

Rec implemented (✓-Yes, X-No, Partial)	Measures implemented by Housing ACT since 2018	TPP	Residual privacy risks	2021 assessment recommendations to mitigate residual privacy risks	2021 assessment suggestions for privacy best practice
<p>2018 Recommendation 1</p> <p>Housing ACT should:</p> <ul style="list-style-type: none"> • create written policies and procedures which govern the use of personal information by staff • implement regular privacy training for Housing ACT staff that includes authorised uses of personal information. 					
<p>Partial</p>	<p>Housing ACT advised the OAIC that it has not developed documented internal policies and procedures governing the use and disclosure of personal information under the Housing Assistance Act, including:</p> <ul style="list-style-type: none"> • the limited circumstances where Housing ACT can share personal information with other parts of CSD • how these specific circumstances should be applied to Housing ACT’s daily work, which can be used and disclosed or how to manage this data over its lifecycle. This is important given data related to long term clients and tenancies can endure for decades. <p>Housing ACT’s response to 2018 Recommendation 2 noted that work has commenced on developing information handling policies such as data governance and management policies for CSD and a specific date was provided to complete this work (July 2020). During the follow up assessment, Housing ACT advised that this work was not completed due to whole of ACT government data management initiated from the Office of the Chief Digital Officer, as well as the impacts of the COVID-19 pandemic on Housing ACT’s and CSD’s resources.</p> <p>Housing ACT advised that it has:</p> <ul style="list-style-type: none"> • implemented aspects of 2018 Recommendations 1, 2 and 3 relating to establishing regular training. 	<p>6</p>	<p>Lack of documented policies and procedures raises the medium privacy risk that Housing ACT staff may be using, disclosing or protecting personal information inconsistently with the requirements of TPPs 6 and 11 as well as the Housing Assistance Act.</p> <p>In relation to Housing ACT’s regular privacy training, the OAIC has observed some potential areas for improvement. Specifically, there is a medium privacy risk that Housing ACT staff are not fully aware of their privacy obligations due to the training not covering all relevant privacy issues and some staff may not be undertaking the training annually.</p>	<p><u>2021 Recommendation 1</u> - Housing ACT should implement parts of Recommendations 1, 2 and 4 from the 2018 assessment by:</p> <ul style="list-style-type: none"> • documenting policies and procedures related to the use, disclosure, and protection of personal information. These policies and procedures should include: <ul style="list-style-type: none"> ○ permitted uses and disclosures under privacy, housing and other relevant legislation as well as relevant Memorandums of Understanding (MoUs) and sharing agreements ○ how authorised uses and disclosures should occur, including procedures for using and disclosing personal information ○ internal practices, procedures and systems that are used to protect personal information ○ ensuring staff are aware of and have access to these documented policies and procedures and are used to 	<p><u>2021 Suggestion 1</u> - If documented policies, procedures and systems are developed and managed by CSD and apply to Housing ACT, these documents could also include details concerning the unique functions and personal information handling responsibilities of Housing ACT staff. Alternatively, separate policies could be created by Housing ACT which are specific to Housing ACT’s activities and sit underneath CSD’s policy framework.</p> <p><u>2021 Suggestion 2</u> - Internal practices, procedures and systems which relate to the use, disclosure and protection of personal information may be addressed in a single policy or in a number of separate policies.</p> <p><u>2021 Suggestion 3</u> - In reviewing its refresher privacy training Housing ACT could either:</p>

