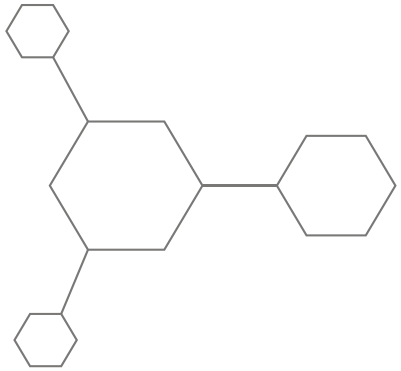
EBOOK

COMPLYING WITH AUSTRALIA'S SLACIP ACT & SONS REGULATIONS FOR CRITICAL INFRASTRUCTURE

archTIS



CONTENTS

WHAT ARE THE SLACIP ACT AND SONS?

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 share information securely. They impact a broad range of industries deemed critical infrastructure, including Energy, Telecom, Financial Services, Utilities, Healthcare and Education.

At the high level, the amendments to the SOCI Act include:

- Expanded the definition of critical infrastructure
- Government Assistance Measures
- Notification of Data Centre Providers
- Positive Security Obligations
    - Register of critical infrastructure assets
    - Mandatory cyber security incident reporting
    - Risk Management Program
- Systems of National Significance
    - Enhanced cyber security obligations

WHAT IS THE PURPOSE OF THE SLACIP ACT AND SONS?

Responsible Entities deemed Critical Infrastructure must register their assets; and 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.[1]

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 parties that work with, and supply these entities must also have a secure method to share and collaborate on files.

[1] https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/slacip-bill-2022

WHO DOES SLACIP AFFECT?

The following categories of organisations are subject to the requirements laid out in the SLACIP Act:

- Critical Data Storage or Processing
- Financial Services and Markets
- Communications
- Defence
- Higher Education and Research
- Food and Grocery
- Healthcare and Medical
- Water and Sewage
- Space Technology
- Transport
- Energy

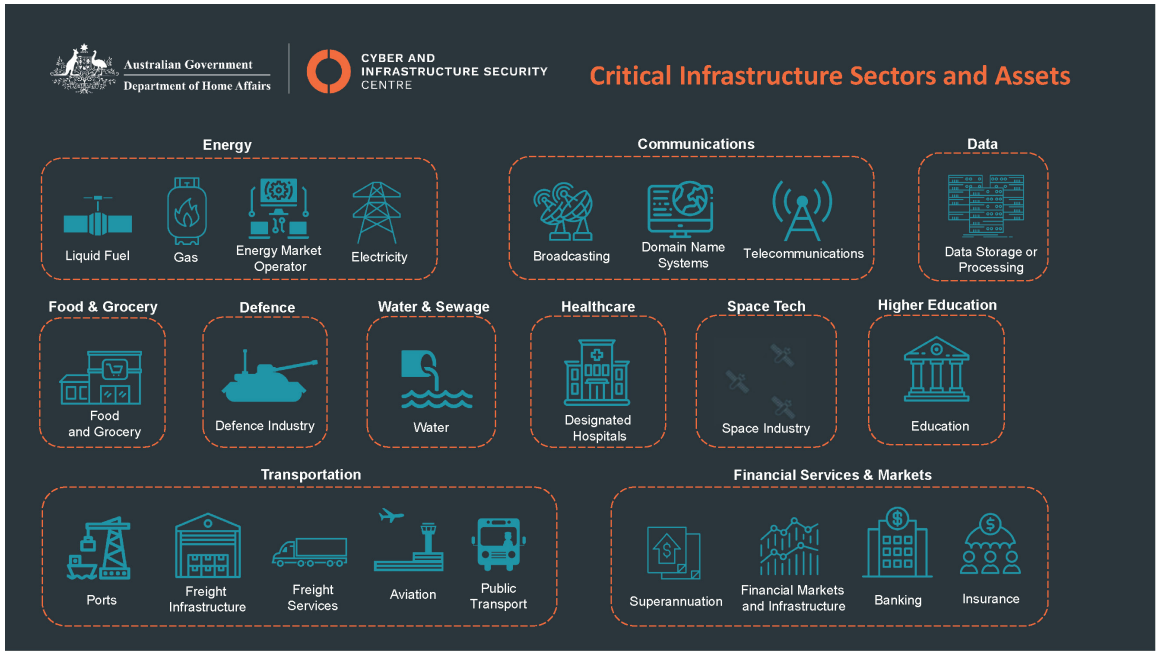


Diagram above is from the Cyber and Infrastructure Security Outreach, Department of Home Affairs | 2023

WHO DOES SONS AFFECT?

