Policy name	Office Management of Confidential Information
Policy date	February 2026
Authorisation	Executive Housing & Property
Policy owner	Executive General Manager, Housing Operations
Policy type	Mission Australia Housing Operational Policy
Policy setting	

1 Purpose

1.1 Overview

1.1.1 This policy sets out the principles to be followed to ensure the Confidentiality of Information held in offices managed by Mission Australia Housing (MAH). We aim to:

- Ensure off MAH office spaces remain secure and confidential information remains confidential.
- Ensure staff understand the importance of maintaining confidentiality when managing the office, including security of files, computer systems, telephone systems, key storage, and alarm codes; and
- Complies with the specific legal and contractual obligations placed upon MAH by government, funders, and other housing partners.

1.2 Coverage

1.2.1 This document is a national policy and covers Mission Australia Housing (MAH), and its entities. All references to Mission Australia Housing, MAH and Housing means MAH and its entities unless specifically stated otherwise.

1.2.2 This policy applies to all the MAH office spaces.

1.2.3 This policy applies to all forms of housing provided by MAH including social, affordable and transitional housing.

1.2.4 This policy applies to housing provided by MAH in the jurisdictions of New South Wales (NSW), Tasmania (TAS), Victoria (VIC), Queensland (QLD), Western Australia (WA) and the Northern Territory (NT). Where jurisdiction-based variations exist in policies and procedures, these will be identified in the document.

1.3 Information on procedures and other related policies

1.3.1 This policy is one of several interlinked policies that support MAH's delivery of housing services. To assist you, these are identified where relevant in this policy and the supporting procedures.

2 Scope

2.2 Parts of Mission Australia that this policy covers

2.2.1 This policy applies to all MAH staff and visitors to MAH offices.

2.3 Definitions

2.3.1 Key terms used in this policy are defined in the following table.

Term	Definition
Applicant	A person applying for housing assistance with MAH.
Confidentiality	Is the right of an individual not to have personally identifiable information disclosed to others without that individual's express informed consent.
Keys	Are either the keys or swipe cards or other means such as access codes to enter a building, either the office or properties.
Record	Is a manual or electronic record containing a Tenant or applicants personal and tenancy information.
Systems	Systems that create, process and manage data to support business processes.
Tenant	Under state-based residential tenancy and rooming accommodation legislation, a Tenant is a person who has entered explicitly into a lease agreement. The term is used more broadly in this policy to refer to Tenant's and residents under rooming accommodation agreements, unless explicitly distinguished.

3 Policy

3.2 Guiding principles

3.2.1 It is important to uphold strict confidentiality processes within the office environment to protect Tenant's and applicants.

3.2.2 All staff visiting a MAH office have a responsibility to ensure that they follow the **Office Management of Confidential Information policy and procedure** to ensure the safety of the offices and confidential information.

3.2.3 Confidential information will include any information about Tenants or Applicants that will be reasonably required for staff to perform their duties. Staff should refer to the **MA Enterprise Privacy Policy** for examples of Confidential information that may reasonably be asked for.

3.2.4 In the wrong hands, confidential information can be misused to commit illegal activity, which in turn could lead to legal action taken against MAH that could result in significant financial or other penalties for the individual or the organisation.

3.2.5 All staff are accountable for the efficient, effective, and appropriate use, management and security of records and information resources that are received, created, acquired or retained in the performance of official duties.

3.2.6 Systems in place to manage information need to operate to ensure:

- The information is accurate and can be trusted;
- Are complete and unaltered;
- Managed across their lifecycle and protected from unauthorised use and inappropriate deletion; and
- Are findable and readable.

3.2.7 The MAH Office Management of Confidential Information policy complies with relevant laws and procedures, including jurisdictional requirements of the states and territories in which it operates.

3.3 Management of reception and general office areas

3.3.1 MAH will record all visitors to the offices and access to office spaces will be limited to those with an authorised purpose.

3.3.2 MAH will ensure clear desks in the office, minimising the risk of access to documents and information on desks.

3.3.3 All conversations with tenants or applicants should be contained to designated areas so that sensitive information cannot be overheard.

3.3.4 Meetings with staff related to their employment or performance should be undertaken in designated staff meeting rooms or offsite.