Rec implemented (✓-Yes, X-No, Partial)	Measures implemented by Housing ACT since 2018	TPP	Residual privacy risks	2021 assessment recommendations to mitigate residual privacy risks	2021 assessment suggestions for privacy best practice
2018 Recommendation 1 Housing ACT should: <ul style="list-style-type: none"> • create written policies and procedures which govern the use of personal information by staff • implement regular privacy training for Housing ACT staff that includes authorised uses of personal information. 					
	<ul style="list-style-type: none"> • developed regular refresher privacy training for all staff <ul style="list-style-type: none"> ○ CSD has developed an online training module which applies to Housing ACT staff. The online module retains a record of who has completed the training, though managers are not automatically notified that staff members have completed the training. <p>Housing ACT intends for the training to be mandatory and undertaken annually, though they were unable to confirm if this occurs in practice.</p> <p>Housing ACT advised that the training does not consider Housing ACT's specific information handling practices. Housing ACT noted that it could request additional training from CSD if a specific need is identified.</p>			<p>inform induction and refresher privacy training undertaken by staff</p> <ul style="list-style-type: none"> • reviewing its MoU and other information sharing arrangements to ensure they are up to date and contain sufficient detail on current information handling practices. <p><u>2021 Recommendation 2</u> - Housing ACT should review its refresher privacy training to ensure it:</p> <ul style="list-style-type: none"> • contains material on Housing ACT's specific and unique personal information handling practices. • is informed by documented policies and procedures related to the use, disclosure, and protection of personal information by Housing ACT • is mandatory and undertaken annually by all Housing ACT staff. 	<ul style="list-style-type: none"> • amend the existing refresher training developed by CSD, or • request their own additional bespoke training from CSD.

Rec implemented (✓-Yes, X-No, Partial)	Measures implemented by Housing ACT since 2018	TPP	Residual privacy risks	2021 assessment recommendations to mitigate residual privacy risks	2021 assessment suggestions for privacy best practice
<p>2018 Recommendation 2</p> <p>Housing ACT should:</p> <ul style="list-style-type: none"> • create clearly written policies and procedures which govern compliance with TPP 6, including the authorised disclosure of personal information by staff under privacy, housing and other relevant legislation • conduct regular privacy training that includes the authorised disclosures staff can make and how these disclosures should occur • review its MoU arrangements for sharing information to ensure they: <ul style="list-style-type: none"> ○ are up to date and reflect current information handling practices ○ provide sufficient detail on the authorised disclosures of personal information staff can make and how they should occur ○ contain up to date information sharing protocols when required by the MoU. 					
<p>Partial</p>	<p>See response above to 2018 Recommendation 1 for Housing ACT measures in relation to:</p> <ul style="list-style-type: none"> • documented policies and procedures governing the disclosure of personal information • conducting regular privacy training that includes the authorised disclosures staff can make and how these disclosures should occur • reviewing its MoU arrangements for sharing information. <p>Other than specific agreements with third parties, and the 'Executive Level Correspondence' business rule document, which sets out how Housing ACT responds to Ministerial requests for information, the OAIC did not observe any policies or procedures that specify how staff handle authorised third-party disclosures of personal information, including requests from law enforcement agencies (LEAs).</p> <p>Housing ACT has not implemented the part of the 2018 Recommendation 2 which relates to Housing ACT reviewing its MoUs and other arrangements for sharing information to ensure they are up to date. Housing ACT advised that review of information sharing agreements has commenced but is incomplete due to delays caused by the COVID-19 pandemic. Housing ACT did</p>	<p>6</p>	<p>See medium residual privacy risk identified in relation to 2018 Recommendation 1 above.</p> <p>See medium residual privacy risk identified above in relation to regular privacy training noted against 2018 Recommendation 1.</p> <p>Where MoUs and other arrangements for sharing information are out of date and insufficiently detailed, this raises the medium privacy risk of unauthorised discloses of personal information by Housing ACT staff. In particular, there is a medium privacy risk of disclosures which are inconsistent with relevant laws and established procedures relevant to disclosing personal information.</p>	<p>See 2021 Recommendations 1 and 2 above.</p>	<p>See 2021 Suggestions 1, 2 and 3 above.</p>

