South Australian Protective Security Framework

GOVSEC5:

Managing the security of contractors and service providers

SOUTH AUSTRALIAN PROTECTIVE SECURITY FRAMEWORK

Contents

SOUTH AUSTRALIAN PROTECTIVE SECURITY FRAMEWORK

Purpose

1. Security risks can arise through the procurement of goods and services and effective risk management is required to reduce the likelihood and consequence of security issues or incidents.

2. This policy supports the South Australian Government's procurement requirements[1] which detail how agencies procure goods and services. The requirements of this policy seek to ensure security risk is a considered element in all procurement processes.

Core Requirement 5

Manage any security risks that arise from the procurement of goods and services

Supporting Requirements

3. To ensure any security risks that arise from the procurement of goods and services are managed, agencies[2] **must:**

    I. identify and mitigate security risks to the agency's people, information and assets generated by the procurement

    II. ensure relevant security terms and conditions are included in contracts and service agreements that mange identified security risks to the procurement

    III. manage and monitor:

        a. security risks for changes or incidents that could affect the procurement, service agreement or security of the agency

        b. the performance of the contractor (including subcontractors) over the lifetime of the contract

    IV. implement appropriate security arrangements to manage the completion or termination of a contract or agreement

[1] The State Procurement Board (SPB) issues the Procurement Policy Framework to guide procurement in the South Australian Government. A new South Australian Government Procurement Framework is currently being prepared by Procurement Services South Australia and is expected to commence in December 2020. This footnote will be amended accordingly.

[2] This policy applies to all South Australian public sector agencies (as defined in section 3(1) of the *Public Sector Act 2009*) and to any other person or organisation that is generally subject to the direction of a Minister of the Crown; all of which are referred to in this policy as "Agencies".

SOUTH AUSTRALIAN PROTECTIVE SECURITY FRAMEWORK

Terminology

Term	Meaning
MUST	Use of the word **must** (or **required** or **responsible for**) indicates a requirement or action of the policy to which all agencies must adhere or undertake
MUST NOT	Use of the words **must not** indicates an action prohibited by this policy
SHOULD	Use of the word **should** (or **recommended**) indicates an action that agencies ought to undertake, unless prevented by legitimate circumstances or justification
SHOULD NOT	Use of the words **should not** (or **not recommended**) indicates an action which agencies should avoid, unless legitimate circumstances prevent another course of action being taken
MAY	Use of the word **may** indicates an action which is completely optional, but may be provided as a suggestion or considered best practice

Definitions

Term	Definition
agency	as per the definition of *public sector agency* (as defined in section 3(1) of the *Public Sector Act 2009*) and to any other person or organisation that is generally subject to the direction of a Minister of the Crown; all of which are referred to in this policy as “Agencies”.
compromise	includes, but not limited to, loss, misuse, interference, unauthorised access, unauthorised modification, unauthorised disclosure.
contract	a formal and legally binding agreement which outlines the terms and conditions for the provision of goods or services by an external entity or third party to a South Australian Government agency (same as **service agreement**)
contractor	the external or third-party contracted to provide services to an agency (same as **service provider** and for the purposes of this policy, includes subcontractors)
controls	see **risk treatment**
employee	see **personnel**
mitigation	see **risk treatment**
personnel	all people that an agency employs (including contracted employees)
personnel security	the policies and procedures that seek to mitigate the risk of personnel exploiting their legitimate access to an agency’s information or assets for unauthorised purposes
procurement	the process of finding and agreeing to terms for the provision of goods and services
protection	the treatments, mitigations or controls implemented to prevent or minimise the likelihood, of compromise to an agency’s people, information or assets
resources	an agency’s people, information and assets

