Office of the Legislative Assembly

Information Security Policy

Contents

Version information

Owner	Date and source of approval	Version and OLARIS #	Description of changes	Next review due
Records and Information Manager	Clerk, April 2018	18/000579	Initial draft	April 2020
Manager, Security and Building Services	Clerk, December 2023	OLA23-0219	Updated to reflect ACT PSF INFOSEC requirements; strengthened statements on Office information holdings; defined the use/carry and storage of information.	October 2025

1. Overview and Purpose

1.1. The Office of the Legislative Assembly (the Office) creates, holds and receives a wide range of information from a variety of sources, including the Assembly, ACT community and ACT Government. Some of this information is official and sensitive in nature (official information).[1]

1.2. Information security at the Office aims to protect the integrity and security of official information.

1.3. Loss, misuse, unauthorised access, theft, or compromise of this official information can result a loss of confidence and trust—on the part of MLAs and the ACT community—in the Office's ability to perform its statutory functions effectively.

1.4. Staff must maintain a secure environment and protect official information by:

a) maintaining appropriate information security – including through the proper use, storage, transfer, handling, and disposal of official information;

b) applying the 'need-to-know' principle;

c) being aware of protective markers and how they are applied;

d) mitigating information security risks; and

e) reporting information security breaches to the Security and Building Services team.

1.5. All staff must be aware of their information security responsibilities and consider the security of information when working from the Assembly precincts, home, or another offsite location, or when travelling on official business.

Scope

1.6. This policy applies to all Office staff and contractors engaged by the Office.

Contact

1.7. Staff can contact the Office's Manager, Security and Building Services or Records and Information Manager, where they have a question about information security or their obligations under applicable laws and security policy.

[1] Official information is or relates to documents, submissions, consultations, policies, strategies, practices and procedures of the Assembly, its committees, or the Office, which are by their nature confidential.

2. Information security management

Sensitive official information at the Office

2.1. Staff of the Office often have access to information, data, documents and records that are held in electronic and paper form, or by virtue of having knowledge of a fact arising from their official role (for example, knowledge about the internal deliberations of a committee or the contents of an in-camera hearing). This can include:

a) sensitive information about the internal workings of government administration, the Assembly and its committees, MLAs and their offices;

b) information subject to non-disclosure provisions arising from legislation and the standing orders;

c) commercially sensitive information; and

d) personal information about MLAs, their staff, and staff of the Office.[2]

2.2. Employees of the Office may also have access to confidential and sensitive information in several formats including information on political, policy, legislative or procedural decisions which have not yet been made public and release of which may be an offence or constitute a contempt of the Assembly. This access can be routine or rare, depending on the role performed by a staff member.

2.3. Access to this type of information must remain confidential, shared only with those persons who are lawfully entitled to receive it, and must not be discussed in a public environment or with a person who does not have a need-to-know.

2.4. Gossiping or sharing information outside of these requirements represents a substantial threat to the integrity and security of the Office's and the Assembly's official information.

2.5. The proper functioning of the Assembly, its committees, MLAs and the Office of the Legislative Assembly depends on maintaining confidences and ensuring the integrity and security of confidential or sensitive information.

Protection of information

2.6. Because the Office handles sensitive information, there may be highly consequential impacts where unauthorised access to information occurs. Not only can unauthorised access lead to reputational damage and an erosion of trust, but it can potentially undermine the integrity and democratic posture of the Assembly's legislative, representative and scrutiny functions.

2.7. Office staff must use, store, dispose and transfer all official information in accordance with its value to the Office, the Assembly, its committees and the Territory, by:

[2] See the Information Privacy Act.

a) only accessing information that is required for their role, functions or duties (i.e., the application of the need-to-know principle);

b) complying with conditions of employment and relevant legislation, including the *Public Sector Management Act (1994)* (PSM Act), *Archives Act (1983)* and the *Crimes Act (1914)* (Cth), *Territory Records Act (2002)* when handling official information;

c) complying with relevant Office policies, including the IT Security Policy and Framework/Acceptable Use Policy and the Records, Information & Data Policy;

d) having the appropriate security clearance and/or need-to-know prior to accessing official information; and

e) periodically reviewing information to ensure classifications remain appropriate.