Rec implemented (✓-Yes, X-No, Partial)	Measures implemented by Housing ACT since 2018	TPP	Residual privacy risks	2021 assessment recommendations to mitigate residual privacy risks	2021 assessment suggestions for privacy best practice
	not provide the OAIC with any updated MoUs or information sharing agreements.		Disclosures made by Housing ACT, such as to LEAs, may contain sensitive information, such as an individual's criminal record. The consequences of an unauthorised disclosure under these circumstances would likely cause serious harm to individuals.		
<p>2018 Recommendation 3</p> <p>Housing ACT should:</p> <ul style="list-style-type: none"> • establish clear privacy governance mechanisms in the form of procedures for oversight, accountability, and lines of authority for decisions related to privacy and personal information security. This would involve developing a formal central privacy management function that is responsible for coordinating privacy and information security matters across Housing ACT's business areas • regularly evaluate its privacy governance mechanisms to ensure their continued effectiveness • implement regular training for all staff which would also cover the protection of personal information and how staff should respond in the event of a data breach. 					
Partial	<p>Housing ACT advised the OAIC that, with the exception of managing a data breach (see 'Data Breach response plan' section below), privacy governance mechanisms within CSD and Housing ACT appear to operate in an ad hoc manner. The OAIC was not provided with any other documents that comprehensively set out Housing ACT's privacy governance arrangements including clear governance mechanisms for managing all privacy and information security related issues (not just data breaches) within Housing ACT and between Housing ACT and CSD.</p> <p>According to CSD's Data Breach Policy and interviews with Housing Act staff, the Deputy Director General (DDG) of CSD is the key position responsible for privacy management across CSD including Housing ACT. It appears that the DDG holds some of the responsibilities of a 'Privacy Champion', a senior management position with overall responsibility for</p>	11	<p>The lack of documented privacy governance mechanisms within Housing ACT raises a medium privacy risk that privacy and information security issues are not being properly identified, considered and addressed. More comprehensive agency wide governance measures specific to privacy matters would, in the opinion of the OAIC, enhance Housing ACT's privacy and security culture.</p> <p>See medium residual privacy risk identified above in relation to regular privacy training</p>	<p>See 2021 Recommendations 2 above in relation to regular privacy training and the protection of personal information.</p> <p>2021 Recommendation 3 Housing ACT should fully implement 2018 Recommendation 3 and formalise privacy governance arrangements including the 'Privacy Champion' and a 'Privacy Officer' to assist the Privacy Champion in managing privacy issues. This documented governance should clearly establish clear procedures for oversight, accountability and lines of authority for decisions related to privacy and personal information security.</p>	<p>See 2021 Suggestion 3 above, 2021 Suggestion 4 - to ensure consistency with the governance currently set out in the Data Breach Policy, Housing ACT could formally designate the DDG as the 'Privacy Champion', the senior member of staff with overall accountability for privacy and personal information security matters. Housing ACT could also consider appointing one of the current data custodians within Housing ACT as the 'Privacy Officer' responsible for daily management, coordination and reporting of</p>

Rec implemented (✓-Yes, X-No, Partial)	Measures implemented by Housing ACT since 2018	TPP	Residual privacy risks	2021 assessment recommendations to mitigate residual privacy risks	2021 assessment suggestions for privacy best practice
	<p>promotion, awareness and accountability of privacy (as that term is used under the Code). However, other than a brief reference in the Data Breach Policy, the DDG's privacy role is not formalised or documented.</p> <p>It is also unclear if the DDG is supported by a 'Privacy Officer' or a privacy team (either within CSD or Housing ACT) responsible for operational matters, such as coordinating and managing privacy related functions across CSD and Housing ACT on a daily basis. The OAIC did not observe any documented governance which sets out a privacy officer position or formal central privacy management function for Housing ACT or CSD.</p> <p>Housing ACT advised that privacy complaints or the reporting of privacy or information security incidents involving Housing ACT are likely to come through two areas:</p> <ul style="list-style-type: none"> the Quality Complaints and Regulation (QCR) team for privacy complaints received externally i.e., from individual complainants (members of the public), or the People Management Branch (PMB) when privacy issues are identified internally. <p>While these privacy and information security related complaint handling processes discussed above are not formally documented, staff interviewed by the OAIC exhibited an understanding of how to escalate such matters.</p> <p>See response above to 2018 Recommendation 1 for measures implemented by Housing ACT in relation to regular privacy training. Housing ACT advised the OAIC that regular privacy training covers the protection of personal information and how staff should respond in the event of a data breach.</p>		noted against 2018 Recommendation 1.	This would involve CSD and/or Housing ACT developing a formal central privacy management function, consisting of a privacy officer or a privacy team responsible for coordinating privacy and information security matters across Housing ACT's business areas and reporting these issues to CSD's senior management. Documented governance arrangements should clearly note which staff members within Housing ACT and CSD have been appointed to key roles and responsibilities in privacy and information security management.	<p>privacy and information security issues.</p> <p><u>2021 Suggestion 5</u> – Housing ACT, in developing a formal central privacy management function, could consider:</p> <ul style="list-style-type: none"> leveraging existing positions, committees and functions currently undertaken by QCR and PMB, or linking to, or incorporated into, existing governance processes that may be in place for engaging with Shared Services on ICT security matters.

