ASIC
Australian Securities & Investments Commission

Security policy

July 2024

About this policy

The policy describes ASIC's responsibilities for and approach to protecting the security of our people, information and assets.

Contents

A Policy objective **3**
Purpose 3
Scope 3

B Security governance **4**
Governing principles 4
Non-compliance 5

C Accountabilities and responsibilities **7**

D Security risk management **15**
Australian Government's Protective Security Policy Framework 15
Security governance processes 15
Quality assurance 16
Supply chain security 16
Information security 17
Cyber security and information technology 18
Personnel security 19
Physical security 21
Travel security and working remotely 22

Key terms **24**

Supporting resources **27**

Appendix 1 – ASIC Security Policy Framework **31**

A Policy objective

Purpose

1 This *Security Policy* aims to protect ASIC (**we**, **our**, **us**) and our people, information and assets from security threats, and ensure a fair, strong and efficient financial system for all Australians.

2 Having a proactive security culture provides the most effective protection against security threats. It is achieved by implementing physical, administrative and technical security treatments, and gaining their organisation-wide acceptance.

3 This policy acknowledges ASIC's role in maintaining national security through:

- occasionally sharing and receiving classified information from other Australian Government agencies
- regularly engaging with equivalent international agencies and groups and sharing information in accordance with Australian Government policies and advice.

4 This policy supports and aligns with:

- Accountable Authority Instructions
- the ASIC Code of Conduct
- the ASIC Risk Management Framework
- the Australian Government Department of Home Affairs (**DHA**) Protective Security Policy Framework (**PSPF**).
- the Australian Government Investigations Standards.

For more information, email protective.security@asic.gov.au.

Scope

5 This policy applies to current and former ASIC team members, including ASIC Commission members and contingent workers, collectively referred to in this policy as '**you**' or '**your**'.

6 Elements of this policy also apply to ASIC job candidates, and to contracted services providers who are part of ASIC's supply chain.

7 This policy establishes ASIC's approach to security for information-sharing arrangements with domestic and international partners.

B Security governance

8 For the purposes of this policy, ASIC Security comprises security governance, physical security, personnel security and information security, including those relating to information technology (IT) and cyber security.

9 At ASIC, we create, handle, store and transmit significant amounts of commercially sensitive information. Mishandling this information could adversely affect Australian businesses and the economy.

10 We are responsible for protecting classified information provided to us by other Australian Government agencies, handling it appropriately to avoid adverse outcomes for other agencies, the Australian Government and Australian residents.

11 We rely on information provided by other Australian Government agencies to undertake enforcement work and other activities. Security failures, or even perceived failures, may have an impact on those agencies' ability and/or willingness to share information with ASIC, affecting our regulatory mission.

Governing principles

12 We must take a risk-based and intelligence-led approach to security-related decision making.

13 Our security risk appetite is consistent with our operational risk appetite, as stated in ASIC's risk appetite statement.

14 Our protective security arrangements will be consistent with the Australian Government's PSPF.

15 Our information and cyber security arrangements will operate in accordance with the Australian Cyber Security Centre's (**ACSC's**) Cyber Security Principles.

16 We will determine the security environment – including threats, vulnerabilities and security risks – by undertaking a security risk assessment at least annually.

17 We will maintain a register of current security risks and the treatments we apply to reduce their likelihood and/or mitigate their impact.

18 We will develop the Protective Security Assurance Plan to ensure that security-related activities are performed to an acceptable standard and achieve the intended results.

19 We will use the quality assurance process to ensure continuous improvement in security practices and culture.

Security risk management

20 We will identify, analyse, assess and treat security threats, vulnerabilities and risks in accordance with:

- the *ASIC Risk Management Framework*
- ISO31000:2018 *Risk Management Principles and Guidelines*
- HB 167:2006 *Security Risk Management*
- the Australian Government's *Protective Security Policy Framework*
- the ASIO T4 Technical Design Notes 1-15, and
- the *Australian Government Information Security Manual* (ISM).

Supply chain security

21 To mitigate the effects of supply chain security risks, we will source goods, services and technology developed, manufactured and/or supplied by Australian providers, based in Australia, where possible.

22 Where Australian goods, services or technology providers are not available, we will consider international contingent workers and suppliers, based on advice from intelligence agencies and an assessment by the ASIC Protective Security team.

23 If the Protective Security team deems the security risks associated with engaging an overseas contingent worker or supplier are outside tolerance, the team may implement security controls. Where controls are not appropriate or feasible, it may be determined that the contingent worker or supplier presents an unacceptable security risk.

Non-compliance

24 Non-compliance with any aspect of this policy will be considered a security incident and managed in accordance with the ASIC Code of Conduct.

25 If a team member has three security incidents reported against them within a six-month period, they will be referred to their Executive Director for a disciplinary review.

26 Notifications of potential non-compliance with this policy should be submitted in the Notifiable Incidents, Threats and Reportable Observations (**NITRO**) Register.

27 We will investigate all security incidents and, where necessary, report the findings to the Agency Security Advisor **(ASA)**, the Chief Information Security Officer **(CISO)** or the Chief Security Officer (**CSO**).

28 Investigation outcomes related to holders of national security clearance will align with the DHA's Personnel Security Adjudicative Guidelines.