2.8. Disclosure of Territory information, other than to authorised persons, may be an offence under section 153(2) of the *Crimes Act 1900,* punishable by a fine or up to two years imprisonment or both.

2.9. The following three principles apply in safeguarding information:

a) **Confidentiality** – avoid disclosing sensitive information to anyone not authorised to access it.

b) **Restricted availability** – information is only made available to staff or others who have a legitimate need-to-know.

c) **Integrity** – information has not undergone unauthorised modification.

2.10. Protections need to be applied during all stages of the information lifecycle – from creation, copying and storage, through to movement, use and destruction:

a) under-classification (i.e., incorrectly assigning a lower level of security classification than is warranted by the nature of the information) results in information not having the appropriate protections required; and

b) over-classification (i.e., incorrectly assigning a higher level of security classification than is warranted by the nature of the information) reduces access/discoverability and increases information management costs.

The need-to-know principle

A person's position of authority within the Office or any other organisation does not provide them automatic 'need-to-know'. Granting access to sensitive material because it is convenient to do so, or because a person is seen as being important, are not valid reasons to provide access.

For example, just because a person is a minister, a senior ministerial adviser, or official in a government directorate does not mean that an entitlement to information access arises.

2.11. In line with the need-to-know principle, official information should only be made available to individuals who require access to do their work and who are duly authorised to access that information.

2.12. The originator or initial receiver of information is responsible for determining who has a need-to-know.

2.13. Security classified information may only be accessed by staff who hold the minimum security clearance required to access that information:

Minimum Clearance Required to access	Information Markings
Not Applicable	OFFICIAL and OFFICIAL: Sensitive
Baseline	PROTECTED
Negative Vetting 1	SECRET
Negative Vetting	TOP SECRET
Positive Vetting	TOP SECRET

2.14. The Office does not have positions that require a staff member to hold and maintain a security clearance at Negative Vetting Level 1 or above.

Clear Desk

2.15. While the Office does not have a clear desk policy, OFFICIAL: Sensitive information must not be left out in the workplace after the close of business or during extended absences from the workplace.

2.16. Desks and printers **should** be kept clear of loose papers and OFFICIAL material be organised neatly, using drawers, trays for example.

2.17. When printing official information, staff muse utilise the Office's 'follow-me-print' function attached to their Building Access Pass[3].

2.18. At the close of business, or during extended absences, staff should:

a) lock their computer screens;

b) clear whiteboards and desks of sensitive information; and

c) lock and secure keys to cabinets, drawers and offices.

[3] Printing large volumes of sensitive information can be defined as inappropriate use of ICT systems and Assembly data and may pose a security risk to the Assembly.

3. Information and protective marking guideline

3.1. Office staff who create information - sometimes referred to as originators – need to determine which information and/or protective marker to apply. For guidance on how to classify a document, please see Annexure A.

3.2. Official information held by the Office must be protected from intentional or unintentional disclosure, manipulation, modification, copying or erasure. Protective markers indicate the level of protection to be applied to official information. The Office uses the following dissemination limiting markers:

a) OFFICIAL

b) OFFICIAL: Sensitive

i) OFFICIAL: Sensitive – Legislative Secrecy

ii) OFFICIAL: Sensitive – Personal Privacy

iii) OFFICIAL: Sensitive – Legal Privilege

3.3. Once information has been identified as requiring some form of protection, a marker is assigned. All emails and word documents and Office records require a dissemination limiting marker to be assigned by an Office staff member as part of the creation process.

3.4. A protective marker indicates the sensitivity of the information and the level of protection required during the use, storage, disposal and transfer of the information.

3.5. The originator should add the relevant marker to their document:

a) The first letter of each word capitalised.

b) Bold and in red colour.

c) Size 12 font.

d) On both header and footer and centre aligned.

e) On all pages.

