



SECURITY CLEARANCE POLICY

Document information

Date approved/effective: XX Month 2024

Date last reviewed: 18 April 2017

Approved by: XXXX

Policy Custodian: Security and Emergency Management Division, Justice and

 Community Safety Directorate

Review date: Month 2026

CONTENTS

[1. Definition of Terms 3](#_Toc177308923)

[2. purpose 3](#_Toc177308924)

[3. Scope 3](#_Toc177308926)

[4. Background 4](#_Toc177308936)

[5. Roles and responsibilities 4](#_Toc177308937)

[6. purpose of a security clearance 5](#_Toc177308938)

[7. When IS a security clearance required 5](#_Toc177308945)

[8. RecruitMENT 7](#_Toc177308946)

[9. security clearance vetting process 8](#_Toc177308948)

[10. PROCESS for obtaining a security clearance 9](#_Toc177308949)

[11. TEMPORARY access 10](#_Toc177308950)

[12. RETENTION OF EXISTING security clearances 12](#_Toc177308951)

[13. maintaining A SECURITY CLEARANCE 12](#_Toc177308953)

[14. LOSS of Security Clearance 13](#_Toc177308955)

[15. breachES 14](#_Toc177308958)

[16. PERSONNEL SEPARATION FROM ROLE 14](#_Toc177308959)

[17. Enquiries 15](#_Toc177308962)

© Australian Capital Territory 2024

This work, the Security Clearance Policy is licensed under a [Creative Commons Attribution 4.0 licence](http://creativecommons.org/licenses/by/4.0).
You are free to re‑use the work under that licence, on the condition that you credit the Australian Capital Territory Government as author.

The licence does not apply to the ACT Government logo.

# Definition of Terms

| **Term** | **Definition**  |
| --- | --- |
| Identified Position | Position or group of positions that have been identified as requiring a security clearance.  |
| Security Classified information | Information that is classified at or above PROTECTED level, according to the Australian Government Protective Security Policy Framework (PSPF). |
| Security Clearance Register | Register of positions requiring a security clearance in a directorate and the personnel in those positions, to be maintained by the directorate.  |
| Security vetting | The term used for an assessment of a person’s suitability to hold a security clearance by an authorised vetting agency. The vetting process can deliver a level of assurance about the credentials and integrity of the directorate or agency’s workforce. |

# purpose

* 1. Under the [*ACT Government Protective Security Framework*](https://actgovernment.sharepoint.com/sites/extranet-JACSSEMD/Document%20Library/Forms/AllItems.aspx?id=%2Fsites%2Fextranet%2DJACSSEMD%2FDocument%20Library%2FProtective%20Security%2FACT%20Protective%20Security%20Framework%2FInformation%20Paper%20%2D%20ACT%20Protective%20Security%20Framework%2Epdf&parent=%2Fsites%2Fextranet%2DJACSSEMD%2FDocument%20Library%2FProtective%20Security%2FACT%20Protective%20Security%20Framework) (ACT PSF), the ACT Public Sector (ACTPS) must implement policies and procedures to protect people, information and assets, and manage protective security in a consistent manner.
	2. This policysets the requirements for the management of personnel security risks through a security clearance process for public employees working in or with the ACT Government.

# Scope

* 1. These guidelines have been developed for whole-of-government use and are issued by the Head of Service under section 17(2)(a) of the *Public Sector Management Act 1994* (PSM Act). The guidelines bind all staff engaged under the PSM Act and all public sector employers within the meaning of section 152(1)(a) of the PSM Act. 11.
	2. These guidelines are intended to have a broad application and apply to any person who is part of the ACTPS. To remove doubt, these guidelines apply to all public employees as defined in the *Legislation Act 2001*.
	3. For the purpose of these guidelines, public employee(s) means an officer, temporary employee, casual employee, public sector member, senior executive member, board and committee members, person employed under the [*Legislative Assembly (Members' Staff) Act 1989*](https://www.legislation.act.gov.au/a/1989-19/) (ACT), and contractors or consultants exercising a function of a public sector entity.