29 ASIC may be obliged to notify the Australian Government Security Vetting Agency (**AGSVA**) if it is determined that a policy breach or breaches are so frequent and/or of a magnitude that they affect your ongoing suitability to hold national security clearance.

30 It is mandatory that you have an active security clearance at a level commensurate with your role and responsibilities. Inability to maintain suitable active security clearance may affect your employment.

31 Non-compliance with this policy may result in security remediation activities.

32 Breaches or suspected breaches of law will be referred to the relevant authorities.

C Accountabilities and responsibilities

Accountability	Responsibilities
Accountable Authority	The accountable authority is the Chair of ASIC. The Chair is answerable to the portfolio minister for ASIC's security, and will: • determine our tolerance for security risks • manage our security risks • consider the implications of their own risk management decisions for other entities, sharing information on those risks where appropriate • approve the Annual Security Assessment Report to the DHA.
Chief Security Officer (CSO)	The CSO is a Chief Executive Officer. The CSO reports to the Accountable Authority and is responsible for ASIC's protective security planning and security posture. The CSO will: • be ASIC's Chief Executive Officer (CEO) • hold a security clearance of Negative Vetting Level 1 or higher • set the strategic direction for security within ASIC • coordinate communication between the Protective Security team and business functions • oversee the application of security practices and procedures, including the establishment, implementation, monitoring and review of security controls • investigate, respond to and report on security incidents • oversee ASIC's PSPF Annual Security Assessment Report to reflect our maturity position and detail how we are addressing areas of vulnerability • submit the Annual Security Assessment Report to the DHA via the PSPF portal • appoint suitably qualified security advisors in accordance with PSPF Policy 2: Management structures and responsibilities • issue security directions to ASIC team members and contingent workers, including directions on PSPF compliance from the Secretary of the DHA • use appointed security advisors to improve security awareness and capability through training and targeted communication, to better protect ASIC's people, information and assets.

Chief Information Security Officer (CISO)	The CISO leads ASIC's cyber security function. As an appointed security advisor under the PSPF, the CISO will: • hold a security clearance of Negative Vetting Level 1 or higher • set the direction and convey the vision for ASIC's cyber security strategy • be responsible for ASIC's cyber security policy, procedures and operations • provide strategic guidance and lead ASIC's cyber security program • provide cyber security and other security advice to; the CSO, the CRO, the ASA and other ASIC team members and executive forums • operate as ASIC's accreditation authority for ACSC's Infosec Registered Assessors Program (IRAP) • act as the accreditation authority to certify that systems comply with prescribed information security controls and guidelines, have been appropriately audited, have effective security controls and operate effectively, Cyber Authority to Operate (CATO) • manage ASIC's response to cyber-related crises, incidents and emergencies • contribute to the PSPF Annual Security Assessment Report on cyber components, to reflect ASIC's our security maturity position and detail how we are addressing areas of vulnerability
Security Governance Committee	Along with the Accountable Authority and the CSO, the Security Governance Committee will: • provide governance oversight of this policy, including any changes or updates • provide governance oversight of reporting mandated by this policy, including plans, policy breaches and quality assurance activities.
Executive Committee	The Executive Committee will provide governance oversight of any matters related to ASIC policy, including changes or updates escalated to it by the Security Governance Committee.
Chief Risk Officer (CRO)	The CRO is a security advisor under the PSPF and is authorised by the CSO to oversee and direct personnel and protective security. The CRO will: • report to the CSO • undertake Senior Executive Leader level liaison with AGSVA and other Australian Government agencies, as appropriate • perform other responsibilities delegated by the CSO.
Agency Security Advisor (ASA)	The ASA is the Senior Manager, Protective Security. The Senior Manager, Protective Security reports to the CRO. The ASA will:

	• provide protective security advice to ASIC and be responsible for administrative security matters • liaise with other government departments about briefings, clearance levels and other security matters • advise senior management on appropriate measures to ensure the security of team members, contingent workers, clients and information • monitor ASIC's security procedures and systems on an ongoing basis • be responsible for the development and operation of ASIC's Security Plan • help to prepare ASIC's PSPF Annual Security Assessment Report to accurately reflect ASIC's security maturity position and detail how we are addressing areas of vulnerability • be responsible for developing internal systems deemed appropriate by the DHA to undertake ASIC's own baseline security vetting of employees and contingent workers • take on other responsibilities delegated by the CSO.
ASIC Security teams	ASIC's Protective Security team, CRO, and Cyber Security, Digital Data & Technology Group (DD&T) teams will: • develop the biennial Security Plan in accordance with the PSPF, to foster continuous improvement in security culture and maturity • conduct security risk assessments to determine the security environment, including threats, vulnerabilities and security risks • communicate security-related intelligence to ASIC decision makers and team members, as appropriate • oversee security for contingent workers, suppliers and partners that form ASIC's supply chain, and implement controls to manage security risks. The Personnel Security team will vet and monitor the ongoing suitability of ASIC team members to hold national security clearance through the Continuous Organisational Suitability Assessment Program (COSA). The Protective Security team will administer the Annual Attestation for all ASIC team members and report the results to the ASIC Management Committee.
Security-sensitive position (SSP) holders	Some positions at ASIC are categorised as SSP by meeting one or more of the following criteria: • the position is the Accountable Authority or CSO • the position is the CISO • the position is a Security Advisor nominated by the CSO • has a Negative Vetting Level 2 security clearance or higher (as determined by the Personnel Security team) • the position has IT administrative privileges or data centre access • the CSO or CISO has determined a role to be SSP.