Rec implemented (✓-Yes, X-No, Partial)	Measures implemented by Housing ACT since 2018	TPP	Residual privacy risks	2021 assessment recommendations to mitigate residual privacy risks	2021 assessment suggestions for privacy best practice
<p>2018 Recommendation 4</p> <p>Housing ACT should:</p> <ul style="list-style-type: none"> ensure that it sufficiently documents all internal policies including practices, procedures and systems that are used to protect personal information create a policy and procedures document register which clearly sets out all of Housing ACT's internal policies and procedures for privacy and information security, their date of issue, ownership, and when they are due for review regularly evaluate its current policies and procedures to ensure their adequacy and currency. 					
<p>Partial</p>	<p>For the most part the OAIC did not observe any information security policies or procedures specific to Housing ACT.</p> <p>The OAIC was provided with an 'ICT Security Plan for Homenet' in the 2018 assessment. This contained a documented process for undertaking information security risk assessments for Homenet, the ICT system used by Housing ACT to administer payments and communicate with clients. Housing ACT advised that the Homenet ICT Security Plan has not changed since it was last viewed by the OAIC in 2018. The OAIC did not observe any documented processes for Housing ACT's other ICT systems.</p> <p>The OAIC was also provided with ICT related policies developed by Shared Services which apply across the ACT Government such as the 'ICT Security Incident Response Policy' and the 'ACT Government Acceptable Use Policy'. However, these documents cover information security at a high level and are not specific to the protection of personal information by Housing ACT.</p> <p>Housing ACT advised the OAIC that it had developed a policy register known as the 'Quality Management System (QMS)' also referred to as the 'Information Management System (IMS)', in response to Recommendation 4 of the 2018 assessment. This register records all of Housing ACT's internal policies and procedures, their date of issue, ownership, and</p>	<p>11</p>	<p>See medium residual privacy risk identified in relation to documented policies and procedures noted against 2018 Recommendation 1 above.</p> <p>Despite the establishment of the IMS/QMS, the OAIC was provided with policies and other documents which appeared to be out of date or did not have a review date. For example, a guidance document on the CSD's website refers to the repealed 'Information Privacy Principles'. This raises the medium privacy risk that staff are applying out of date information handling practices set out in documents which have not been regularly reviewed.</p>	<p>See 2021 Recommendation 1 above.</p> <p>2021 Recommendation 4 - Housing ACT should use its QMS/IMS so that its policies and procedures (both internal and public facing guidance available on their website) are regularly reviewed and updated to ensure their continual adequacy and currency.</p>	<p>None</p>