# Background

* 1. Personnel security is a key line of defence in good protective security management.
	2. Some positions in the ACTPS involve the handling of sensitive information or management of high value assets. Security clearances are often used for positions that require additional vetting to ensure sound character, integrity, reliability and that the person is not vulnerable to improper influence.
	3. The PSM Act allows the Head of Service to require that a person must hold a security clearance to be eligible for certain offices in the ACTPS.
	4. The ACTPS security clearance process is aligned to the [*Commonwealth Protective Security Policy Framework*](https://www.protectivesecurity.gov.au/). Security clearances are managed through the Australian Government Security Vetting Agency (AGSVA).

# Roles and responsibilities

| **Role** | **Responsibilities** |
| --- | --- |
| Agency Security Executive (ASE) | The Senior Executive Service (SES) level officer under the ACT PSF to oversee directorate security arrangements. If there is no ASA within a directorate or agency, the ASE may need to take on the tasks of the ASA set out in this policy. |
| Agency Security Advisor (ASA) | Officer appointed by the ASE to support the day-to-day implementation and management of directorate security arrangements.Some agencies may have an equivalent role that undertakes this work, but has a different name.  |
| Australian Government Security Vetting Agency (AGSVA)  | The central vetting agency for the Australian Government, and the agency that conducts security vetting for the ACTPS.  |
| Security and Emergency Management Division (SEMD) | Leads, advises, assists, and coordinates the government’s security and emergency management arrangements to strengthen resilience, drive collaboration, and develop strategies and policy settings that enhance community wellbeing.Manages the engagement with AGSVA and is responsible for coordinating the application, renewal, and maintenance of security clearances for public employees at all levels of the ACTPS. |

# purpose of a security clearance

* 1. The ACT PSF highlights the potential threat that can come from ‘trusted insiders’ insiders acting maliciously or under coercion, or through inadvertent actions. Additional vetting through a security clearance assist to address the risk from trusted insiders acting maliciously or under coercion.
		1. Trusted insiders are people who have privileged access to information and assets, and because of that access may be able to compromise security.
	2. The security vetting process considers the integrity of a person such as their honesty, trustworthiness, maturity, tolerance, resilience, and loyalty to Australia. It also seeks to determine that the person is not unduly vulnerable to influence or coercion.
	3. A security clearance affords access to certain levels of security classified information as set out below. It does not automatically give access to security classified information, as access is always determined on a ‘need to know’ basis in consultation with the author.

|  |  |
| --- | --- |
| **Clearance level** | **Security classified information level** |
| BASELINE | PROTECTED |
| NEGATIVE VETTING 1 | SECRET |
| NEGATIVE VETTING 2 | TOP SECRET |

# The Requirement for a security clearance

* 1. Security clearances are required for high risk positions, such as those with privileged access to finances and accounts, information and/or high value assets. A security clearance must be maintained for the duration of employment in a high risk position.
	2. The *Security Clearance Eligibility and Risk Assessment Tool* allows users to determine whether a security clearance is required for a position or group of positions, and determine the appropriate level of clearance.
		1. Directorates and agencies may also need to develop their own processes to identify high risk positions according to their operations.

**HIGH RISK POSITIONS**

**A lot of**

Trust

**A lot of**

Money

Data

Assets

## Positions of Trust and Designated Security Assessed Positions

* 1. There are two types of security clearance requirements for positions in the ACTPS.
		1. **Position of Trust (PoT):** Public employees may be required to hold a security clearance if they occupy a position of trust that requires additional assurance. This is the most common type of security clearance requirement.
		2. **Designated security assessed position (DSAP):** Public employees who need access to security classified resources must hold a security clearance. This includes classified information, systems that hold classified information, and classified assets.
	2. Public employees in a PoT will typically require a Baseline clearance. Public employees in a DSAP must obtain a minimum Baseline clearance, or Negative Vetting Level 1 (NV1) depending on the requirements of the role.
	3. DSAPs should be kept to a minimum and are generally restricted to those positions set out below.