	SSP holders will: • maintain a valid national security clearance at a level commensurate with their role • undertake additional security training as required • participate in face-to-face security briefings • take part in a debrief as part of the cessation process.

People Leaders	ASIC's People Leaders include Commissioners, Regional Commissioners, Executive Directors, Senior Executive Leaders (SELs), Senior Managers, Managers and team leaders. They will:
	• ensure their own conduct and the conduct of their teams is in accordance with this policy at all times
	• ensure their teams take part in all mandatory security awareness training in a timely manner
	• report any information to the Personnel Security team that may affect a team member's suitability to hold national security clearance
	• ensure that positions that report to them are assessed to determine their correct national security clearance, and that this is monitored and reassessed if circumstances change
	• undertake any necessary activities to maintain a valid national security clearance
	• report all notifiable security incidents, security threats and security-related observations to the Protective Security team in a timely manner, using appropriate channels
	• review and countersign the Clearance Holder Cessation Declaration form completed by their team member:
	  ○ upon team members leaving ASIC because of resignation, redundancy or termination
	  ○ upon team members taking leave of a period greater than three consecutive months (including maternity and sick leave), or
	  ○ when contingent workers complete their contract term, or their contract has been terminated
	• ensure all relevant PeopleSoft HR requirements related to cessation are fulfilled prior to the end date.

Contract managers	A contract manager is an ASIC employee who has exercised their section 23(1) delegation under the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) or has received authorisation from a section 23 delegate to manage a contracted supply to ASIC (AAIs 3.2.19). Contract managers are identified in the PeopleSoft contract management system. They will: • ensure they follow their obligations under the PGPA Act (refer to 'Supporting Resources') • ensure they and their contingent workers always comply with this policy • ensure their teams take part in all mandatory security awareness training in a timely manner

	• report any information they believe may affect a contingent worker's suitability to hold national security clearance to the Personnel Security team
	• ensure the positions that report to them are assessed to determine the correct national security clearance, and to monitor and reassess if circumstances change
	• undertake any activities associated with maintaining a valid national security clearance
	• report all notifiable security incidents, security threats and security-related observations to the Protective Security team in a timely manner through the NITRO Register
	• review and countersign the Clearance Holder Cessation Declaration form completed by their team members and contingent workers:
	  ○ upon team members leaving ASIC because of resignation, redundancy or termination
	  ○ upon team members taking leave for longer than three consecutive months (including maternity and sick leave), or
	  ○ when contingent workers complete their contract term, or their contract has been terminated.
	• ensure PeopleSoft HR forms relating to cessation compliance are completed prior to a contingent worker's end date.

ASIC team members, including contingent workers	All ASIC team members will: • ensure their conduct always complies with this policy • access ASIC premises in accordance with the Access Management Protocol and take reasonable steps to ensure their own acts or omissions do not increase the risk of unauthorised access • correctly assess the sensitivity and/or security classification of the information they create • handle and transmit information in a way that is consistent with its sensitivity, security classification, associated legislation, the ASIC Code of Conduct and the ASIC Information Security Protocol • follow ASIC's 'clean desk principle' in the office and when working remotely • lock their device screens or shut them down when they are not in use in the office or when working remotely • take part in mandatory security awareness training or briefings, including refresher training • undertake any activities associated with maintaining a valid national security clearance (this applies to prospective candidates for ASIC roles) • complete and submit an Annual Attestation where a team member has full and current access to the ASIC IT network • assist the Protective Security team by providing information to support quality assurance measures, as part of the Quality Assurance Framework

	• report all notifiable security incidents, security threats and security-related observations to the Protective Security team in a timely manner and through appropriate channels
	• limit the personal use of ASIC assets, email addresses and credentials, in accordance with the Acceptable ICT use policy and External Communications policy, particularly when such use may introduce or increase security risks to themselves or ASIC
	• complete and submit the Clearance Holder Cessation Declaration form:
	  ○ upon team members leaving ASIC because of resignation, redundancy or termination
	  ○ upon team members taking leave for longer than three consecutive months (including maternity and sick leave), or
	  ○ when contingent workers complete their contract term, or their contract has been terminated.
	• ensure all relevant PeopleSoft HR cessation requirements are met prior to their end date.

Former ASIC team members	Former ASIC team members include former Commissioners, former employees (permanent, temporary and casual) and former contingent workers. They will continue to: • maintain the confidentiality and integrity of ASIC information, including sensitive and classified information, and knowledge of ASIC systems and methodologies • act in accordance with any relevant laws, regulations, determinations and agreements that apply to their former duties at ASIC • notify ASIC if they are in contact with foreign nationals, foreign intelligence officials or people suspected of being foreign intelligence officials, where the basis for such contact is, or appears to be, because of their former employment with ASIC • discharge their security clearance holder responsibilities if they have an active Australian Government security clearance. Former ASIC team members are bound by these obligations regardless of the reason they left ASIC, such as through resignation, redundancy, termination or the end of a statutory appointment.
Suppliers and service providers	Suppliers and service providers include any organisation or entity providing personnel, goods or services to ASIC. This includes organisations bound by contractual agreement with ASIC, other government entities, external consultants, external legal counsel engaged by ASIC, physical goods and services providers, and providers of intangible services such as software-as-a-service, cloud services and software. Suppliers and service providers will: • ensure their conduct complies with this policy always