3.4 Office Keys

3.4.1 The designated staff member responsible for management of the administration of the office ('Office Administrator') is to keep a record of the office keys detailing the persons who have been allocated keys, any security codes associated with the keys and the date keys are returned.

3.4.2 Spare keys will be kept in a locked cabinet.

3.4.3 All key holders must ensure that the keys are kept securely and not left unattended.

3.4.4 Any loss of keys must be immediately reported to the Office Administrator and State Manager.

3.5 Property Keys

3.5.1 MAH may retain duplicate keys to properties.

3.5.2 Identifying property address details will not be kept on keys.

3.5.3 The **Managing Keys Procedure** and the **Office Management of Confidential Information Procedure** will set out how keys will be stored and managed.

3.5.4 Keys will only be issued to the Tenant named on the lease for the property or authorised recipient. The date, key number, and identity of the Tenant who the keys have been released to, should be recorded into a key register.

3.6 Computer Systems

3.6.1 All staff must have a screensaver lock on their PC, and when they are not at their desk, the PC screen should be locked.

3.6.2 At the end of each day, computers in the office, should be turned off and not connected to the internet.

3.6.3 All computers should have a password, an anti-malware program installed and firewalls in place to block unsafe programs and viruses.

3.6.4 Staff should not share or distribute personal passwords for any computer systems (internal or external) that they may access in order to perform their duties.

3.6.5 Following termination of employment, a staff members access to IT systems will be terminated.

3.6.6 An audit will be completed every quarter to ensure staff who have left no longer have access to systems MAH use (internal and external).

3.7 Paper Records

3.7.1 It is important to protect paper documents. All tenant and property files must be secured in a lockable filing system.

3.7.2 All files should be returned to the filing system when they are not in use. Files should not be left on desks overnight, or when staff members are not in the office.

3.7.3 All offices should have a shredder or a secure confidential disposal bin in an easy to access area for secure disposal of any confidential information.

3.8 Record Management

3.8.1 Staff should maintain accurate records of interactions with applicants and tenants. For more information on communication with Tenants see the **Communications with Tenants Policy.**

3.8.2 All staff should uphold the security and privacy of information retained in the information systems that they have access to. For more information, see the **Housing Record Management Policy & Procedure.**

3.9 Tenant Request to Access Files

3.7.1 Tenants can make a request to access their personal information on file at any time.

3.7.2 MAH will generally provide access to the information in the manner requested unless applicable laws allow us to refuse, or prevent us from giving, access to the personal information. For further information see **MA Privacy Policy.**

3.7.3 MAH will not unreasonably refuse requests to access personal Information and we will respond to requests for access within a reasonable time.

3.7.4 MAH will only deny a request for information in exceptional circumstances. This may include:

- The information would breach the privacy of others
- Providing the information would be illegal.
- Providing the information could affect the health and safety of others.

3.10 Archive

3.10.1 Records should be maintained, including retention, archive and disposal in line with contractual responsibilities.

3.10.2 Each office should arrange to annually archive the previous 12 months records of vacated tenancies or properties that have been terminated /disposed of. The **Office Management of Confidential Information Procedure** sets out the procedure for archiving information.

3.11 Telephone Systems

3.11.1 All Tenant's and applicants should be given the main corporate telephone number; this ensures that calls are tracked and directed to the correct teams.

3.12 Office security access

3.12.1 All offices should incorporate a procedure around managing the office security in their localised Operations Management Plans/Manual. Each office should delegate a minimum of two staff members responsible for monitoring the adherence of this procedure for the office.

4 Responsibilities

4.2 Housing staff, including Housing Officers and Client Service Officers, are responsible for:

- Following the policy and procedures.
- Recommending improvements to this policy and associated procedures.
- Protect the privacy of tenants personal and sensitive information on file.
- Provide tenant requested personal information from file with Team Leader approval.

4.3 Team Leaders/Regional Manager are responsible for:

- Incorporating this policy and associated procedures into staff induction and training.
- Ensuring staff are aware of and have access to this policy and associated procedures.
- Escalating feedback about this policy to the policy owner and/or policy writer.
- Approval to provide personal information on file at tenants' request.

4.4 The Operations Manager and State Manager is responsible for:

- Ensuring that MAH complies with this policy and associated procedures.
- Recommending any changes to this policy and associated procedures.