Term	Definition
risk tolerance	the amount of level of risk an agency is comfortable taking after risk treatments have been applied to achieve and objective or manage a security risk
risk treatment	considered, coordinated and efficient actions and resources that mitigate or lessen the likelihood or negative consequences of a security risk
security plan	how an agency articulates how its security risks have been identified, prioritised and will be managed in line with the agency's objectives
security risk	something that can result in compromise, loss, unavailability or damage to an agency's resources, including causing harm to people.
service agreement	see **contract**
service provider	see **contractor**
social engineering	deceiving or manipulating people into divulging confidential or personal information that may be used for fraudulent purposes
subcontractor	a person or entity that undertakes work or duties on behalf of a **contractor**
threat	a declared intent to inflict harm on personnel or property
vulnerability	the degree of susceptibility and resilience of an agency to risks and threats

Acronyms

Acronym	Words
SAPSF	South Australian Protective Security Framework

Guidance

Identifying security risks in procurement

4. The overall value of a procurement can be significantly reduced by negative security outcomes. Agencies remain responsible for identifying, managing and mitigating security risks when the provision of goods and services is outsourced.
5. While an agency **must** manage any security risks, contractors play an important part in identifying, managing and mitigating those risks.
6. The South Australian Governments procurement requirements mandate that risks to the procurement **must** be identified, managed and monitored. This policy mandates that protective security risks are specifically considered within that same process.
7. If security risks identified in procurement processes cannot be mitigated to an acceptable level, or the risks to government or the agency are too great, agencies **should** seek alternate procurement arrangements and record any decisions to do so. This includes where a security risk cannot be quantified or is too complex to be calculated.

Understanding risks, threats or vulnerabilities to procurement

8. If an agency does not understand or appreciate the risks associated with a procurement, they will not be able to identify appropriate risk treatments. For example, cloud technologies may seem more affordable and faster, however, specific contract clauses or operational controls might be required if that contractor stores information in a foreign country.
9. **Table 1** provides some examples of potential risks associated with procuring goods and services:

***Table 1* – Potential risks associated with procurement**

Risk type	Risk description
Insider threat	• It is a known and effective tool to use people (including contractors) with access to an agency's information or resources to obtain that information for purposes not in the interests of the agency, South Australian or the nation more broadly. • Australia, and South Australia more specifically, is an attractive target for exploitation given its prominent role in the Asia-Pacific region, its strong diplomatic ties with other nations and its resource, energy, defence and cyber sectors particularly. • Compromise of an agency's information or resources could be used to gain economic, diplomatic or political advantage against South Australia or Australia (e.g. intellectual property, financial records, ICT system design). Personal information can also be used for malicious activities through social engineering. • State-sponsored actors (e.g. foreign intelligence services) work on behalf of foreign government or entities to intentionally infiltrate, compromise, steal or manipulate information which can have a detrimental impact on state and national security and commercial sectors (e.g. resources, financial, telecommunications) • Technical capabilities are becoming more sophisticated and easier to use. The potential high gains to be made from targeting vulnerable sectors or systems may increase the risk of insider threat to agencies.

Supply chain	• Agencies may engage multiple contractors, or a contractor may engage multiple subcontractors as part of the supply chain. The more parties are subject to any procurement or service provision, the greater or more complex the risk becomes.
	• It is **recommended** to:
	  ○ consider the security risks of each contracted provider independently and holistically
	  ○ reduce vulnerabilities and ensure security continuity to manage risks along the entire supply chain

Foreign involvement	• Arrangements where resources are made or held outside of Australia (by the contractor or a subcontractor) **may** have additional risks. For example, services located offshore are subject to laws of those countries and **may** be subject to lawful and covert collection.
Differences in legal and business cultures	• Tolerance (legal and law enforcement effectiveness) and acceptance of corruption and crime can be vastly different in other countries. • Foreign enterprises **may** be owned, influenced or funded by foreign governments • A lack of visibility into the contractor's or services providers' corporate structure, funding or use of non-reciprocating safe harbours • Extrajudicial behaviours of foreign governments **may** give rise to further risks that need consideration. The lack of the rule of law **may** lead to attempts to misappropriate information or assets (including by organised crime)

