PARLIAMENT OF AUSTRALIA
DEPARTMENT OF PARLIAMENTARY SERVICES

APH Electronic Access Control System Code of Practice (Public Version)

What is the purpose of this document?

The Electronic Access Control System (EACS) Code of Practice (Public Version) provides an outline of:

- a definition of EACS, including transactional and non-transactional data
- the authorised purposes for which EACS can be used
- how to request quarantine of EACS information
- how to request to view and/or release of EACS information
- the process for the destruction of EACS information
- the management of licensees with other electronic access control systems at Australian Parliament House (APH)
- how to lodge a complaint about the operation of EACS at APH, and
- who to contact for further guidance.

What is EACS?

The EACS system uses electric locks, a card reader and access control cards to control access to doors with APH. EACS data provides:

- a system for identity verification to assist in minimising the risk of unauthorised access to, and within, the private areas of APH
- the ability to lockdown APH in the event of a major incident or emergency, and
- the means to investigate or respond to security and emergency incidents or breaches of the *APH Private Area Access Policy*.

EACS data includes **transactional** and **non-transactional data**:

- **Transactional data** is generated when an APH Access Card is used in APH. It contains information about how APH Access Cards have been used, including whose APH Access Card has been used and where. This type of data includes enough information to identify a person.
- **Non-transactional data** includes all other EACS data, including user account records, systems settings or user permissions. This type of data is generated when APH Access Cards are created, when configuring and assigning membership to access groups and when administering the system.

What is the purpose of EACS and the EACS Code of Practice?

At APH, EACS is used as part of a layered security response and provides access control to areas in and around the Parliamentary precincts.

The primary objective of the security arrangements at APH is to provide a safe and secure environment for building occupants and visitors, while ensuring public accessibility, and maintaining the order and decorum of APH.

The EACS Code of Practice provides a framework to oversee the management of EACS in relation to the creation, storage, system use and access, release, retention, and destruction of EACS data.

One of the purposes of the Code of Practice is to function as a safeguard against the possibility that the EACS data may be used in a manner which amounts, or is intended or likely to amount, to an improper interference with the free exercise by a House or committee of its authority or functions, or with the free performance by a member or the member's duties as a member. In this regard, the administration of the EACS and the powers given under the Code of Practice, have effect subject to the powers, privileges and immunities of each House and of the members and the committees of each House.

What are the authorised purposes for which EACS data can be used?

Management of the EACS is undertaken by DPS on behalf of the Presiding Officers. The only authorised purposes for which EACS data can be used are:

- to assist in the control and management of the Parliamentary precincts (including major or special events and traffic management)
- to assist in the day-to-day management of security services including investigation of security threats and incidents, pre-planning of security exercises, emergency evacuation exercises and monthly validation exercises
- to prevent, deter, disrupt or detect crime, criminal damage, vandalism or public disorder
- to assist in identifying, apprehending and where appropriate, prosecuting offenders in relation to criminality
- to provide evidence upon which to take criminal or civil proceedings
- to improve general security observation and monitoring in the areas around the Parliamentary precincts, both in terms of personal and physical security
- to improve operational response of security patrols in and around APH and precinct
- to assist emergency services in responding to incidents, and
- any other incidental purpose related to the above that have been approved in writing by the Presiding Officers and notified to the committee of each House with oversight for parliamentary security.

How to access EACS data

To access APH EACS data for the above-mentioned authorised purposes, the following provides guidance.

If further assistance is required, please contact the DPS Security Reporting and Compliance Team via security.reporting@aph.gov.au.

Quarantine of requested EACS data

- Subject to availability and appropriate approvals, the requested data will first be quarantined.
- If approved, data will be quarantined and retained for a period of 180 days.
- Extensions to the quarantine period may be requested and are subject to approval.
- To request transactional data, the requestor must fill in the EACS – Request to Quarantine Transactional data form.
    - Non-transactional data request does not require quarantine of data.

View and/or release of the requested EACS data

- Transactional EACS data is accessible by Authorised Officers for a maximum period of up to 180 days unless certain conditions are met.
- Non-transactional data can be released to Access Officials on request by completing the EACS – Request to Release Non-Transactional Data form and can only be provided for a point in time.
- On approval, there are two ways that data can be accessed. It can be viewed on site at APH or released to the requestor (e.g. on a USB stick).
- Access is requested through the EACS – Request to Release Transactional Data form.
    - The requestor is asked in the form to include why the data is required and the time/date range for the data being requested.
    - Requests for view or release of transactional data require approval from Presiding Officers.
- If EACS transactional data is released to the requestor, they will be required to acknowledge the conditions of receiving the data (including return and destruction requirements) and agree that at no time shall the data be used for any purpose other than the purpose specified and identified when the data was released.
- Ownership and copyright of all data rests with the Parliament of Australia.

What is the process for the destruction of EACS data?

Unless required under law or otherwise approved under the EACS Code of Practice, any quarantined, viewed or released EACS transactional data must be destroyed within the timeframe specified at the time of release or quarantine.

If the requestor requires access to the data beyond the quarantine period or no longer requires the data, the requestor must complete the EACS Transactional Data – Request to Extend/Destroy form and notify DPS Security Reporting and Compliance Team via security.reporting@aph.gov.au.

What about other Electronic Access Control Systems within APH?

Licensees within APH must report any electronic access controls systems that they own and operate within the Parliamentary precinct and must not operate electronic access control systems outside of their own licenced space. Licensees must follow security policies and procedures as outlined in their contract.

Compliance

The Presiding Officers undertake to provide to the Committee of each House with oversight for Parliamentary security, regular reporting outlining information regarding requests and any alleged breaches or complaints.

How to lodge a complaint

A complaint regarding the operation of the EACS or use of the EACS data at APH must be made in writing to the Assistant Secretary, Security Enabling Services Branch through the DPS Security Reporting and Compliance Team via security.reporting@aph.gov.au.

Further Guidance

Further detail on the application of this guidance can be sought from the DPS Security Reporting and Compliance Team via security.reporting@aph.gov.au.

Definitions

Term	Definition
Data - quarantine	Data quarantine involves separating and storing data away from other data, but within the same network.
Data - release	Data release involves removing data from the system and providing it to requestor.
Data - viewing	Data viewing is the process of looking at data on site at APH (but it does not include removing or copying the data).
Access Official	The Access Officials are nominally designated by the Entity Access Authority within the access arrangements for an area of control, who apply the access controls for that area of control in accordance with the defined access arrangements. *For example: Parliamentarians and their identified delegates perform the functions of an Access Official for their suites, the access arrangements are under the authority of the relevant Entity Access Authority i.e. the Usher of the Black Rod or the Serjeant-At-Arms who reflect these arrangements within the 'Access Protocols for Senators' and Members' Suites in Parliament House.*
Authorised Officer	An Authorised Officer is authorised to access EACS where required as part of their duties in line with the EACS Code of Practice. Authorised Officers must uphold training and security clearance requirements and are subject to routine monitoring and compliance checks.