Rec implemented (✓-Yes, X-No, Partial)	Measures implemented by Housing ACT since 2018	TPP	Residual privacy risks	2021 assessment recommendations to mitigate residual privacy risks	2021 assessment suggestions for privacy best practice
	when they are due for review. Housing ACT advised that each policy document has a 12-month review period. Policies are available to staff on the CSD and Housing ACT intranet.				
2018 Recommendation 5					
Housing ACT must, as a high priority, take steps to develop a data breach response plan which sets out:					
<ul style="list-style-type: none"> • contact details for appropriate staff to be notified • the roles and responsibilities of staff • processes that will assist Housing ACT to identify and contain breaches, coordinate investigations and breach notifications, and cooperate with external investigations. 					
✓	<p>The OAIC was provided with CSD’s finalised ‘Data Breach Policy’ which also applies to Housing ACT. The Data Breach Policy is dated June 2020 and is scheduled to be reviewed every two years. Housing ACT advised that the policy has not been tested.</p> <p>Section 3.1 of the Data Breach Policy contains a table setting out the Data Breach Response Group (Group) roles (for example Team Leader, Senior Privacy Officer, ICT Security Support, Media and Communications etc.) and the contacts (name of staff member and their position within CSD) who will provide assistance in the event of a serious data breach which needs to be escalated to the Group. However, only one of these contacts is listed. Therefore, it is unclear which specific individuals or positions will perform key roles within the Group. Housing ACT advised that the Data Breach Policy does not specify the membership of the Group as it will depend on how significant the breach is to determine the size of the Group to be formed.</p>	11	<p>Noting that Housing ACT has created a Data Breach Policy in response to 2018 assessment Recommendation 5, the OAIC has observed some areas for improvement as there is a medium privacy risk that aspects of the Data Breach Policy may unnecessarily delay the response to a breach. The OAIC is of the view that the policy:</p> <ul style="list-style-type: none"> • may confuse staff as to the correct process for responding to breaches due to its length and complexity. The Data Breach Policy has not been tested with no practice breaches performed by the Group to test its effectiveness • is unclear regarding which personnel should be contacted to participate in 	<p><u>2021 Recommendation 5</u> - Housing ACT should:</p> <ul style="list-style-type: none"> • test the Data Breach Policy to ensure its continued effectiveness • update the membership of the Group found in the Data Breach Policy, clearly setting out the staff making up the Group, their roles, responsibilities, and authorities as well as their contact details. Housing ACT should ensure these contact details remain updated, particularly in the event of organisational changes. Each role in the Group should have a second point of contact in case the first person is not available. 	<p><u>2021 Suggestion 6</u> - The OAIC notes that section 1.3 of the Data Breach Policy states that it is a high level, overarching document and business areas may need to develop specific business protocols, policies, documents and training that support this Policy. The OAIC suggests that Housing ACT and CSD could consider:</p> <ul style="list-style-type: none"> • whether further data breach guidance is needed for Housing ACT given the unique functions, personal information handling practices and systems used by Housing ACT staff. Results from the testing of the Data Breach Policy may demonstrate whether further guidance is warranted • creating a core team and adding other members as

Rec implemented (✓-Yes, X-No, Partial)	Measures implemented by Housing ACT since 2018	TPP	Residual privacy risks	2021 assessment recommendations to mitigate residual privacy risks	2021 assessment suggestions for privacy best practice
			the Group in the event of a serious breach.		they are required. The people selected to be in the Group will depend on the circumstances of the breach.
<p>2018 Recommendation 6</p> <p>Housing ACT should:</p> <ul style="list-style-type: none"> review its risk management processes to ensure that all privacy and information security risks are appropriately monitored, identified, treated, recorded and reported to senior management review the CSD Corporate Risk Register so that it captures information security and privacy risks relevant to Housing ACT. 					
Partial	<p>In response to the OAIC's 2018 Recommendation 6, Housing ACT conducted a review of its risk management processes and developed the 'Housing ACT – Blueprint for Risk Management' (Blueprint) which sets out Housing ACT's process for identifying, monitoring and effectively treating risks as they arise as well as integrating risk into planning processes.</p> <p>Housing ACT's Strategic Risk Register notes several privacy, information sharing and cyber security risks associated with Housing ACT's activities, along with their respective risk ratings (high, medium and low) and controls to treat these risks. Housing ACT's Strategic Risk Register also mentions risks related to data breaches. These risks along with similar ratings and controls also appear in the CSD Strategic Risk Register, which addresses part of the OAIC's 2018 Recommendation 6.</p> <p>The OAIC was also provided with an 'Organisational Change Risk Assessment Template' document, a new Housing ACT process which is used for new projects. However, this document does not specifically call out projects that involve personal information and privacy risks.</p>	6 and 11	<p>Housing ACT advised that it still needs to do more work to ensure that the Blueprint is consistent with the CSD Risk Management Framework especially if any privacy risks identified by Housing There is a medium risk that Housing ACT is not properly managing all privacy and information security risks due to:</p> <ul style="list-style-type: none"> further work required to ensure the Blueprint is consistent with the CSD Risk Management Framework especially if any privacy risks identified by Housing ACT will be treated at the CSD level or if they involve ICT security and systems risks which are managed by Shared Services 	<p><u>2021 Recommendation 6</u> - Housing ACT should fully implement 2018 Recommendation 6 and improve privacy risk monitoring by reviewing Housing ACT's risk management processes so that they:</p> <ul style="list-style-type: none"> are consistent with the CSD Risk Management Framework involve a risk governance forum which has privacy risks as a standing item record and consider privacy and information security risks identified by PIAs, privacy assessments conducted by the OAIC or other privacy assurance reviews. 	None

Rec implemented (✓-Yes, X-No, Partial)	Measures implemented by Housing ACT since 2018	TPP	Residual privacy risks	2021 assessment recommendations to mitigate residual privacy risks	2021 assessment suggestions for privacy best practice
			<ul style="list-style-type: none"> the absence of a risk governance forum which has privacy risks as a standing item to ensure privacy risks are regularly reported to and considered by senior management privacy and information security risks identified by PIAs, privacy assessments conducted by the OAIC or other privacy assurance reviews not being recorded and considered by its risk management processes. 		