**Designated Security Assessed Position**

Positions identified as DSAP:

* Directors-General and Deputy Directors-General
* Security and Emergency Management Committee of Cabinet ACTPS members
* Security and Emergency Management Senior Officials Group members
* JACS Security and Emergency Management Division permanent employees
* ASEs and ASAs
* Staff who regularly access highly sensitive or classified material

**Position of Trust**

Duties require the directorate to have a higher level of assurance about the integrity of the occupant because of the responsibilities, such as:

* Regular access to multiple sensitive documents like tender documents or business cases, or regular access to aggregated sensitive information
* Responsibility for large sums of money

## Assessing A POSITION FOR A SECURITY CLEARANCE

* 1. Directorates are responsible for determining whether a position requires a security clearance, and for identifying public employees who need to apply for a clearance.
	2. All new positions must be assessed to identify whether a security clearance is required, and whenever the responsibilities or functions of a position are reviewed or updated.
	3. Where a position or group of positions is identified as high risk and requiring a security clearance, the *Security Clearance Eligibility and Risk Assessment Tool* should be used to identify the relevant risks and provide a clear justification the security clearance requirement. A copy of the completed assessment for a position should be provided to JACS SEMD on request to confirm appropriate eligibility.
	4. Directorates must develop and maintain a Security Clearance Register of all positions that require a security clearance in accordance with the *Information Privacy Act 2004* and *Territory Privacy Principles*. The Register should include information useful for the directorate, but must include:
		+ If the position is a PoT or DSAP
		+ Position title and number
		+ Full name, date of birth and AGS number of the position holder
		+ Date clearance granted (or status), level of clearance, and revalidation date of clearance
		+ Contract commencement and end date for contractors.
	5. A copy of the Security Clearance Register should be provided to JACS SEMD each year at securityclearances@act.gov.au.
	6. It is recommended that directorates review positions requiring a security clearance every two years, to determine whether the responsibilities of the position still require the occupant to hold a security clearance.
		1. Directorates must implement procedures for the downgrading or cessation of security clearance requirements, including advising JACS SEMD of the change in position eligibility requirement.

# RecruitMENT

* 1. When recruiting to positions identified as requiring a security clearance, directorates and agencies will need to ensure any recruitment documentation, position descriptions, position advertisements or letters of offer clearly inform applicants that a security clearance from AGSVA is required to be obtained and maintained.
		1. The position advertisement should include a link to the AGSVA website, to allow potential applicants to make an informed decision about whether to apply for the position, and what information they will be required to submit to AGSVA when completing their security clearance application.
	2. Unless the advertisement clearly specifies applicants must hold a current security clearance, directorates must not discriminate against applicants who do not hold a security clearance where the applicant indicates a willingness to apply and is eligible to apply for a security clearance.
	3. If an applicant is offered a position but does not have the required security clearance, directorates may choose to wait for the clearance to be granted before the successful applicant commences.
	4. If the directorate chooses to accept the risk of having the successful applicant commence while the clearance process is being undertaken:
		1. arrangements must be made to limit access to sensitive information, or provisional access sought for the public employee (see Section 11).
		2. a process must be in place to manage the situation should the clearance not be granted (for example the recruitment is provisional pending clearance or the directorate agrees to place the applicant in an alternative role)
		3. the prospective public employee must be advised of and understand the implications should the clearance not be granted

# security clearance vetting process

* 1. Some vetting procedures are invasive for the public employee, their family and friends. Additionally, it must be recognised that holding a security clearance is not a one-off occurrence but an ongoing commitment between the person, the ACTPS, and the Commonwealth.

## Citizenship and BACKGROUND Requirements

* + 1. To be eligible for a security clearance through AGSVA, an individual must be an Australian citizen and have a checkable background.
		2. It is possible to seek a citizenship or checkable background waiver in limited circumstances. The Director-General (or agency equivalent) for the relevant directorate may waive the requirements if there is an exceptional business need, which may include the following:
	+ the person is necessary to the agency meeting a critical objective
	+ the role cannot be redesigned so that access to classified information or resources is restricted to existing public employees with the appropriate clearance
	+ the role cannot be performed by an Australian citizen, and there is no conflict of interest in relation to the person’s country of allegiance and the role being undertaken, and
	+ the foreign national is a permanent resident, is actively seeking citizenship and the process will be concluded in a reasonable period.
		1. To obtain the waiver:
	+ The relevant manager and ASA must specifically assess the risk for the position and gather evidence of that assessment to support the waiver
	+ JACS SEMD will seek advice from AGSVA on whether there are immediate concerns about granting a waiver for the person
	+ JACS SEMD will liaise with the ASA to obtain approval for the waiver from the relevant Director-General (or agency equivalent).
		1. If granted, the citizenship or background waiver is only granted for a specific position for a specified period not exceeding 12-months. As such, if a public employee granted a citizenship or background waiver seeks to transfer to a new position the process must be undertaken again for the new position.
	+ AGSVA conducts annual appraisals for citizenship or background waivers to ensure ongoing suitability for the waiver.