Multiple legal jurisdictions	• Information or assets **may** be subject to the laws of multiple jurisdictions. This might occur when:
	  ○ Foreign laws apply to a contractor due to it being located offshore (sometimes in multiple locations)
	  ○ Foreign laws have extra-territorial application to a contractor located in Australia
	  ○ Goods or services transit through a third-party foreign jurisdiction
	• Most foreign jurisdictions have legislative powers that allow access to assets, communications and stored information for purposes of law enforcement and national security. In some circumstances, international law enforcement or national security agencies can access information held overseas or in Australia.
	• Contractors **should** provide assurances that any information they handle will align to the agency's risk tolerances and be managed securely.

10. Agencies **should** consider and seek to identify security risks that could affect or be caused by:
    a. the state or national interest
    b. risks to critical infrastructure (agency-specific, South Australian and national critical infrastructure)
    c. risks to people transacting with the agency via a contractor (or subcontractor)
    d. the ability to maintain control of information or resources that are outsourced, offshore or supply chain arrangement with potentially changing legal frameworks
    e. foreign involvement
    f. insider threat
    g. South Australian Government agencies or other entities
    h. agency security plans

Protective security terms and conditions

11. Relevant security provisions and associated protections **must** be included in contracts or service agreements. The benefit of ensuring security terms and conditions are identified means they are legally enforceable.
12. Agencies **should** do this by including terms and conditions in their procurement documents[3] relating to:
    a. imposing appropriate information, physical and personnel security requirements

[3] Such as requests for tender and subsequent contracts

b. identified security risks relevant to the procurement

c. ongoing management of security risks and any proposed risk treatments

13. **Table 2** outlines some of the **recommended** terms and conditions to be included.

***Table 2* - Recommended terms and conditions**

Security domain	Terms and conditions
Governance	• Governance arrangements include provision for agencies to: o amend (or terminate) a contract where issues of security concern arise (e.g. change of ownership to a non-approved entity, suspected or actual security breaches) o monitor ongoing contracts through all levels of subcontractors and supply chains o manage changes to the provision of goods or services o terminate the contract where the contractor fails or refuses to comply with the security terms and conditions, or mitigate security incidents • That require the primary contractor to: o notify of actual or suspected security incidents (particularly those involving security cleared personnel) and follow the directions of the agency in relation to investigations and outcomes (including other affected agencies or entities) (see SAPSF policy Security governance for more detail on reporting security incidents) o take reasonable steps to prevent, detect and respond to fraud and corruption o implement security measures to identify, manage, monitor and review security risks to the information or assets provided by the agency, including protecting them from compromise at all times o periodically review security measures under the contract to ensure the arrangements are current and address the risks, threat, vulnerabilities or criticalities o be responsible for managing and monitoring the protective security compliance of its subcontractors and supply chain arrangements, including regular security awareness training
Information	• Information handling controls and storage arrangements for sensitive and security classified information **must** be consistent with the requirements of the SAPSF. • Contractors **must** be able to demonstrate they are capable of handling or storing the agency's information securely • Ensure information assets remain the property of the South Australian Government, (including being returned and/or deleted upon completion or termination of the contract) and **must** only be used for the purposes outlines in the contract • No service requiring access to official information, including security classified information, can be subcontracted without the approval of the agency • Address any legal rights that a third-party may have over the contractor that could allow access to the agency's information • Ensure the contractor notifies the agency if they discover or suspect that sensitive or security classified information has been, or will be, transferred overseas without approval from the agency in writing • Ensure information removal from data centres where ownership of contractor is transferred to a foreign entity • Contractors **must** notify the Office for Cyber Security for actual or suspected cyber threats or attacks as per the across government cyber security incident reporting scheme o **Office for Cyber Security** **Department of the Premier and Cabinet** E: watchdesk@sa.gov.au P: 1300 244 168
Personnel	• Contracted personnel **should** meet the requirements of SAPSF policy Recruiting employees, including identity, eligibility and suitability requirements

