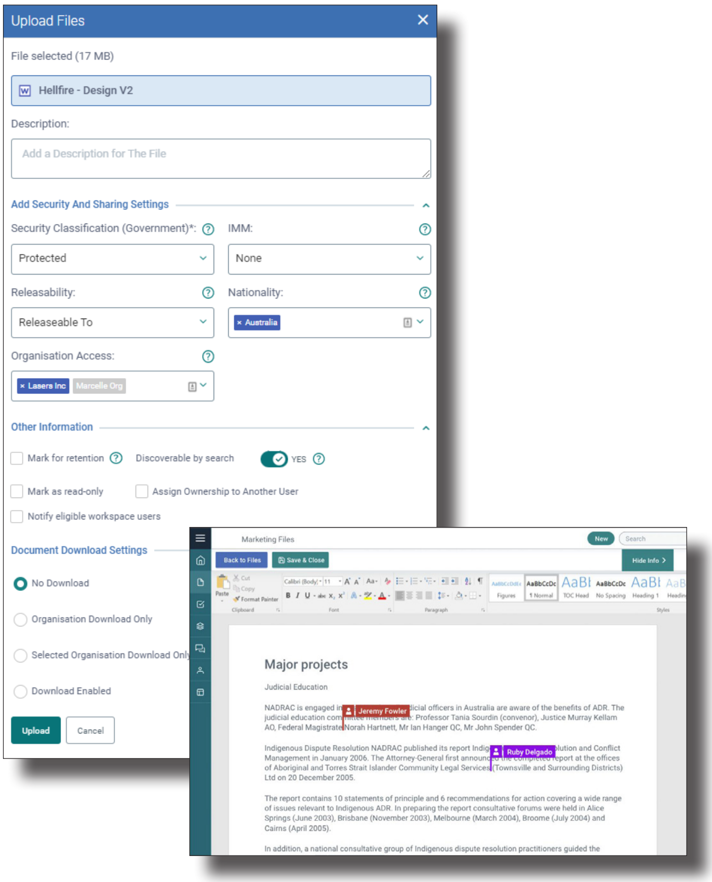
Kojensi allows for easy knowledge transfer in an accredited safe and controlled hosted environment without having to grant access to your internal networks.

With Kojensi, securely collaborate internally, with partners and government, and share files that may have multiple classifications within a single repository for ease of management using Attribute Based Access Control (ABAC) policies.

Information owners can set and enforce strict control over information access and sharing using ABAC policies. Access is only granted once a user meets the requirements to release a file to them based on key attributes including a user's organisation, nationality, clearance, and compartmentalisation of information.

Securely share and co-author sensitive files

Information stays within a secure government-accredited PROTECTED cloud service. Users can edit the files directly within each workspace to ensure the security, integrity and availability of the content. Users can upload multiple files at once or large files, and notify relevant parties that the information is now ready and available to access.



Upload Files

File selected (17 MB)

Hellfire - Design V2

Description: Add a Description for The File

Add Security And Sharing Settings

Security Classification (Government)*: Protected

IMM: None

Releasability: Releaseable To

Nationality: × Australia

Organisation Access: × Lasers Inc, Marcelle Org

Other Information

☐ Mark for retention

Discoverable by search: YES

☐ Mark as read-only

☐ Assign Ownership to Another User

☐ Notify eligible workspace users

Document Download Settings

● No Download

○ Organisation Download Only

○ Selected Organisation Download Only

○ Download Enabled

Marketing Files

Major projects

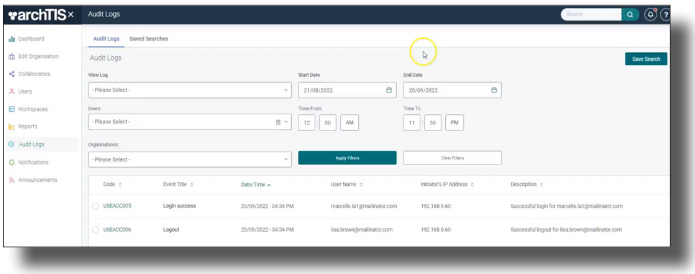
Judicial Education

NADRAC is engaged in [Jeremy Fowler] icial officers in Australia are aware of the benefits of ADR. The judicial education com[…]: Professor Tania Sourdin (convenor), Justice Murray Kellam AO, Federal Magistrate Norah Hartnett, Mr Ian Hanger QC, Mr John Spender QC.

Indigenous Dispute Resolution NADRAC published its report Indig [Ruby Delgado] lution and Conflict Management in January 2006. The Attorney-General first announc[…]eport at the offices of Aboriginal and Torres Strait Islander Community Legal Services (Townsville and Surrounding Districts) Ltd on 20 December 2005.

The report contains 10 statements of principle and 6 recommendations for action covering a wide range of issues relevant to Indigenous ADR. In preparing the report consultative forums were held in Alice Springs (June 2003), Brisbane (November 2003), Melbourne (March 2004), Broome (July 2004) and Cairns (April 2005).

In addition, a national consultative group of Indigenous dispute resolution practitioners guided the



Audit Logs

View Log: - Please Select -

Start Date: 21/08/2022

End Date: 20/09/2022

Users: - Please Select -

Time From: 12 : 00 AM

Time To: 11 : 59 PM

Organisations: - Please Select -

Code	Event Title	Date/Time	User Name	Initiator's IP Address	Description
USEACC005	Login success	20/09/2022 - 04:34 PM	marcelle.la1@mailinator.com	192.168.9.60	Successful login for marcelle.la1@mailinator.com
USEACC006	Logout	20/09/2022 - 04:34 PM	lisa.brown@mailinator.com	192.168.9.60	Successful logout for lisa.brown@mailinator.com

Audit User Activity

Kojensi audits all activity in the platform to ensure compliance and assist with auditing requirements. It includes a robust auditing platform that records a full user interaction history of all changes made to files, workspaces and other administrative tasks.

Designed for Compliance

Kojensi assists organisations to easily comply with compliance requirements such as ITAR, ISM, SLACIP, SoNS, DISP and PSPF.

Data Hosted Locally

Data is hosted locally in Australia by an ASD-certified PROTECTED cloud provider, ensuring all data is stored and processed in local data centres.

Classifications and Markings

Kojensi allows you to add native country specific classifications, helping you to protect highly classified, sovereign information.

archTIS

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