	• ensure their employees and contingent workers undertake security awareness training as directed by ASIC, including refresher training
	• undertake any activities associated with maintaining a valid national security clearance as directed by ASIC and/or the AGSVA
	• ensure that the products and/or services they provide, and the way in which they provide them, does not result in ASIC being unable to meet its obligations under the PSPF
	• respond in a timely manner to reasonable requests to provide information for security purposes and to address security risks
	• notify ASIC of security incidents, or incidents that may have security implications that affect ASIC's people, information and/or assets
	• notify ASIC of significant changes within their organisation that may have an impact on services provided to ASIC or the way in which services are provided, or if the changes may enhance or add to security risks. These changes include, but are not limited to:
	  ○ changes to entity ownership
	  ○ a transition to (new) offshore headquarters
	  ○ changes to the way data and/or information are stored, including the location, and fail-over and retention arrangements
	• notify ASIC of any security incidents or breaches that involve a supplier or service provider, or its supply chain entities, that may directly or indirectly affect ASIC
	• take reasonable steps to manage supply chain security risks to ASIC
	• undertake any other actions in relation to new or emerging risks and issues as directed by the contract manager.

Business owners of IT systems or platforms	The business owners of IT systems or platforms are responsible for their operation and are normally SELs or Senior Managers. They will: • ensure they receive authority to operate a system or platform from the Cyber Security team before its onboarding • ensure all authorisation requirements for operating a system or platform are implemented prior to its use • ensure data stored within systems and platforms complies with this policy and ASIC's Data governance policy • where necessary, sponsor the appropriate Australian Government security clearances for any team members who may require ongoing or incidental access to the ASIC network, or to sensitive or security-classified information belonging to ASIC on a system or platform • ensure appropriate identifying methods and access control to a system or platform match the network's classification data • communicate with business users regarding any additional security requirements, including their impacts, restrictions and outages • engage in initial and ongoing management of agreements between ASIC and contracted parties, ensuring that security standards are maintained in accordance with the agreements or added as they become pertinent

	• report security breaches through the NITRO Register, including breaches of third parties that may affect the security of a system or platform • notify the Cyber Security team of any planned changes that may impact a systems or platform's authority to operate • consult with relevant parties to remediate security vulnerabilities in a system or platform • ensure information is protected at the end of a contractual period between ASIC and a system or platform provider.

Internal Audit	ASIC's Internal Audit team will:
	• maintain an audit schedule for regular auditing of security functions and components
	• implement line three controls to support ASIC's alignment with the PSPF
	• liaise with external entities in relation to audits of ASIC's security functions
	• report discrepancies or concerns that arise from any audit activities within ASIC to the ASIC Protective Security team, when such discrepancies or concerns may impact:
	  ○ the security of our people, information and/or assets
	  ○ any individual's suitability to hold a security clearance.

D Security risk management

Australian Government's Protective Security Policy Framework

33 The PSPF sets out the government's protective security policy and supports government entities such as ASIC to effectively implement the policy across the following outcomes:

- security governance
- physical security
- information security
- personnel security.

34 IT and cyber security arrangements are embedded in the PSPF and support all four of its outcomes.

35 Through our approach to security management, we will strive to comply with all requirements of the PSPF and align with the ACSC's Cyber Security Principles.

Security governance processes

36 As part of meeting ASIC's obligations under the PSPF, we will develop the biennial Security Plan, which will:

- establish ASIC's security goals and objectives
- establish how security risk management intersects and supports ASIC's broader business objectives and priorities
- identify threats, risks and vulnerabilities in relation to protecting our people, information and assets
- assess the maturity of our capability to manage security risks
- outline our strategies to implement security risk management, maintain a proactive risk culture and deliver against the PSPF.

37 The ASA (assisted by the CRO, CISO and Protective Security team) will be responsible for reporting ASIC's performance against the schedule of Security Assurance Activities.

38 As part of the Security Assurance Activities, ASIC will undertake an annual security maturity assessment, the results of which will be submitted to **DHA**.

39 Notwithstanding CSO approval, oversight and governance of this policy and the Security Plan is provided by the:

- Security Governance Committee
- ASIC Management Committee.

40 We will assess security risks using our enterprise risk methodology in addition to the business impact ratings recommended in PSPF Policy 8: Classification system.

Quality assurance

41 We will develop and maintain the Quality Assurance Framework, which will describe how to ensure:

- security treatments are working as intended
- team members are aware of and exercise their security obligations correctly
- People Leaders are aware of their obligations and exercise them correctly
- ASIC's physical, electronic and cyber security assets operate as designed
- ASIC's IT and technical security control measures work correctly and capture reliable and verifiable data.

42 The Protective Security team will report monthly, quarterly and annually against its quality assurance objectives to the relevant committees.

Supply chain security

43 We will maintain a Supply Chain Security Protocol to manage any risks associated with supply chain security, and to comply with the PSPF. This will include:

- processes for assessing supplier and contingent worker company ownership
- personnel security requirements for contingent workers and consultants
- management of the classification and dissemination of information to contingent workers and suppliers
- guidance on minimum requirements for security-related contract inclusions

- monitoring and assessing suppliers on an ongoing basis
- the provision of security-related training for contract managers.