A small subset of critical infrastructure entities must also adhere to SoNS (System of National Significance) if they are identified as an asset of national significance. There are two key factors used to determine whether an asset is of national significance:[2]

1. Does the asset have interdependencies with other critical infrastructure assets?
2. Would its compromise significantly impact national security, defence, or social/economic stability of Australia?

[2] https://www.csa.gov.sg/legislation/codes-of-practice

General Obligations

The general obligations for all Critical Infrastructure providers are that they must:

- Establish, maintain, implement and regularly review a risk management program;
- Identify, (and as far as is reasonably practicable) prevent and mitigate risks and hazards that, could impact the availability, integrity, reliability and confidentiality of critical infrastructure assets, and;
- Provide an annual report to the Government regarding their risk management program.

The additional obligations for Systems of National Significance are to:

- Develop cyber security incident response plans to prepare for a cyber security incident;
- Undertake cyber security exercises to build cyber preparedness;
- Undertake vulnerability assessments to identify vulnerabilities for remediation, and/or;
- Provide system information to develop and maintain a near real-time threat picture.

WHAT DOES THIS LEGISLATION MEAN FOR MY ORGANISATION?

If your organisation falls under Critical Infrastructure in Australia, you need to adopt and maintain a risk management program, including any cyber threats to the digital ecosystem of a critical infrastructure asset and insider threats within a Critical Infrastructure workforce.

In addition to the obligations for critical infrastructure assets under the SLACIP Act, any organisation classified as SoNS must also comply with Enhanced Cyber Security Obligations (ECSO)[3]. Companies that work with and supply these organisations must also have a secure method to collaborate on sensitive and Protected information.

In its role as a regulator under this framework, the Cyber and Infrastructure Security Centre (CISC) drives an all-hazards critical infrastructure regime in partnership with governments, industry and the broader community. The CISC focuses on education, advice and information exchange to help critical infrastructure asset owners and operators understand and meet their regulatory requirements and keep abreast of the evolving risk environment.

[3]https://www.cisc.gov.au/critical-infrastructure-centre-subsite/Files/cisc-factsheet-systems-of-national-significance-enhanced-cyber-security-obligations.PDF

ARCHTIS OFFERINGS

archTIS solutions apply and enforce dynamic, policy-driven access controls (ABAC) that leverage both user and data attributes to ensure your users and partners access, share and collaborate on sensitive and classified information—securely.

KOJENSI

SAAS PLATFORM FOR SHARING SENSITIVE & CLASSIFIED FILES SECURELY

Implement compartmentalised military-grade classified information collaboration and file sharing with the accredited Protected cloud-based Kojensi SaaS document management platform.

NC PROTECT

FOR ADDING ABAC POLICY-BASED ACCESS & DATA PROTECTION TO MICROSOFT APPLICATIONS

Add granular policy-based control over how information is shared, accessed and used to your Microsoft 365 and on-premises file sharing applications to enhance out of the box data protection capabilities.

WHAT ARE THE CHALLENGES TO BECOMING SLACIP AND SONS COMPLIANT?

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 managing sensitive and classified information can be costly and difficult to achieve. Bespoke solutions can take months or longer to build, and the expense is prohibitive for small to medium enterprises. A hosted platform that is built to meet the requirements of SLACIP, SoNS and other Australian government requirements, including ISM, DISP and PSPF, provides a viable option for rapid deployment and onboarding to help quickly assist with information security requirements.

HOW CAN ARCHTIS HELP?

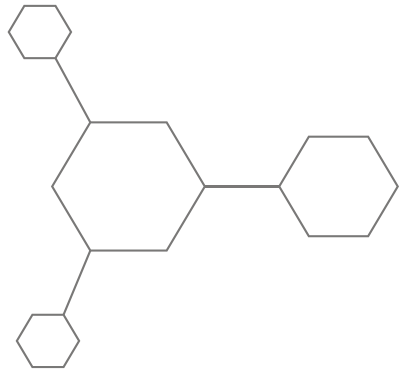
As the leader in policy-enforced information security, archTIS has helped organisations of all shapes and sizes to comply with worldwide regulations by leveraging data protection technologies to meet regulatory requirements. With a focus on data protection requirements, archTIS products enable Critical Infrastructure entities to align the SLACIP requirements and the Cyber and Infrastructure Security Centre (CISC) recommendations for managing risks to Australia's critical infrastructure and their supply chains.