2018 Recommendation 7

Housing ACT should:

- conduct a threshold assessment and if necessary, a full PIA in conjunction with an information security risk assessment on the digitisation of hardcopy client files, and any other major projects involving the handling of personal information, notable the development of the new EDRMS and the Upload Tool**
- develop and implement a PIA and information security risk assessment policy across all its activities.**

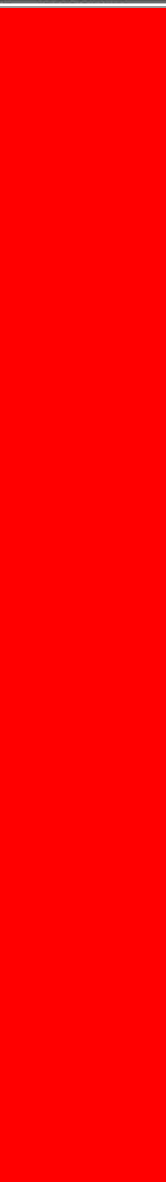
X	<p>Housing ACT staff advised the OAIC that they have not done any PIAs and information security assessments for planned projects, in particular the digitisation of hardcopy client files, the new EDRMS, and the new tool which will allow clients to upload their personal information to multiple organisations simultaneously (the Client Upload Tool). Housing ACT advised that these projects were delayed due to the COVID-19 pandemic though they intend to conduct PIAs and security risk assessments when these projects recommence.</p>	6 and 11	<p>It was not clear from the interviews with Housing ACT staff how Housing ACT undertake PIAs or information security risk assessments. The lack of any discernible policy, procedure or process across all of its activities raises a medium privacy risk that Housing ACT will not adequately consider privacy and information security issues at the design and development stage of new</p>	<p><u>2021 Recommendation 7</u> - Housing ACT should implement 2018 Recommendation 7 by:</p> <ul style="list-style-type: none"> conducting a PIA for the digitisation of hard copy files, Client Upload Tool and development of a new EDRMS when these planned projects recommence developing and implementing a PTA, PIA and information security risk assessment policy 	<p><u>2021 Suggestion 7</u> - A PTA, PIA and information security risk assessment policy could be linked to, or incorporated into, or leverage any existing approaches to information security assessments, PTAs and PIAs employed by Shared Services.</p>
---	--	----------	---	---	--

Rec implemented (✓-Yes, X-No, Partial)	Measures implemented by Housing ACT since 2018	TPP	Residual privacy risks	2021 assessment recommendations to mitigate residual privacy risks	2021 assessment suggestions for privacy best practice
	<p>The OAIC did not observe any CSD or Housing ACT policy or process for undertaking privacy threshold assessment (PTAs), PIAs and information security risk assessment for new projects involving personal information. Specifically, there was no documented policy which demonstrates how Housing ACT applies ‘privacy by design’, advises staff on when they should conduct a PTA or PIA and a methodology for conducting them.</p> <p>The ICT Security Plan for Homenet reviewed by the OAIC in the 2018 assessment did contain a documented process for undertaking information security risk assessments for the Homenet system. However, no other documented process was observed by the OAIC in relation to other systems.</p> <p>Housing ACT advised the OAIC that Shared Services handle many elements of ICT security, including approving any changes made to Housing ACT systems and have policies in place regarding risk assessments. Housing ACT provided the OAIC with the ‘Information Security Assessment’ template document (dated August 2020) developed and used by Shared Services which provides ACT Government data owners with a two-stage methodology to examine the information security requirements of an ICT system (including cloud services):</p> <ol style="list-style-type: none"> 1) Threshold Assessment and Privacy Impact Assessment 2) Information Security Assessment. 		<p>projects involving personal information.</p>	<p>across all Housing ACT’s activities which requires project planners to consider ‘privacy by design’ and sets out:</p> <ul style="list-style-type: none"> o a process for identifying privacy and information security risks for a given project o how to undertake a PTA to determine whether a full PIA is needed o outline a similar process for conducting information security risk assessments. 	