44 Our contract managers, contingent workers, consultants and suppliers must comply with the protocol in all instances.

Information security

45 We will maintain an approach to information classification that is consistent with PSPF Policy 8: Classification system, including:

- classification levels up to the PROTECTED level
- caveats that apply to ASIC's remit.

46 The 'need-to-know principle' applies to all sensitive and security-classified information. It reflects the need for team members and contingent workers to access information only when there is a genuine requirement to do so to complete their work. This guards against the risk of unauthorised access or misuse of information.

47 Notwithstanding the need-to-know principle, all ASIC team members and contingent workers must apply the 'share everything you can principle'. The policy is designed to limit practical impediments to information sharing within the organisation but does not override a team member's or contingent worker's information security responsibilities.

48 Our IT network gateway is certified to accommodate information that has the correct security classification up to the PROTECTED level.

49 Only team members and contingent workers with a valid national security clearance (including authorised temporary access provisions) will be permitted access to ASIC's IT network.

50 OFFICIAL information (including sensitive and security classified information) should remain on ASIC's IT network where possible. It should only be transmitted outside the network when there is a genuine business need.

51 In instances where external transmittal is justified, before the transmitting of any information can occur, the ASIC team member transmitting the information must be satisfied that the:

- means of transmittal is appropriate for the sensitivity and/or security classification of the information
- intended external recipients have a genuine need to know the information and, where necessary, possess the appropriate

security clearance to receive sensitive and/or security classified information

- physical and/or digital storage arrangements for the information being transmitted meet the minimum requirements for sensitive and/or security classified information, both in transit and at the intended destination.

The use of automated processes and email features, such as rules for auto-forwarding emails to a non-ASIC email address, is not permitted.

52 Using your personal email account to receive and store OFFICIAL information is not permitted, unless the information being transmitted and stored contains your own personal information, such as performance reviews, remuneration information or training records.

53 Our Zone 2 premises will maintain provisions to:

- handle, store and destroy physical information up to the PROTECTED level, including digital storage media
- have discussions at the PROTECTED level
- have ad hoc discussions at the SECRET level.

54 We will maintain an Information Security Protocol that provides detailed directions regarding the handling of official and security classified information. This includes:

- requirements for correctly classifying, disseminating, storing and destroying physical and digital information, in accordance with the requirements of the PSPF and ASIC's Information records management policy
- establishing locations for audible dissemination of information (for example, in-person or virtual briefings, discussions and meetings) involving security classified information
- arrangements for disseminating classified information outside ASIC, including sharing classified information overseas
- arrangements for accepting, handling, storing and destroying information above the PROTECTED level.

55 Team members must always comply with the Information Security Protocol, including when working remotely.

Cyber security and information technology

56 We will maintain an internal Cyber Security Strategy, Standard, Policies, Protocols and Operating Procedures, which provide detailed

directions regarding ASIC's cyber security requirements. Together they cover:

- ASIC's cyber security governance measures
- ASIC's conformance with Australian government standards
- system and application protection measures
- threat detection, collection and analysis
- incident response measures, including for business continuity and disaster recovery
- system owner responsibilities
- network infrastructure security arrangements
- oversight and assessment of vendors and third-party vulnerabilities
- identity management, access control and passphrase management
- device security
- overseas device use risk mitigation
- internal and external reporting of cyber security incidents
- cyber supply chain risk management for ASIC's *fourth party* partners
- cyber literacy and learning materials available to all ASIC team members and contingent workers.

57 All ASIC team members are required to comply with the internal Cyber Security Standard, Policies, Protocols and Operating Procedures in all instances. Exceptions, exemptions or waivers are to be issued to the Cyber Security team for consideration.

58 We will periodically assess our systems, applications and infrastructure to ensure our security controls are working as intended.

Personnel security

59 Our personnel security team will ensure ASIC team members are eligible and suitable to have ongoing access to sensitive and security-classified information.

60 To meet minimum requirements, our team members and identified contingent workers must:

- undergo an ASIC suitability and baseline assessment, which includes a national police check

- hold a BASELINE national security clearance at a minimum
- complete an Annual Attestation administered by the Protective Security team, where the team member has full and current access to the ASIC IT network
- report any changes in circumstances to the Personnel Security team and/or AGSVA (depending on the issuer of their clearance)
- report any contact with a foreign national, a foreign intelligence official or someone suspected of being a foreign intelligence official to the Protective Security Team, via NITRO.
- complete the security clearance revalidation process within three months of their clearance expiring. If revalidation is not completed in this time frame, the team member's security clearance will be changed to 'inactive'.

61 We will maintain a Personnel Security Protocol to manage personnel security risks. This will include:

- minimum requirements for clearance holders, including citizenship and other prerequisites
- identifying the responsibilities of team members, People Leaders and recruitment managers
- the provision of personnel security awareness training
- reporting processes and criteria.

62 All ASIC team members will be required to comply with the Personnel Security Protocol in all instances.

63 We will facilitate an Insider Threat Program to address security risks associated with trusted insiders.

64 The Insider Threat Program will determine how ASIC prevents, detects and responds to threats posed by trusted insiders, noting that the sources and vectors for insider threats are likely to be subject to ongoing change.

