National Library of Australia

# Personnel Security

Facilities and Security

Procedure

---

**Approved by:** [redacted]

**Date approved:** 19 September 2023

**Next Review:** 19 September 2024

**Document tracking:**

| Date | Name | Role | Revision |
|---|---|---|---|
| 25/06/2023 | | **Agency Security Adviser** | **Initial draft** |
| 19/09/2023 | [redacted] | **Chief Security Officer** | **Review and approval** |

---

# Contents

# Overview

The Personnel Security Procedure describes the processes surrounding the management of staff and contractors to assist in protecting the National Library of Australia (the Library) collections, information, assets and people. This includes the processes for onboarding of new staff, assessing ongoing suitability of staff with Australian Government Security Clearances and the separation of personnel.

Personnel security is based on three major components:

- identification of suitable staff to access agency information, resources and assets;
- educating staff about their security responsibilities; and
- monitoring and evaluation of a staff member's continuing suitability.

Personnel security policies and procedures ensure that people to whom official, sensitive or classified material, or other nationally significant material, are entrusted (or who need to enter specified areas):

- are eligible to have access;
- have had their identity established;
- are suitable to have access (based on a determination of honesty, trustworthiness, maturity, tolerance and loyalty), and
- are willing to comply with the standards that safeguard those resources against misuse.

Additionally, processes which are integral to appropriately managing personnel security are:

- Onboarding pre-employment screening – is the primary activity used to establish an individual's integrity to access information, assets, and collection items, before they commence employment with the Library. Australian Government Security Clearances are required for a number of designated positions in the Library to provide additional assurances of an individual's suitability and integrity.
- Ongoing management of personnel – assessing and managing ongoing suitability helps to ensure that individuals continue to meet suitability requirements which were previously established on engagement.
- Separating personnel – ensures departing personnel fulfil their obligations to safeguard Library and Australian Government information and resources.

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]

FaS are responsible for the issuing of Access Passes, arranging any additional access requirements and the processing of security clearances.

# Roles & Responsibilities

The following table outlines the key roles and responsibilities required to manage and implement all Security Procedures

| | |
|---|---|
| Library Executive | Accountable for the management of protective security risks that have Library-wide or significant impacts. |
| Chief Operating Officer | Reviews the Agency Security Plan.<br>Appoints the Chief Security Officer. |
| Chief Information Officer (CIO) | Reviews the Agency Security Plan and the *IT Security Policy*.<br>Appoints the Chief Information Security Officer. |
| Chief Security Officer (CSO)<br>***Director, Facilities and Security*** | Responsible for operational management of NLA protective security arrangements.<br>Owns the Agency Security Plan.<br>Appoints the Agency Security Adviser.<br>Oversees the management and investigation of security incidents. |
| Chief Information Security Officer (CISO)<br>***Director, Technology Operations*** | Responsible for management of NLA electronic information, IT and cyber security arrangements.<br>Appoints the IT Security Adviser.<br>Responsible for overseeing IT or cyber related security incidents. |
| IT Security Adviser (ITSA)<br>***Assistant Director, Technology Operations*** | Responsible for implementing electronic information security management, cyber security management, the *IT Security Policy* and supporting procedures.<br>Responsible for cyber security and IT related incidents and reporting. |
| Agency Security Adviser (ASA)<br>***Assistant Director, Security*** | Operational responsibility for managing protective security relating to personnel, assets and non-electronic information.<br>Responsible for the maintenance of the Agency Security Plan and supporting procedures.<br>Responsible for day-to-day implementation of the Agency Security Plan and supporting procedures.<br>Manages the Security Risk Register.<br>Responsible for managing personnel, assets and non-electronic related information security incidents.<br>Oversees the Security Control Centre and security contractors. |
| Director, Knowledge and Website Management | Responsible for ensuring information holdings generated or managed by Library personnel are managed according to the *IT Security Policy*. |
| Library Staff & Contractors | Responsible for understanding and applying robust security practices to protect the Library's people, collections, information and assets.<br>Required to complete annual security awareness training. |

