Australian Securities & Investments Commission

Protective Security Policy Framework Requirements:

Information Broker Access

What is the Commonwealth Protective Security Policy Framework?

The Protective Security Policy Framework (**the PSPF**) sets out the Australian Government's protective security policy and provides guidance to Australian Government bodies to support the effective implementation of the policy across the following four areas of security:

- Governance: to manage security risks and support a positive security culture
- Personnel: to ensure employees and contractors are suitable to access Government resources, and meet appropriate standards of integrity and honesty
- Information: to maintain confidentiality, integrity and availability of official information
- Physical: to provide a safe and secure physical environment for people; information and assets.

The PSPF consists of sixteen core requirements. Most core requirements have several supporting requirements that are designed to form a standard approach to implementing security across Government.

For more information see www.protectivesecurity.gov.au.

How does the PSPF apply to Information Brokers licensed by ASIC?

Information Brokers are licensed to access and distribute information and documents contained on ASIC's Registers under an agreement.

To maintain the security of the systems, processes and information held by ASIC, Information Brokers must comply with, and ensure that all subcontractors and personnel comply with, relevant PSPF core requirements. These core requirements are set out in the table below and are ASIC's minimum compliance standard. Information Brokers may choose to implement additional requirements.

PSPF Minimum Core Requirements

#	Policy Title	Core Requirement
Governance		
3.	Security planning and risk management	Must implement security arrangements to manage risks corresponding to the classification of material provided by ASIC (including personnel, information and physical security measures to protect the material and property at all times from unauthorised access, misuse, loss, interference, unauthorised modification and unauthorised disclosure)
4.	Security maturity monitoring	Should periodically review its security arrangements under the Agreement to ensure the arrangements are current and address the risks and security environments
6.	Security governance for contracted service providers	Is responsible for managing and monitoring protective security of its subcontractors
6.	Security governance for contracted service providers	Must ensure its contracted providers adhere to a professional code of conduct and these PSPF minimum core requirements
7.	Security governance for international sharing	Must, where you know or suspect that any Sensitive or Security Classified Information relating to the Agreement has been or is likely to be transferred overseas without approval in writing, promptly provide details to ASIC and follow reasonable directions from ASIC in relation to the matter
Information Security		
9.	Access to information	Must maintain confidentiality and not disclose official information to a third

		party, except for the purpose of providing clients with professional advice
9.	Access to information	Must require their personnel to protect ASIC's information and assets
9.	Access to information	Resources and information provided by ASIC, or generated because of the contract, belong to the government and are not used for any purpose other than the goods or services covered by the contract
9.	Access to information	Must ensure that no service that requires access to ASIC information be subsequently subcontracted to a different agreed provider, without written approval by ASIC
9.	Access to information	Must allow ASIC representatives to access your premises, records and equipment to monitor compliance with protective security conditions
10.	Safeguarding information from cyber threats	Must take reasonable steps to prevent, detect and respond to fraud and corruption

Personnel Security

13.	Ongoing assessment of personnel	Must report to ASIC when any personnel have had any incidental or accidental contact with Security Classified material
13.	Ongoing assessment of personnel	Must report to ASIC key changes in circumstances of personnel and the reporting and investigation of security incidents or breaches involving personnel. For example, you must notify ASIC if personnel:

		have been expelled from an accrediting body have been arrested or are undergoing disciplinary proceedings have been dismissed in circumstances of dishonesty or other security concerns.
13.	Ongoing assessment of personnel	Remind personnel who have accessed official information that the confidentiality requirements are ongoing
13.	Ongoing assessment of personnel	Must immediately notify ASIC of actual or suspected security incidents and follow direction from the ASIC in relation to incident investigations, including providing assistance to rectify the situation. Where entities jointly hold personal information (such as an entity and contracted provider), both entities have obligations to notify the Office of the Australian Information Commissioner and affected individuals in the event of an eligible data breach
Physical Security		
15.	Physical security for entity resources	Must ensure your premises and facilities used to handle, or store ASIC's information are protected to prevent unauthorised access to ICT assets and hard copy information
ASIC will:		
14.	Separating personnel	Revoke ICT access upon contracted provider's personnel leaving the provider
Mitigation of foreign interference risk includes:		

14.	Ongoing assessment of personnel	You must inform ASIC on any ownership changes (including of subsidiaries) or changes to ownership structure, operational management and day-to-day control and contracting arrangements for companies with access to the ASIC's data
1.	Role of accountable authority	ASIC maintains the right to cancel or amend the Agreement, remove servers and data or associated equipment, recover records (or maintain protective security measures if records cannot be returned) without penalty if there is a change in ownership or management
7.	Security governance for international sharing	Offshore control or access to ASIC's infrastructure, systems and data is prohibited