Official information

3.6. Any information created as part of official duty, that is not sensitive and not security classified, is considered OFFICIAL. This forms most of the routine information created in the government and at the Office. Information of this type should be marked OFFICIAL.

3.7. Information prepared by staff outside the scope of their role i.e., not as part of their work for the Office, is considered UNOFFFICIAL.

Protective markings

3.8. The OFFICIAL: Sensitive protective markings indicates that the information requires protection. A marker is used when the information does not meet the threshold of security classification but should be restricted to personnel with a legitimate need-to-know.

3.9. OFFICIAL: Sensitive information at the Office is information that, if the subject of unauthorised access, would:

a) result in a loss of confidence by Members of the Legislative Assembly (MLA) in the Office's ability to advise the Assembly, its committees, and its MLAs independently and competently in relation its functions under the Legislative Assembly *(Office of the Legislative Assembly) Act 2012*; or

b) expose the Commonwealth; the Territory; the Assembly, its committees, or its MLAs; or staff of the Office to possible improper interference (including foreign interference); or

c) be a breach of legislation, the standing orders, or a contempt against the Assembly.

3.10. Examples of **OFFICIAL: Sensitive** information in the context and in consideration of the Office's unique operating environment is:

Marker	Definition	Example(s)
OFFICIAL: Sensitive	Compromise would result in a loss of confidence by Members of the Legislative Assembly (MLA) in the Office's ability to advise the Assembly, its committees, and its MLAs independently and competently in relation its functions under the *Legislative Assembly (Office of the Legislative Assembly) Act 2012.*	Protective security and business continuity planning, risk assessments. Information coming to the attention of an Office staff member concerning Inter-party/inter-MLA discussions about policies, legislation, procedural tactics or strategies associated with parliamentary processes.
OFFICIAL: Sensitive – Legal Privilege	This marking is used to identify information that is subject to legal professional privilege.	Correspondence seeking or receiving advice from any legal professional body/person, including the ACT Government Solicitor's Office or Solicitor-General.
OFFICIAL: Sensitive – Personal Privacy	This marking is used for information that contains a fact or opinion, whether true or not, about an individual or an individual who is reasonably identifiable. This marking should be applied to all sensitive personal information as defined	Personnel records, including financial information about MLAs, their staff, Office staff. Information about members, their staff and OLA staff relating to

Marker	Definition	Example(s)
	under the *Information Privacy Act 2014* and personal health information under the *Health Records (Privacy and Access) Act 1997*. Staff handling this information should also be aware of their obligations under the OLA Privacy Policy.	geographical movements and physical location, leave requests or timesheets.
OFFICIAL: Sensitive – Legislative Secrecy	This marking is applied to information where the disclosure of which, in one or more circumstances, would be unlawful due to a legislative or a parliamentary procedural requirement.[4] Additionally, where there is a statutory prohibition on disclosure of certain information, this marker would apply[5].	Confidential internal deliberations of committees and decision made prior to authorisation. [6] Confidential advice provided by the Office to MLAs (and working papers and correspondence relating to that advice).
CABINET	This marking is to be applied to: Any document including but not limited to business lists, minutes, submissions, and memoranda that has been submitted or proposed to be submitted to Cabinet. Official records of Cabinet. Any other information that would reveal the deliberations or decisions of Cabinet or matters submitted or proposed to be submitted to Cabinet. Additional handling requirements for Cabinet information are outlined in the ACT Government Cabinet Handbook.	Cabinet and Budget submissions.

[4] The Assembly's contempt power and its other powers, privileges and immunities arise by way of statutory provision. See s 24 of the *Australian Capital Territory (Self-Government) Act 1988* (Cth) and the *Parliamentary Privileges Act 1987* (Cth)

[5] For example, it is an offence under the section 44 of the *Public Interest Disclosure Act (2012)* (Act) to use or divulge 'protected information' (protected information, under that Act, means information about a person that is disclosed to, or obtained by, a person to whom this section applies because of the exercise of a function under this Act by the person or someone else).