# Access Pass

The Library's Access Pass conforms to the design and layout guidelines stipulated by the Australian Government for all government agencies. The Access Pass incorporates various features including:

- [redacted]
- [redacted]
- [redacted]
- [redacted]

Staff are issued with an Access Pass, which is programmed with their unique access control profile. A completed *Request for Security Access Pass or Change of Access* form is used to build the staff member's access control profile. This form provides the governance mechanism that links access control within the Library's buildings to staff position descriptions.

When the expiry date on an Access Pass has passed, the access control functions are deactivated automatically through the Electronic Access Control System (EACS). For ongoing Library staff, the Access Pass is valid for [redacted]. Contractors' access is provided depending upon the nature of engagement as outlined in the Table below:

| Type of employment | Building Pass Expiry from activation | National Police Check Revalidation required |
|---|---|---|
| Ongoing staff | [redacted] | Yes |
| Temporary staff | [redacted] | Yes |
| Contractors (unless otherwise stated) | [redacted] | Yes |

Upon expiration of an Access Pass, staff and contractors are required to complete a *Request for Security Access Pass or Change of Access* form and follow the process for requesting an Access Pass. The revalidation ensures the EACS has a current photo of the individual and the correct access privileges.

[redacted]

## Request for Security Access Pass

1. The *Request for Security Access Pass or Change of Access* form is completed by the delegate and approved by the employing Director.
2. Director to ensure the staff member is only provided access to locations where they are required to work.
3. The signed form must be uploaded into the MyNLA Service Hub 48 hours before the new starter begins employment.
4. FaS review the request in Service Hub, identifying what access is required, start and finish dates and that the relevant Director has signed the form.
5. Upon approval from FaS, the request is assigned via the [redacted] Ticketing System to Security Operations team within the Security Control Centre (SCC).
6. Upon receipt of the request in [redacted], the SCC guard processes the request, ensuring the appropriate door and entry rules are established in the EACS.
7. SCC guard confirms to FaS via [redacted] that the request has been processed.
8. FaS send an acknowledgment to the originator, identifying that the request has been processed.

9. New starter to arrive at the SCC after 9:00am on day of commencement to finalise the process and receive the Access Pass.

## Change of Access

Change of access privileges for staff is progressed through the *Request for Security Access Pass or Change of Access Procedure.*

## Contractors

In house ongoing

Access for in-house ongoing contractors is progressed through the *Request for Security Access Pass* form. This applies to [redacted], [redacted], [redacted], [redacted], [redacted] and [redacted] personnel and may be applied to other contracted service providers if the need arises.

Contractors must sign out their Access Pass daily through the *Staff & Contractor Access/Key Register.* Access Passes are to be returned to the SCC at the end of the day or on completion of work for the day.

In house non-ongoing (over 3 months)

Access for in-house non ongoing contractors is progressed through *the Request for Security Access Pass Procedure.* The Access Pass remains with staff during the period of their employment.

Short term (under 3 months)

Pre-prepared contractor passes (non-photographic) are issued to [redacted] catering staff members and other frequent contractors. These contractors provide regular service and maintenance.

Some short term pass holders may retain their Access Pass depending on the length of time they are expected to be on site to complete work. A limited number of contractors may visit multiple Library sites in a day and it may become necessary to hold the Access Pass for a several days until work is completed. Approval must be sought from the Agency Security Advisor (ASA).

The SCC monitors the *Staff & Contractor Access/Key Register* to ensure Access Passes have been returned.

## Research Fellows and Volunteers

Research Fellows and Volunteers are to follow the same process as contractors. Research Fellows will often attend the Library sporadically during a year and are therefore required to leave their Access Pass at the SCC when not expecting to be attending the Library for an extended period. Research Fellows and Volunteers are permitted to take their Access Pass off site when it is in frequent regular use.