# PROCESS for obtaining a security clearance

* 1. If an applicant has been offered a position requiring a security clearance and already holds the appropriate level of security clearance, there is only a need for the public employee to advise AGSVA of their change in circumstances, and for the directorate to update directorate records and complete the *Security Clearance Request and Transfer Form* to JACS SEMD. JACS SEMD will also ensure AGSVA is advised that the ACTPS is the new sponsor for the security clearance.
	2. Where a successful applicant does not hold the required security clearance, directorates must contact JACS SEMD to initiate the security clearance process for the public employee. AGSVA will not deal directly with ACTPS directorates or agencies.
	3. Directorates (usually the direct manager) must complete the *Security Clearance Request and Transfer Form* to support the request for a security clearance, which must be approved by the relevant ASA, and provided through to JACS SEMD.
		1. Requests for a new or existing Negative Vetting 2 (NV2) clearance must be endorsed by the relevant Director-General (or agency equivalent). For Directors-General (or agency equivalents) requiring an NV2 clearance, endorsement of the Director-General, JACS is required.
		2. Positive Vetting (PV) security clearances are not typically required in the ACTPS. PV clearances are granted at the discretion of the Head of Service on advice from a Director-General (or agency equivalent) and must be supported by a business case and risk assessment. Evidence of prior agreement for co-sponsorship of the PV security clearance by a Commonwealth agency must also be provided to the Head of Service in accordance with the [Commonwealth PSPF Policy 12](https://www.protectivesecurity.gov.au/publications-library/policy-12-eligibility-and-suitability-personnel).
	4. Once JACS SEMD has processed a security clearance request, AGSVA will issue the public employee with a myClearance pack for completion. Instructions and timeframes will be provided by AGSVA.
	5. After a myClearance pack has been completed, the security vetting process can take some time and varies depending on the security clearance level – advice on estimated timeframes is available on the [AGSVA site](https://www.defence.gov.au/security/clearances/about/vetting-time-frames).

## costs

* + 1. Directorates/agencies are responsible for meeting the costs of security clearances and ongoing maintenance for their employees.
		2. JACS SEMD administers and processes payments to AGSVA, and will recover the cost of a security clearance from the relevant directorate.

# TEMPORARY access

* 1. Where there is a critical need for a public employee to access classified or highly sensitive information and they do not hold the required level of security clearance, it is possible to apply for either Short Term Access or Provisional Access.
	2. Temporary access allows limited and supervised access to classified information
		1. Access must be directly supervised in-person by a public employee with the appropriate level of security clearance for the documents being accessed.
		2. If the classified information originates outside the ACTPS, the authoring agency for the information must be consulted and agree to the granting of temporary access to that information. Authoring agencies are not obligated to grant this access.
	3. Temporary access cannot be sought for ongoing access to classified information, for routine business needs, or to circumvent security clearance application processes.

## Short Term Access

* + 1. Short Term Access allows access to classified information for no more than three (3) months for a public employee who does not hold the required security clearance, and is generally used to allow access to classified information while an AGSVA MyClearance pack is completed.
	+ Short term access is generally granted for PROTECTED information.
	+ Any requirement for short term access to:
	+ SECRET information requires the public employee to first hold a BASELINE security clearance, or
	+ TOP SECRET information requires the candidate to first hold a current NV1 security clearance.

## Provisional Access

* + 1. Provisional Access allows ongoing access by an public employee to classified information after they have submitted their AGSVA myClearance pack while the vetting process is underway, and can only be granted up to SECRET.
		2. To gain Provisional Access, the application status must be at ‘In Analysis’ which can be confirmed by JACS SEMD (securityclearances@act.gov.au).