[6] See standing orders 241 and 277.

Information security breaches

3.11. The Office uses a three-tiered system for managing information security non-compliance, referred to as a security breach.

3.12. The purpose of issuing a breach notice is to re-enforce proper information security practice and help reduce the likelihood of a similar incident occurring.

3.13. A security breach notice may be issued to staff in a hard copy or via email. For example, if a report was made to the Manager, Security and Building Services, the Manager will assess the information and in consultation with the Office's Agency Security Executive[7], will discuss the matter with the staff member.

3.14. Following discussion with the staff member and based on evidence gathered, the Manager, Security and Building Services and Agency Security Executive will determine if a breach has occurred or issue a warning. A record of the outcome will be recorded.

3.15. If clear negligent actions and behaviour has occurred resulting in the loss of sensitive information, a higher tiered breach may be applied.

3.16. The three tiers of security breaches are set out below:

a) **Security Notice** – an accidental or unintentional failure to observe the guidelines set out in this policy, potentially or actually causing limited reputational damage to the Office. The Manager, Security and Building Services and Agency Security Executive may opt to provide a warning in this instance and re-educate the staff member.

   i) **Example** – A staff member unintentionally sends an email marked OFFICIAL: Sensitive outlining an Office physical security risk assessment to an external vendor.

b) **Security Infringement** – a negligent or reckless action that leads, or could lead, to the loss, damage, corruption or disclosure of official or sensitive resources with the potential for significant damage to the Office's reputation and damage the Assembly's trust if the Office.

   i) **Example** – A staff member intentionally sends and email marked OFFICIAL: Sensitive containing an MLAs personal records, including financial information, to an external party without consent.

c) **Security Violation** – a deliberate action that leads, or could lead to the loss, damage, corruption or disclosure of official or sensitive resources with the potential for grave damage to the Office's reputation and damage the Assembly and public's trust if the Office.

   i) **Example** – Deliberate misuse and disclosure of Embargoed information.

[7] The Office's Executive Manager, Business Support

Multiple security breaches

3.17. Poor information security poses a significant risk to the Office, and this is reflected in the management of security breaches. Multiple breaches within a 12-month period may have serious consequences for the staff member:

a) **First breach** – staff to be counselled by Manager, Security and Building Services.

b) **Second breach** (or any security infringement) - staff to be counselled by Agency Security Executive.

c) **Third breach** (or any security violation) – staff to be counselled by the Clerk.

3.18. Staff members who incur three or more security breaches within a 12-month period may be considered to have breached the *Public Sector Management Act 1994* (PSM Act) and *OLA Staff Code of Conduct*.

Recording and reporting security breaches

3.19. Information on security breaches is managed centrally and retained by the Manager, Security and Building Services.

3.20. Breach reporting is confidential and is issued by Agency Security Executive to the Office's Executive Management Committee.

3.21. Under certain extreme circumstances, security breaches may be referred to the Australian Federal Police and may result in criminal prosecution.

Security Classifications

3.22. Security classifications are used to reflect the potential damage to the national interest, organisations or individuals from compromise of the confidentiality of the information. The security classifications include:

a) PROTECTED

b) SECRET

c) TOP SECRET

3.23. On rare occasions, Office staff may receive a hardcopy of security classified information from an external party (security classified information cannot be transmitted on the Office's ICT network). If this occurs, the responsible staff member **must** contact the Manager, Security and Building Services or Records and Information Manager as soon as possible to discuss handling and storage requirements.

Principal of aggregation

3.24. Collections of protectively marked information may require a higher protective marking than any one of its component parts where the compromise of combined information would cause greater damage to the Office's reputation.

3.25. For example, a collection of OFFICIAL documents may require a collective rating of OFFICIAL: Sensitive if, together, they disclose an understanding of an internal process, deliberation or consideration that could cause harm to the Office, the Assembly or the Territory were unauthorised disclosure to occur.