The following chart maps archTIS' solution capabilities to the requirements of the SLACIP and SOCI Acts.

ARCHTIS CAPABILITIES MATRIX FOR SLACIP AND SOCI ACT REQUIREMENTS

SLACIP /SOCI REQUIREMENT	ARCHTIS SOLUTIONS
CIRMP All Hazard Rules The Rules contain obligations relating to protections within four key hazard	**Kojensi SaaS Document Management and Information Sharing Platform** **NC Protect for Microsoft 365 and SharePoint Server On-Premises Environments**
1. Physical security and natural hazards Physical security risks to parts of the asset critical to the functioning of the asset, including physical access to sensitive facilities (e.g., control rooms) or natural disasters.	**Kojensi SaaS Document Management and Information Sharing Platform** Kojensi provides a turnkey solution with an ASD-certified PROTECTED information sharing cloud service and is also available on-premises to support SLACIP compliance requirements. Kojensi SaaS is hosted from within an accredited Australian facility, to provide a ready-to-use platform that meets ISM standards for physical data centre accreditation.
2. Cyber and information security 'Cyber' risks to digital systems, computers, datasets, and networks that underpin critical infrastructure systems. This includes improper access, misuse, or unauthorised control.	**Kojensi SaaS Document Management and Information Sharing Platform** Kojensi enables secure knowledge transfer in an accredited, safe and controlled hosted environment without having to grant access to your internal networks. • Built into the core of Kojensi is a policy engine that applies your information security and governance requirements to all platform users and files stored within Kojensi. • Facilitates the secure management of protected information, enabling secure sharing and collaboration among entities, sub-entities, and government bodies. • Supports the secure sharing of files with multiple classifications within a single repository for ease of management. • Enforces strict control over information access and sharing using ABAC-enabled policies set by the information owners. • Grants access to files only if a user meets the policy requirements based on key attributes, including a user's organisation, nationality, clearance, and compartmentalisation of information. • Includes a robust auditing platform that records a full user interaction history of all changes made to files, workspaces and other administrative tasks. • Assists in meeting SOCI, SLACIP, SoNS, and other Australian Government Acts and frameworks, including DISP, PSPF, ISM, C2M2, CPS234, etc. • Kojensi empowers CI organisations to establish a robust data security posture in accordance with SLACIP Act mandates, bolstering regulatory compliance and upholding the principles of critical infrastructure protection.

2. Cyber and information security (cont)	NC Protect for Microsoft 365 and SharePoint On-Premises Environments
'Cyber' risks to digital systems, computers, datasets, and networks that underpin critical infrastructure systems. This includes improper access, misuse, or unauthorised control.	NC Protect software aligns with the provisions of the SLACIP Act by offering dynamic data-centric security, which automates the identification and classification of unstructured data in Microsoft 365 and SharePoint on-premises, cloud, and hybrid environments. • By utilising attribute-based access and control (ABAC) policies, NC Protect facilitates compliance with the SLACIP Act's requirements for data access, usage, and sharing rights based on real-time data and user attribute comparisons. • NC Protect's capabilities extend to scanning the Microsoft environment, adding metadata tags to documents, or leveraging sensitivity labels, thereby enabling evaluation of data and user attributes to determine appropriate access and protection levels in compliance with SLACIP Act guidelines. • The software's robust auditing features provide organisations with a comprehensive audit trail of document access, ensuring adherence to SLACIP Act reporting requirements and supporting regulatory compliance efforts. • NC Protect's granular access and usage control, combined with its auditing capabilities, enable organisations to effectively comply with SLACIP Act data security obligations and industry regulations. • By implementing NC Protect, organisations can strengthen their data security framework in accordance with the SLACIP Act, safeguarding sensitive information and supporting regulatory objectives. • The ABAC solution offered by NC Protect promotes seamless information sharing and collaboration, facilitating secure data exchange with partners and stakeholders in compliance with SLACIP Act guidelines. • NC Protect ensures consistent data protection across various environments, including on-premises, cloud, and hybrid setups, aligning with the SLACIP Act's emphasis on safeguarding critical infrastructure assets. • The software's automated identification, classification, and protection of unstructured data enhance data security, addressing SLACIP Act requirements and strengthening organisational compliance efforts. • NC Protect empowers CI organisations to establish a robust data security posture per SLACIP Act mandates, bolstering regulatory compliance and upholding the principles of critical infrastructure protection.



3. Personnel

The 'trusted insider' risk posed by critical workers who have the access and ability to disrupt the functioning of the asset.