65 The Insider Threat Program will include:

- allocation of responsibilities for addressing insider threat vectors
- descriptions of prevention, detection and response initiatives, and arrangements for managing insider threat vectors
- a framework covering the program, this Security policy, the ASIC Code of Conduct, the Continuous Organisational Suitability Assessment Program, the DHA's Adjudicative Guidelines and any other relevant processes, policies, procedures and guidelines.

66 Any reports about corruption and/or law enforcement misconduct provided to security teams will be sent to the Chief Legal Officer and/or CRO through approved mechanisms.

67 The Chief Legal Officer, in consultation with ASIC's CRO, is responsible for referring instances of alleged corruption to the National Anti-Corruption Commission (**NACC**).

Physical security

68 The security design of ASIC facilities will be in accordance with ASIO T4 Technical Notes 1–15.

69 Wherever possible, we will maintain:

- Zone 1 for all publicly accessible areas
- Zone 2 for all general office areas
- Zone 3 for all data centre areas
- Zone 4 for all areas where **SECRET** information and systems are handled and stored.

70 The CSO must approve deviations from security zoning after a security risk assessment.

71 We will maintain the Access Management Protocol for all ASIC sites, covering:

- issuing of ASIC ID passes and access privileges
- provisions for contingent worker and visitor access
- the role of the National Monitoring Centre (**NMC**) in permitting access privileges.

72 All ASIC team members will be required to comply with the Access Management Protocol in all instances.

73 Where appropriate, you will be issued with identification and a means of accessing ASIC premises. You are responsible for the security of these items and must contact the NMC as soon as practicable if they are lost, stolen or damaged. This must also be reported in NITRO.

74 All ASIC premises are secured by a network of digital surveillance cameras and an electronic access control system (**EACS**). The NMC constantly monitors the cameras and EACS. It uses these systems exclusively to:

- protect ASIC's people, information and assets
- ensure the safety and welfare of occupants

- ensure only authorised persons enter restricted areas of ASIC premises
- assist in the case of serious incidents or emergencies.

75 Data from ASIC's digital surveillance cameras and EACS is not stored on the ASIC IT network, and can be accessed only when:

- there is reasonable suspicion that a crime has been committed
- a security incident has occurred or is suspected of occurring and requires investigation.

The release of data from digital surveillance camera recordings and EACS records must be expressly approved by the CSO or ASA, where such data identifies individuals or makes individuals reasonably identifiable.

Travel security and working remotely

76 ASIC security teams will assist travel security advice for team members who travel domestically or overseas for ASIC business.

77 ASIC security teams will provide direction and advice to team members working remotely and their People Leaders to ensure security risks are identified and effective controls are implemented.

78 Working for ASIC from an overseas location is not permitted. The CSO or CISO may approve overseas work in exceptional circumstances, provided security risks can be properly managed.

79 ASIC-issued devices may not be taken overseas for the purposes of personal travel without the express permission of both an Executive Director and the ASIC Protective Security team. The ASIC Protective Security team and Cyber Security team will give directions for travelling overseas with secure devices.

80 ASIC team members are not permitted to use ASIC-issued devices to access virtual private networks (VPNs) that disguise network traffic coming from another country.

81 ASIC will maintain a Travel Security Protocol that provides direction for team members travelling within Australia and overseas. This protocol will cover:

- domestic travel for business and personal purposes
- international travel for business and personal purposes
- the notification and approval process for business and personal international travel

- any briefings required before international business travel
- the debriefing process after international travel.
- IT and device requirements
- contact reporting.

82 ASIC will maintain an Overseas Device Use Protocol which describes the minimum cyber security requirements and controls for the use of devices that provide access to ASIC's systems remotely.

83 All ASIC team members will be required to comply with the Travel Security Protocol and the Overseas Device Use Protocol when travelling domestically or internationally for ASIC business or personal purposes.

84 If a team member with an Australian Government security clearance at a Negative Vetting Level 2 and/or a compartment briefing undertakes personal travel against the Protective Security team's advice to a country identified by ASIO as being an extreme threat of foreign espionage, they will lose their compartment brief and/or undergo a review to determine if they will keep their Negative Vetting Level 2 security clearance.

Key terms

Term	Meaning in this document
Commission member	A person appointed by the Governor-General as the Chairperson, the Deputy Chairperson or a member of ASIC under sections 9(2) and 10 of the *Australian Securities and Investments Commission Act 2001* (ASIC Act).
Senior Executive	A Senior Executive Leader or Executive Director.
Accountable Authority	The most senior position within an Australian Government organisation, who is ultimately responsible for the activities of the organisation and its people.
ACSC	Australian Cyber Security Centre.
ACSC's Cyber Security Principles	The guiding principles supporting the Australian Government's *Information Security Manual*. These principles are produced by the ACSC.
AGSVA	Australian Government Security Vetting Agency, responsible for providing national security clearances to Australian Government agencies and other selected bodies.
Annual Security Assessment Report	A self-assessed report schedule completed by ASIC, assessing its compliance with the PSPF. The report is submitted by the Accountable Authority to the DHA annually.
ASIC	Australian Securities and Investments Commission – referred to in this policy as 'we', 'our' and 'us'.
Caveats	Additional markers applied to sensitive or classified information, stipulating how the information should be handled and who it can be shared with.
Classification	A grading provided to information based on the potential for its compromise to cause harm.
Contingent workers	Personnel who are contracted to ASIC for specific purposes under finite time periods (for example, for projects) and are provided with access to ASIC's IT network.
Contract manager	An ASIC employee who has exercised their section 23(1) delegation under the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) or has received authorisation from a section 23 delegate to manage a contracted supply to ASIC (AAIs 3.2.19). Contract managers are identified in the PeopleSoft contract management system.
DHA	Australian Government Department of Home Affairs.
Information security	The specific focus on the protection of information, whether physical, digital or verbal.
ISM	The Australian Government *Information Security Manual.*