Rec implemented (✓-Yes, X-No, Partial)	Measures implemented by Housing ACT since 2018	TPP	Residual privacy risks	2021 assessment recommendations to mitigate residual privacy risks	2021 assessment suggestions for privacy best practice
2018 Recommendation 8 Housing ACT should improve ICT security by: <ul style="list-style-type: none"> • creating and maintaining an information asset register • considering updating its version of Homenet to a supported version as soon as practicable • implementing measures to improve the security for personal information transmitted and received via email. 					
Partial	<p>Housing ACT advised that it has not created an information asset register or deployed any other method for tracking Housing ACT's information holdings. Housing ACT staff were uncertain as to what personal information is stored on the G: Drive. The OAIC was advised that staff in some instances may create spreadsheets that contain personal information (extracted from Homenet or hardcopy client files) to assist with their duties and save them on the shared drive. It is not clear how many of these files are deleted once a staff member has completed their work and how many are left on the G: Drive. These files could contain significant volumes of personal and sensitive information.</p> <p>Homenet was upgraded in February 2021 to a version which is supported by the vendor through ongoing software updates. As the older version of Homenet did not have the capability to digitise hard copy files, this upgrade was prioritised as part of Housing ACT's aim to digitise its hardcopy records and utilise Homenet as the sole repository of client information. Housing ACT also informed the OAIC that they have implemented a forward program for yearly updates to Homenet.</p> <p>The OAIC did not observe any Housing ACT or CSD policies or procedures for sending personal information via email. However, Housing ACT do send reminder emails to staff on:</p>	11	<p>As was noted in the 2018 assessment, Housing ACT advised that they use unsecured email to conduct much of the communication between staff and clients, especially in relation to clients providing information relevant to their eligibility for housing assistance. Housing ACT do not encourage use of emails in this way though it will be used if it's the client's preferred method of communication. Housing ACT staff also use unsecured email when receiving health and financial information about clients from third parties.</p> <p>These issues surrounding the current use of email use have not been addressed. The OAIC considers there to be a medium privacy risk that Housing ACT has not taken reasonable steps to secure personal information transmitted via email.</p>	<p><u>2021 Recommendation 8</u> – Housing ACT should fully implement 2018 Recommendation 8 by:</p> <ul style="list-style-type: none"> • establishing measures to improve the security for personal information transmitted and received via email, including: <ul style="list-style-type: none"> o developing internal policies or procedures for staff sending personal information via email o developing educational material for clients highlighting the risks associated with sending personal information via email and promoting secure methods for communicating with Housing ACT o where possible, Housing ACT should consider more secure alternatives for communicating with clients, such as via a secure website, over the phone, in person, or using emails with password protected 	<p><u>2021 Suggestion 8</u> - Housing ACT could consider disseminating educational material for clients on email security through a variety of channels such as, in person at the Housing ACT shopfront, on its website and to established tenancy groups on social media platforms.</p>

Rec implemented (✓-Yes, X-No, Partial)	Measures implemented by Housing ACT since 2018	TPP	Residual privacy risks	2021 assessment recommendations to mitigate residual privacy risks	2021 assessment suggestions for privacy best practice
	<ul style="list-style-type: none"> the importance of including dissemination limited markers in emails (indicating access to information in the email should be limited), or when there are attachments not to include attachment passwords in the content of the email. <p>Housing ACT further advised the OAIC that Shared Services handle many elements of ICT security including email security. The OAIC was provided with the 'Acceptable Use of ICT Resources Policy' (dated January 2020) a high-level ACT Government wide policy developed by Shared Services which instructs ACT Public Service employees and contractors in the acceptable use of ICT resources. The policy advises that when handling official information, staff must:</p> <ul style="list-style-type: none"> protect it with measures that match the information's value, classification and sensitivity if they need to send classified or sensitive information to outside recipients, they should consult with Shared Services ICT Security for advice on the best way to do so consider whether approved secure communication options including file encryption and encrypted media are needed. <p>Housing ACT advised they are (at the time of the assessment) trialling the use of a secure website to provide housing assistance services. However, as many Housing ACT clients are also vulnerable people, including homeless people with limited or no access to online communication, Housing ACT primarily engages with clients in person at the Housing ACT shopfront which is the preferred method of interaction for most of Housing ACT's clients.</p> <p>Housing ACT advised that it provides general information and makes important announcements to clients through digital channels, including sending</p>			<p>attachments to send personal information.</p> <ul style="list-style-type: none"> undertaking some basic information asset management by developing and maintaining a list or register which provides a high-level description of the types of and location of personal information it handles. 	