## Visitors

1. Staff member directs the visitor to attend the SCC and make themselves known to the SCC guard.
2. Visitor to sign the Staff and Contractor Access/Key Register log.
3. The Visitor pass does not have access control privileges encoded. Visitors must always be escorted by a member of staff through the restricted access-controlled areas of the building.

4. Staff member escorts visitor back to the SCC on completion of their visit.
5. Visitor hands the Visitor Pass and the SCC guard logs return of Visitor pass on the Staff and Contract Access/Key Register log.

## Events

The SCC holds [redacted] Access Passes pre-encoded for Events occurring in the Library. The Events team will advise the SCC when they are required. [redacted]. Events staff are to follow the contractor sign in procedure.

## Lost or stolen Access Pass

Lost or stolen Access Pass are to be:

- Reported immediately to the SCC guard via extension [redacted] or in person,
- SCC will cancel the Access Pass immediately, preventing unapproved access to the building. The SCC will provide a Temporary Staff Access Pass,
- Complete a *Request for Security Access Pass or Change of Access* form, providing any relevant information regarding circumstances surrounding the loss in the Notes section. Director's signature is required to approve the creation of a new Access Pass.

[redacted]

[redacted]

[redacted]gister

[redacted]

[redacted]

[redacted]

## Extended leave, temporary transfer or secondment

Separating personnel include those taking extended leave. Personnel taking extended leave six months or greater will have their Access Pass suspended until their return.

1. When the SCC guard is informed of the person's last day of work, their Access Pass will be set to expire at [redacted] on the last day of employment. The Access Pass will be deactivated, not removed from the EACS.
2. On leaving the building, the separating person is to hand in their Access Pass to the SCC [redacted].

# Definitions

| | |
|---|---|
| AGSVA | Australian Government Security Vetting Agency |
| ASIO | Australian Security Intelligence Organisation |
| Baseline | A security clearance which provides access to security classified resources up to and including PROTECTED |
| Contact Reporting Scheme | A scheme administered by ASIO that assists in identifying intelligence gathering or hostile activity directed against Australia and its interests, government employees, contractors and people who hold Australian government security clearances. |
| DSAP | Designated Security Assessed Positions (DSAP)<br>Positions identified by an entity which requires an Australian Government security clearance due to handling of national security information. |
| National interest | A matter which could have impact on Australia or Australia's international reputation and bilateral relations, public confidence in the areas of tourism, trade, the economy and government and the security and safety of all Australians. |
| Library site | A physical space where business is performed. For example, a site can be a building, a floor of a building or a designated space on the floor of a building. |
| National security | A term used to describe the safety of the nation from espionage, sabotage, politically motivated violence, attacks on Australia's defence systems, foreign interference, organised crime, as well as the protection of Australia's borders. |
| Personnel | Employees and contractors, including secondees and service providers engaged by the NLA as well as anyone who is given access to Australian Government resources held by the entity as part of entity sharing initiatives. |
| Need-to-go | Access to a restricted area is limited to those who require access to do their work |
| Need-to-know | Access to information based on an operational requirement **to undertake duties** |
| Negative Vetting (NV) | A security clearance assessment process which provides:<br>Access to security classified resources up and including PROTECTED (Baseline)<br>Access to security classified resources up and including SECRET (NV1)<br>Access to security classified resources up to and including TOP SECRET (NV2) |
| Personnel security | A system to ensure that only those people whose work responsibilities require them to access official information and official resources have such access. |
| Protective security | A combination of procedural, physical personnel and information security measures designed to protect information, functions, resources, staff and visitors from security threats. |
| Security clearance | An acknowledgement by AGSVA that an individual is suitable to have heightened access privileges to facilities, ICT systems and/or to access security classified information (the level of security classification dependent on the clearance level granted) on a need-to-know basis. |

[redacted]