Term	Meaning in this document
National Monitoring Centre	The NMC monitors all ASIC sites.
National security clearance	A status granted to individuals by the AGSVA or another vetting agency (including ASIC) that allows the individual to access classified information.
Network	In the context of this policy, this refers to ASIC's IT network.
NITRO	The Protective Security team's security incident register in myRAD. The Notifiable Incidents, Threats and Reportable Observations Register.
People Leaders	ASIC team members who have people management responsibilities.
Personnel security	The specific focus on personnel and their behaviours and activities.
Physical security	The specific focus on material security controls to protect people, assets and information. This includes, but is not limited to, security hardware, electronic security systems, guarding and security incident response.
Policy owner	The person responsible for drafting, arranging approval, implementing, communicating, training and reviewing this policy.
Protocols	Documents that provide specific and detailed information on how ASIC's *Security policy* obligations are implemented.
PSPF	The Australian Government's *Protective Security Policy Framework*.
Security breach	An incident in which an individual or group fails to operate in accordance with the *Security policy* or secondary directives or guidance.
Security risk	The likelihood of an adverse security outcome occurring as a product of a threat, vulnerability or criticality.
Security risk assessment	A process an organisation uses to determines its security risks, which may include threat analysis, criticality analysis, vulnerability analysis and risk assessment in accordance with HB167:2006 Security Risk Management.
Security threat actor	A group or individual that has the intent, capability and/or opportunity to adversely affect the security of an organisation.
Security vulnerability	A shortcoming in an organisation's defences that may be exposed by a threat actor.
Supply chain	A network of internal and external resources, including contingent workers, subcontractors, suppliers and secondary suppliers, that facilitates the operation of an organisation.

Term	Meaning in this document
Team members	ASIC employees (permanent, temporary and casual), contingent workers, Commissioners and appointees, including those: • employed by ASIC under s120(1) of the ASIC Act • engaged as a consultant under s121 of the ASIC Act • seconded under s122 of the ASIC Act • employed by ASIC under common law contract • appointed under a provision of the ASIC Act.
Treatments	Actions taken by an organisation to eliminate or reduce the likelihood or impact of a security risk.

Supporting resources

Supporting Policy Documents

ASIC Protective Security Framework

ASIC Security Plan 2023 – 25

ASIC Protective Security Assurance Plan

ASIC Internal Cyber Security Standard

ASIC Strategic Security Risk Assessment (restricted access)

Policies and protocols

Access Management Protocol

External Communications Policy

Information and Records Management Policy

Information Security Protocol

Travel Security Protocol

Overseas Device Use Protocol

Personnel Security Protocol

Protective Security Assurance Plan

ASIC Cyber Incident Response Plan

ASIC Cyber Security Protocol – Administration

ASIC Cyber Security Protocol – Platforms

ASIC Cyber Security Protocol – Equipment Sanitisation and Destruction

ASIC Procurement Policy

ASIC Vulnerability and Patch Management Policy

Standards and guidance

Australian Government Protective Security Policy Framework

Australian Government Essential Eight Mitigation Strategies

PSPF ISM and E8 Contextual Relationship Overview (2024)

ISO 31000:2018 Risk Management – Guidelines

Australian Government Information Security Manual

HB 167-2006 Security Risk Management Handbook

Document control

Policy ownership

The Chief Risk Officer is responsible for the development and implementation of this policy.

This policy is reviewed in accordance with ASIC's *Enterprise Policy Design and Review Handbook*.

Policy approval

Version	Approver	Approval date
V1	Chief Security Officer – Carlos Iglesias	August 2012
V2	Chief Security Officer – Carlos Iglesias	July 2013
V3	Chief Security Officer – Carlos Iglesias	November 2015
V4	Chief Security Officer – Carlos Iglesias Digital Information Security Council	July 2017
V5	Chief Security Officer – Carlos Iglesias Digital Information Security Council	6 December 2019
V6	Chief Security Officer – Carlos Iglesias Digital Information Security Council	13 July 2020
V7	Chief Security Officer – Warren Day Digital Information Security Sub-Committee	11 September 2020
V8	Chief Security Officer – Warren Day Digital Information Security Sub-Committee	27 July 2021
V9	Chief Security Officer – Warren Day Digital Information Security Sub-Committee	6 September 2021
V10	Chief Security Officer – Zlatka Hammer Digital Information Security Sub-Committee	20 February 2022

V11	Chief Security Officer – Zlatka Hammer Digital Information Security Sub-Committee	20 May 2022
V12	Chief Security Officer – Zlatka Hammer Digital Information Security Sub-Committee	8 December 2022
V13	Not recorded	
V14	Not recorded	
V15	Digital Information Security Sub-Committee	Out of session – July 2024