CISC Recommendations:

- Identify essential components or systems and who has access and control over these systems. 'Principle of least privilege'.
- Heightened monitoring of personnel with access to critical systems and ensuring these are checked and updated regularly, on a 'need-to-know' basis.
- Cyber Security training for staff, including data storage, anti-phishing and password security.
- Multi-factor authentication for personnel credentials, especially for critical positions/employees.

Kojensi SaaS Document Management and Information Sharing Platform

Kojensi adds controls to prevent sensitive data abuse once access has been granted to authorised users to help mitigate insider threats.

- Kojensi offers the ability to centrally manage sensitive information in a controlled collaboration environment.
- Access policies are defined by the Document Owner/Creator and enforce the concept of least privilege by default.
- Ability to dynamically remove access when policies or access conditions change.
- Force users to view sensitive files in a Secure Reader that disables print, copy, save, and download capabilities – enforcing secure read-only access.
- Automatically add a secure watermark to documents via the Secure Reader that can't be removed to identify the user handling the file, including name, date, etc.
- Uses Multifactor Authentication (MFA) for login.
- Enforces 'need to know' access.
- Includes a robust auditing platform that records a full user interaction history of all changes made to files, workspaces and other administrative tasks.
- Already compliant with ISM security controls to support PROTECTED information including password security, MFA and data storage (and auditing).

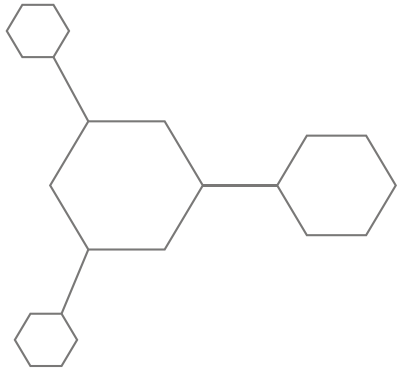
NC Protect for Microsoft 365 and SharePoint On-Premises Environments

NC Protect enables organisations to extend archTIS' policy-enforced data protections into corporate systems.

Admins and other users need to access sensitive data for day-to-day tasks, but security should not just stop at determining access. NC Protect provides additional real-time controls to prevent sensitive data abuse once access has been granted to authorised users to help mitigate insider threats.

- For example, disable options to print, download and/or copy sensitive documents in Office applications (Word, Excel, PowerPoint).
- Or force users to view sensitive files in a Secure Reader that disables print, save, and download capabilities – enforcing secure read-only access.
- Automatically add a secure watermark that can't be removed to identify the user handling the file including name, date, time, location, IP address, etc.
- Redact sensitive words and phrases in Office documents (Word, Excel, PowerPoint) or from files viewed in the built-in Secure Reader.
- Apply required visual markings (headers, footer, classification labels).
- Change usage/viewing rights based on the user's location or device (e.g., home or WiFi).
- Mitigates privileged access by preventing admins from opening information they are not authorised to access.
- Enforces 'need to know' access.
- Leverages Microsoft Entra ID (formerly Azure AD) attributes.
- Includes a robust auditing platform that records a full user interaction history of all access to, actions taken with, and changes made to files and NC Protect policies.

4. Supply chain	Kojensi SaaS Document Management and Information Sharing Platform
Risk of disruption to critical supply chains leading to a relevant impact on the critical infrastructure asset. The threat could be naturally occurring, malicious or purposefully intended to compromise the critical infrastructure asset. Organisations are targeted by focusing on weaker links in their supply chain. **CISC Recommendation:** Ensure vendors with access to sensitive data/systems have sufficient security personnel and cyber security resilience policies built into contract arrangements.	Kojensi can be the central platform for your organisation and your suppliers to securely collaborate on sensitive information. This enables organisations to access a trusted platform to collaborate but maintain global and specific permissions across information managed through the platform. • Kojensi allows for easy knowledge transfer in an accredited, safe and controlled hosted environment without having to grant access to your internal networks. • Ensures sensitive information is separated from potentially vulnerable supplier systems. • Users can set up a secure workspace to collaborate internally and with third parties for the required Plans, Assessments, and Asset Registers, and other sensitive information while ensuring only cleared users can see and access sensitive and protected information. • Kojensi's ABAC policies ensure users will only have access to information they are authorised to. • The ability to identify, flag and audit special types of information (i.e., Protected Information) to make the job of compliance and reporting easy. **NC Protect for Microsoft 365 and SharePoint On-Premises Environments** NC Protect can be deployed across existing collaboration tools within your supply chain. NC Protect can force users to share sensitive information only via secured collaboration tools: • Enables secure third-party access to Microsoft 365 tools, including SharePoint, Teams and OneDrive. • Automatically encrypt files sent by email or alternatively remove email attachments and replace them with secure links to the files in SharePoint. • Enable the ability to have consistent access rules across different tenancies and domains.