	• Security clearance requirements **must** be applied to contractors as the agency would to its employees. The agency is **responsible for** managing any security clearance throughout the term of the contract • Any contractors without the correct security clearances **must not** be given unescorted access to areas where security classified information is handled or stored or access/administrator rights to systems which hold or process security classified information • It is **recommended** to have all contractors sign confidentiality or non-disclosure agreements if they will be accessing official government information • The contractor **must** seek written approval from the agency to share the agency's information to any third parties • Provisions for revoking physical and ICT access when personnel from the contractor exit the company or role • Reminding departing personnel of their ongoing security obligations
Physical	• Physical security measures **must** be consistent with the requirements of the SAPSF for all sites or locations where South Australian or Australian Government • Contractors **must** be able to demonstrate they have the appropriate physical protections to protect information, or assets holding information (including ICT assets)

Managing and monitoring security risks and performance

14. Good contract management includes oversight and review to ensure adherence to all essential security requirements and enable new or changing security risks to be identified.
15. Agencies **must** monitor any contract for changes to the identified risks, threats, vulnerabilities or criticalities as well as the performance of the contractor in complying with the terms and conditions over the lifetime of the contract. Agencies **should** identify an appropriate contract manager to be responsible for managing and monitoring each contract.
16. If an agency's risks are subject to regular change (e.g. internal or external security environment changes), a flexible approach to contracts and their management **may** be required. As such it is **recommended** that agencies:
    a. develop positive working relationships with contractors based on open communication to help issues be resolved efficiently and effectively
    b. ensure contractors (including subcontractors) effectively communicate security risks to their employees and all relevant security terms and conditions of the contract that **must** be followed
    c. inspect any premises of the contractor (including subcontractors) prior to the contract commencing to verify that protective security measures have been applied to the standard required by the contract, and then reinspect periodically during the contract for any changes and overall compliance
    d. ensure all contractor personnel requirements have been achieved or obtained, such as:
        i. security clearances and clearance maintenance requirements
        b. legislative or policy requirements
        c. conflicts of interest
        d. confidentiality or non-disclosure agreements
    e. test and monitor (through site visits and audits) the contractor's processes for handling and storing the agency's information. Where required, seek access to vulnerability and risk assessments, business continuity plans and security threat advice that could affect the security of contract or information

Managing completion or termination of contracts

17. Security arrangements governing the completion or termination of contracts helps to prevent the compromise of official government information and damage to the agency. Agencies **must** put in place arrangements to securely manage the completion or termination of all contracts.

18. It is **recommended** that at the completion of a contract, agencies:

    a. recover all information (electronic and hard-copy) and assets under the control of the contractor (or ensure the contractor maintains all security measures if for legal reasons the information or assets cannot be returned)

    b. require the contractor to delete all agency information on the contractors ICT systems[4]

    c. ensure sponsorship of any security clearances is removed and the authorised vetting agency notified (see SAPSF policy Employee separation for more details)

    d. obtain formal acknowledgement from contractors and their employees of their continuing obligations to maintain confidentiality.

Document control

Approved by: Jim McDowell	Title: Chief Executive, Department of the Premier and Cabinet
Contact person: James Doherty	Telephone: 0447 180 915
Division: Security and Emergency Management, Intergovernmental and Diplomatic Relations	Date of approval: 20 April 2020
Revision number: 1.2	Date of review: 2 November 2020
Next review date: December 2021	

Change log

Version	Date	Changes
1.0	20/04/2020	First issue of policy
1.1	21/08/2020	Definition of 'personnel' updated
1.2	2/11/2020	Footnote 1 updated regarding the Procurement Policy Framework

[4] If security classified information (**PROTECTED** or above) was held, destruction **must** be as per the requirements of the South Australian Cyber Security Framework or the Commonwealth Information Security Manual