Version history

Version	Changes	Approval date
V1	Document introduced as 'ASIC's Security Policy Framework'	August 2012
V2	Changes to Infosec 4 and outsourcing/offshoring arrangements	July 2013
V3	Change FMA Act to PGPA Act & PSPF PERSEC	November 2015
V4	Update to reflect the Intelligent Risk Security Health Check 2016 and the Security Threat Risk Assessment 2017	July 2017
V5	Updated to compliment the 2018 PSPF reforms and to incorporate the updated Information, Personnel and Physical Security Policies	6 December 2019
V6	Updated to incorporate section K – Working remotely, pandemics and other extended events	13 July 2020
V7	Minor update to include information caveats and Share Everything You Can obligations	11 September 2020
V8	Review of structure and policy obligations including the Policy principles, PSPF compliance and adherence to ISM and ACSC's Cyber Security principles.	27 July 2021
V9	Minor updates to standardise terminology between the policy and IT Security protocols	6 September 2021
V10	Minor updates to align with restructure in Cyber Security team	20 February 2022
V11	Updates to include Security Sensitive Position Holders, Responsibilities for Contractors and Suppliers and Insider Management Protocol	20 May 2022
V12	Reformatting in accordance with the Enterprise Policy Handbook and inclusion	8 December 2022
V13	Inclusion of additional information security restrictions s59-61.	12 April 2023

V14	Minor Update - Inclusions of Business Owners of IT systems/platforms in Part C	29 May 2023
V15	Updates to include changes to the PSPF Policy 8: Classification System, adjustments to meet organisational restructure, update hyperlinks, removal of the term contractor and updated cessation obligations.	July 2024

Distribution

Version	Distribution list	Effective Date
V1	Not recorded	August 2012
V2	SharePoint	July 2013
V3	MyASIC	November 2015
V4	MyASIC	July 2017
V5	MyASIC	March 2020
V6	MyASIC	July 2020
V7	SharePoint	September 2020
V8	SharePoint	August 2021
V9	SharePoint	September 2021
V10	SharePoint	February 2022
V11	SharePoint	May 2022
V12	SharePoint	8 December 2022
V13	SharePoint	19 April 2023
V14	SharePoint	19 May 2023
V15	SharePoint	

Appendix 1 – ASIC Security Policy Framework

<table>
<tr><th colspan="5">Oversight and Governance</th></tr>
<tr><th>Legislation</th><th colspan="3">Australian National Audit Office | Dept. Home Affairs | Government Security Committee</th><th>ASIC Policies and Procedures</th></tr>
<tr><td rowspan="6">Australian Securities and Investments Commission Act
Commonwealth Procurement Rules
Crimes Act
Criminal Code Act
National Anti-Corruption Commission Act
National Security Information (Criminal and Civil Proceedings) Act
Public Governance, Performance and Accountability Act
Security of Critical Infrastructure Act</td><td colspan="3">Australian Government Protective Security Policy Framework</td><td rowspan="6">Acceptable ICT Use Policy
Accountable Authority Instructions
Business System Owner Roles and Responsibilities
Code of Conduct
Change of Circumstances Notification
Data Governance Policy
Employee Security Guidelines
Fraud and Anti-Corruption Policy
Information Security Protocol
Mobile Device Security Protocol
Printing Policy
Security Policy
Travel Security Protocol</td></tr>
<tr><td colspan="3">ASIO Technical Notes 1-15 | Security Construction and Equipment Committee Evaluated Product List | Australian Government Information Security Manual</td></tr>
<tr><td colspan="3">Accountable Authority
Chief Security Officer
Executive Risk Committee
Integrity Sub-Committee
Data and Information Security Sub-Committee
The Protective Security Plan</td></tr>
<tr><td>Prevention</td><td>Detection</td><td>Response</td></tr>
<tr><td>Recruitment & Interview
ASIC Suitability
Security Clearance
Education & Awareness
Integrity Risk Assessments
Ongoing suitability
Security Zones</td><td>Change in Circumstances
Compliance Incident Management System
Electronic Access Control System
Internal Audits
Law Enforcement Referrals
Notifiable Incidents, Threats & Reportable Observations
Ongoing disclosure obligations
PGPA Act breaches
Public Interest Disclosures
Security Assurance Program
Sentinel / Security Event and Incident Management
Speak Up</td><td>Code of Conduct investigation
Continuous improvement
Disciplinary action
Law Enforcement referral
National Anti-Corruption Commission referral
Remedial action procedures
Review for Cause (security clearance)
Security breach investigation</td></tr>
<tr><td colspan="5">Culture of Security Maturity</td></tr>
<tr><td>Culture Surveys</td><td>Internal Security Maturity Reporting</td><td>Mandatory and Targeted Training</td><td>PSPF Security Maturity Report</td><td>Speak Up</td></tr>
<tr><td colspan="2">Security Threat and Risk Assessments</td><td colspan="3">Assurance and Controls</td></tr>
<tr><td colspan="2">Identifies critical assets and information
Identifies risks, threats and vulnerability gaps
Evaluates security capability and associated controls</td><td colspan="3">Annual Attestation
Embedded control activities
Regular control monitoring and testing program</td></tr>
</table>