Use and Disclosure of Protected Information

The Security of Critical Infrastructure Act 2018 (the Act) limits the use and disclosure of information obtained or created in accordance with the Act – which is known as protected information. It is an offence to use or disclose protected information unless authorised.

Unauthorised use or disclosure of protected information attracts an offence that is punishable by imprisonment for 2 years or 120 penalty units, or both.

Kojensi SaaS Document Management and Information Sharing Platform

Kojensi can operate as a secure place to author, manage and control all Protected Information.

- 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.
- Enables the authoring of Protected Information using familiar MS Office-like tools in the browser – meaning high risk CI/SoNS information never has to touch corporate systems.
- Upload corporate information and control access to this data with Home Affairs, ACSC and other parties to protect corporate data assets.
- Collaborate with Home Affairs, ACSC and others whilst authoring Plans, Assessments and Registers using co-authoring, tasks, comments and chat (all contained within the Kojensi Platform).
- Comprehensive version management, auditing and reporting making observability of Protected Information compliance easy.
- Revoke access to information instantly.
- Ensures only authorised users can access Protected information.
- Controls the ability for users to download, print and copy information (through our secure reader).
- Watermark documents to embed user information into versions of Protected Information
- Enables an alternative collaboration platform, independent of corporate systems, highly relevant when suffering a cyber incident within corporate systems, this provides a secure channel to work with Home Affairs and ACSC in navigating these scenarios. Comprehensive data protection, including a backup and data archiving regime that complies with ISM guidance.

NC Protect for Microsoft 365 and SharePoint On-Premises Environments

- Secure collaboration internally and with third parties for the required Plans, Assessments, and Asset Registers, while ensuring only cleared users can see and access Protected information.
- Ensures only authorised users can access Protected information.
- Mitigates privileged access by preventing admins from opening information they are not authorised to access.
- Manages the ability to share Protected information with unauthorised users via Microsoft 365 applications (SharePoint, OneDrive and Teams) and Exchange email to ensure information is only shared with authorised individuals.
- Redact sensitive content (words and phrases) from documents in Office or in the built-in Secure Reader.
- Prevent the downloading or saving (e.g., to a thumb drive or computer) of protected information.
- Encrypt files with Protected information both at rest and in motion if required. Including the ability to encrypt using external HSM (i.e., manage your own keys).

KEY TAKEAWAYS

Organisations can leverage the archTIS suite of policy-driven information security solutions to become compliant today and remain compliant in the future.

The SLACIP Act and SoNS regulations play a crucial role in enhancing the security and resilience of Australia's critical infrastructure sector. By implementing a robust Risk Management Program and leveraging secure information sharing platforms like Kojensi and NC Protect for Microsoft application users, organisations can meet compliance requirements and effectively manage the risks associated with critical infrastructure assets.

Here is the summarised advice on addressing the requirements of the SLACIP and SOCI Acts.

Access Control

1. Enhance access control with policy-enforced ABAC policies
2. Ensure only authorised users can access Protected information
3. Ensure third party data hosting services are properly accredited and physically secure

Data Security & Encryption

1. Simplify data security, and accelerate time to compliance
2. Implement granular access control to sensitive data
3. Proactively mitigate insider threats
4. Secure protected data at rest and in motion with encryption

Contact us for comprehensive access control and data protection solutions that address SLACIP Act and SoNs compliance.

archTIS

ABOUT ARCHTIS LIMITED

archTIS Limited (ASX:AR9) is a provider of innovative software solutions for the secure collaboration of sensitive information. The company's award-winning data-centric information security solutions protect the world's most sensitive content in government, defence, supply chain, enterprises and regulated industries through attribute based access and control (ABAC) policies. archTIS products include Kojensi, a multi-government certified platform for the secure access, sharing and collaboration of sensitive and classified information; and NC Protect for enhanced information protection for file access and sharing, messaging and emailing of sensitive and classified content across Microsoft 365 apps, SharePoint Server, NetApp, Nutanix Files and Windows file shares.

For more information visit archtis.com. Follow us on twitter @arch_tis

archTIS

archTIS.com | info@archtis.com

Australia | United States | United Kingdom