## Applying for temporary access

* + 1. For temporary access up to SECRET, the applicant’s manager must complete the *Request for Temporary Access to Security Classified Resources.* The request must identify exceptional circumstances, identify and assess risks of granting the temporary access (including those to other affected agencies), and determine effective risk mitigation strategies.
		2. The *Request for Temporary Access to Security Classified Resources* must be endorsed by the relevant ASA and sent to JACS SEMD (securityclearances@act.gov.au).
		3. For temporary access up to TOP SECRET, the public employee must already hold a current NV1 clearance, and the business case must also be endorsed by the relevant Director-General (or agency equivalent).
		4. JACS SEMD will consult with AGSVA on the application and provide advice on the risk of granting temporary access to the JACS SEMD Executive Group Manager (EGM).
		5. After considering the risk of granting temporary access and advice from AGSVA and JACS SEMD, the JACS SEMD EGM will make a decision to grant or decline temporary access.
			1. If temporary access is approved, the public employee must sign a *Declaration of Secrecy – Temporary Access* and provide a copy to the relevant ASA and JACS SEMD (securityclearances@act.gov.au).
			2. If temporary access is not approved, JACS SEMD will advise the relevant ASA.
		6. If additional risks are identified, or if previously identified risks can no longer be effectively mitigated, the requesting officer must advise JACS SEMD at the first opportunity.
		7. Temporary access should be recorded in the relevant Security Clearance Register.

# RETENTION OF EXISTING security clearances

* 1. Public employees in positions that do not require a security clearance will not be supported to maintain their security clearance sponsorship. When a security clearance is not sponsored, it is made inactive until the public employee is in a position with a security clearance requirement.
	2. Where a public employee has an existing security clearance that is higher than the level required for the position, the ACTPS will only sponsor the security clearance level required for the position.
	3. Security clearances that are inactive, or sponsored at a lower level, can be reactivated by AGSVA for a period from when the original clearance was granted. This is different for each security clearance level. AGSVA will advise if a security clearance can be reactivated or if a new application is required.

# maintaining A SECURITY CLEARANCE

* 1. Security clearances are valid for extended periods, and invariably the circumstances of security clearances holders changes over that time.
	2. Directorates must have arrangements in place to ensure all security clearance holders are aware of their responsibilities to report specified changes of personal circumstances (at the time of the change) to AGSVA.
	3. Security clearance holders are also required to report changes in circumstances to their ASA if they are likely to impact on employment suitability.
	4. Security clearance holders are able to report changes directly to AGSVA through the [myClearance portal](https://www.defence.gov.au/security/clearances/applicants-holders/reporting-changes-in-circumstances). Changes that should be reported include:
* change of name or identity;
* entering into or ceasing a significant relationship;
* overseas travel;
* residence in foreign countries;
* relatives residing in foreign countries;
* changes in citizenship or nationality;
* non-routine communication with foreign government officials;
* significant changes in financial circumstances;
* changes in health or medical circumstances;
* involvement in criminal activity;
* change of employment status; and
* security incidents.
	1. Under the ACT PSF (Personnel Security), annual performance development processes provide an opportunity for supervisors to assess and report any changes in behaviour and ensure public employees report changes in personal circumstances and potential conflicts of interest.
	2. Directorates must have processes in place to advise JACS SEMD of adverse changes in personality or suspicious behaviour displayed by public employees holding a security clearance in accordance with AGSVA obligations.
	3. For further guidance, contact JACS SEMD (securityclearances@act.gov.au) or refer to the [AGSVA website](https://www.defence.gov.au/security/clearances).

## security AWARENESS TRAINING

* + 1. Under the ACT PSF, there is a requirement for annual security awareness training to be completed by public employees that hold a security clearance in accordance with AGSVA obligations.
		2. Security awareness training should be relevant to the directorate/agency, consider the impact on existing business practices or systems and appropriate to the target audience and consider the roles, responsibilities and need-to-know in relation to sensitive issues.

## revalidation of security clearances

* + 1. A security clearance revalidation is a periodic review conducted by AGSVA to ensure that public employees are still suitable to hold a security clearance at the granted level.
		2. Clearance holders and JACS SEMD will be notified by email when a periodic revalidation is due, and a new clearance application will be issued.
		3. A security clearance will be cancelled if a clearance holder does not complete a revalidation.