4. Information handling requirements (including storage, carry and disposal)

Minimum requirements for Official information

4.1. Official information must be handled appropriately, with consideration being given to the following:

Item	Requirement
Protective Marking	There is no requirement to apply text-based markings to OFFICIAL information, but it is good practice. If using text-based markings, apply protective marking OFFICIAL to documents (including emails) in line with part 3.5 of this policy.
Access	Personnel should apply the need-to-know principle for OFFICIAL information, but it is not a mandatory requirement.
Use	OFFICIAL information and mobile devices that process, store or communicate OFFICIAL information, can be used in and outside the Office with no restrictions.
Storage	OFFICIAL information and mobile devices that process, store or communicate OFFICIAL information can be left unattended, however a clear desk policy should be considered. It is recommended that mobile devices are in a secured state if left unattended. Storage of OFFICIAL information in a lockable container is recommended in and outside the Office.
Records and Information Management System	OFFICIAL information located in the Office's records and information management system (OLARIS) must be saved with the need-to-principal applied. It is recommended that staff consult the Office's Records and Information Manager to help determine and identify access privileges prior to saving or

Item	Requirement
	marking their work if unsure.
Carry	There are no specified handling requirements.
Transfer	For transfers outside the Office, it is recommended that information be placed in an opaque envelope or folder and sealed to minimise risk of unauthorised access.
Overseas travel	OFFICIAL information can be taken on domestic and overseas travel.
Disposal	Apply disposal procedures in accordance with the *Territory Records Act 2002*.

Minimum requirements for OFFICIAL: Sensitive information

4.2. Official: Sensitive information must be handled appropriately, with consideration being given to the following:

Item	Requirement
Protective Marking	Apply text-based protective marking OFFICIAL: Sensitive to documents and emails in line with part 3.5 of this policy.
Access	The need-to-know principle applies to all OFFICIAL: Sensitive information.
Use	OFFICIAL: Sensitive information and mobile devices that process, store or communicate OFFICIAL: Sensitive information can be used in any are of the Office. Outside the Office (including at home) For regular ongoing and occasional home-based work, exercise judgement when using devices or hard copy information that is rated Official: Sensitive. If required, the Manager, Security and Building Services can provide a security assessment to assess environmental risks. For use anywhere else outside Office facilities (for example, café or airports), apply judgement to assess environmental risk.
Storage	OFFICIAL: Sensitive information can be left unattended for short periods. Mobile devices that process, store or communicate OFFICIAL: Sensitive information can be left unattended if in a secured state. When storing physical OFFICIAL: Sensitive information or devices inside the Office, store in a lockable container. If storing outside the Office, personnel should place in an opaque envelop or lockable container. For regular ongoing home-based work, storage in a security container may be required (see Manager, Security Building Services for more information).

Item	Requirement
Records and Information Management System	OFFICIAL: Sensitive information located in the Office's records and information management system (OLARIS) must be saved with the need-to-principal applied. It is recommended that staff consult the Office's Records and Information Manager to help determine and identify access privileges prior to saving or marking their work if unsure.
Carry	When carrying physical OFFICIAL: Sensitive information inside and outside the Office (for example, to external meetings), personnel should use an opaque envelope or folder.
Transfer	When transferring OFFICIAL: Sensitive information inside the Office, it is recommended that personnel place in an opaque envelope or folder. When transferring outside the Office, place in an opaque envelope and consider using a seal.
Overseas travel	**Travel in Australia** When travelling with OFFICIAL: Sensitive information, or a mobile device that processes, stores or communicates OFFICIAL: Sensitive information, apply requirements for carrying outside Office facilities. **Travel outside Australia** When travelling overseas with OFFICIAL: Sensitive information or a mobile device that processes, stores or communicates OFFICIAL: Sensitive information apply requirements for carrying outside Office facilities and any additional requirements as required by the Manager, Security Building Services.
Disposal	Apply disposal procedures in accordance with the *Territory Records Act 2002.*

Annexure A – Classification flowchart