# LOSS of Security Clearance

* 1. In the event of a refused, cancelled or surrendered security clearance, directorates will assess the duty statement of the position with a view to taking the following actions:
		1. for conditional arrangements – a decision that no change is required as the extent of the registration allows current duties to continue;
		2. a change in duty statement, or functions so that the public employee is no longer in a position requiring a security clearance;
		3. a transfer, either internally or to another directorate, to a position that does not require a security clearance;
		4. for a temporary employee or an officer on probation – end the employment;
		5. for a confirmed officer – redeployment under s 122 of the PSM Act;
		6. where a suitable position is not found or accepted by the confirmed officer, action to retire the officer on the basis that the person is no longer qualified to perform their duties under s 123 of the PSM Act; or
		7. a suspension with or without pay in accordance with s 32(2) of the PSM Standards, while the preceding actions are taken.
	2. Section 32(2) of the PSM Standards provides for periods of suspension from employment with or without pay until:
		1. where a security clearance has been cancelled by AGSVA– the date of effect; or
		2. the employee is transferred under ss 122 or 123 of the PSM Act.
	3. For more information, please see the [*Redeployment – Loss of Eligibility Policy*](https://www.cmtedd.act.gov.au/__data/assets/pdf_file/0003/1738416/Loss-of-Eligiblity-Redeployment-Policy-Final.pdf)*.*

# breachES

## VIOLATIONS of security clearance conditions

* + 1. AGSVA sets out obligations on security clearance holders on its [website](https://www.defence.gov.au/security/clearances/applicants-holders/maintaining-your-clearance#revalidations), and provides these to individuals on the granting of a clearance. The consequences to a security clearance of a breach of these obligations will be determined solely by AGSVA.
		2. Violations of security clearance conditions must be reported to JACS SEMD and AGSVA as a change in circumstances.

## Security Breaches

* + 1. Any breach of security, whether deliberate or accidental, can compromise integrity, and incidents involving public employees or contractors are particularly serious if the person occupies a PoT or DSAP.
		2. Directorates should have in place processes for reporting and managing security breaches, and these should be easily accessible to all public employees. These processes should include a requirement to advise JACS SEMD of incidents involving security clearance holders.

# PERSONNEL SEPARATION FROM ROLE

* 1. Directorates and agencies must inform JACS SEMD by email ([securityclearances@act.gov.au](file:///C%3A%5CUsers%5Cluke%20janeczko%5CAppData%5CLocal%5CMicrosoft%5CWindows%5CINetCache%5CContent.Outlook%5CKGAHOY4P%5Csecurityclearances%40act.gov.au)) when public employees leave a position requiring a security clearance, regardless of the reason for their departure, and regardless of whether the person is moving into a different position that also requires a security clearance.
	2. JACS SEMD will liaise with AGSVA for appropriate action to be taken. Where a person ceases to be employed in the ACTPS, the sponsorship of their security clearance will cease.
	3. Public employees must complete a *Declaration of Secrecy – Cessation of Duties* prior to departing a position requiring a security clearance. A copy of the signed form should be provided to JACS SEMD and the relevant ASA.
	4. ASAs must also undertake exit interviews with security clearance holders to identify any potential security concerns and to provide information on ongoing obligations.

# Enquiries

* 1. Enquiries about this policy can be directed to JACS SEMD via JACSSEMD@act.gov.au

##  Other Types of VETTING

* + 1. CMTEDD has an internal Personnel Vetting Program for some CMTEDD personnel that is similar to the AGSVA security vetting process but does not allow access to classified information.
		- Questions about this process should be directed to [PersonnelVetting@act.gov.au](file:///C%3A%5CUsers%5Cluke%20janeczko%5CAppData%5CLocal%5CMicrosoft%5CWindows%5CINetCache%5CContent.Outlook%5CKGAHOY4P%5CCMTEDDSecurity%40act.gov.au).
		1. The Working With Vulnerable People registration is another form of background checking used by the ACT Government to ensure the suitability of personnel to hold certain roles that involve contact with groups of people who are identified as vulnerable. This is not a security check and does not give access to classified information.
		- More information on the Working With Vulnerable People registration is available [here](https://www.accesscanberra.act.gov.au/business-and-work/working-with-vulnerable-people/working-with-vulnerable-people-scheme).