Rec implemented (✓-Yes, X-No, Partial)	Measures implemented by Housing ACT since 2018	TPP	Residual privacy risks	2021 assessment recommendations to mitigate residual privacy risks	2021 assessment suggestions for privacy best practice
	communications to tenancy groups established on social media platforms and run by clients who act as representatives of the cohort.				
2018 Recommendation 9 Housing ACT should implement comprehensive audit logging in relation to electronic systems that contain personal information as soon as practicable.					
✓	<p>Housing Act advised that it has implemented this recommendation and that all of its electronic systems used to handle personal information have audit logging capability. The OAIC was advised that:</p> <ul style="list-style-type: none"> Homenet has different levels of audit logging capability. At the time of the assessment, Housing ACT was conducting tests to determine which level of audit logging to apply as more targeted audit logging can impact the performance of the system. Housing ACT further advised that audit logs are reviewed on a quarterly basis for H-drive, Shared Services need approval from the staff member to monitor content as it is the staff member's personal storage area. Shared Services can monitor access at the folder level but not at the file level. They can also monitor the volume of files in that drive. 	11	N/A	N/A	N/A
2018 Recommendation 10 Housing ACT should consider reviewing its current physical security measures concerning hardcopy client files and consider better tracking, auditing and monitoring of access to its hardcopy client files, especially files which have been taken out of the hardcopy storage rooms for extended periods of time. This review should also consider the development of a physical security policy around the storage of hardcopy personal information.					
X	Housing ACT has finalised some policies since the 2018 assessment such as CSD's 'Records, Information and Data Management Policy Records Management Program' dated June 2018 which was provided to the OAIC as its response to 2018 Recommendation 10. This policy applies to all of CSD including Housing ACT and contains some high-level governance on the handling	11	During this assessment, Housing ACT advised that despite recent efforts at digitisation and a drive to place all client information on Homenet, there is still a heavy reliance on physical records.	<u>2021 Recommendation 9</u> - Housing ACT should implement 2018 recommendation 10 and review its current physical security measures concerning hardcopy client files. This review should then inform the development of a Housing ACT	None

Rec implemented (✓-Yes, X-No, Partial)	Measures implemented by Housing ACT since 2018	TPP	Residual privacy risks	2021 assessment recommendations to mitigate residual privacy risks	2021 assessment suggestions for privacy best practice
	<p>of data and records. However, it does not cover operational and procedural issues in detail nor does it consider the unique information handling practices of Housing ACT with respect hardcopy client files.</p> <p>The policy refers to the ‘Records, Information and Data Management Procedures’ which detail the way in which staff – including volunteers, contractors and consultants – in CSD will create, capture, manage, care for, keep and access records, information and data. This document may address the issues referred to in the 2018 assessment, but the OAIC was not provided with this document.</p> <p>From interviews with Housing ACT staff, it was unclear whether a review of physical security measures concerning Housing ACT’s hardcopy files was undertaken and whether this policy was informed by this review.</p> <p>In addition, Housing ACT advised that due to the COVID-19 pandemic, Housing ACT implemented changes regarding the handling of physical files. New procedures were introduced which stated that physical hardcopy files could not be taken offsite. Due to the need for staff to work remotely, Housing ACT issued laptops to staff and digitised specific records when staff requested that they needed to access them for their work. These procedures were communicated to staff via email, verbally through line managers and on the CSD intranet but have not been formalised and documented as a regular procedure.</p> <p>The OAIC was advised that procedures for the handling of personal information are still largely communicated informally by staff and managers.</p>		<p>Therefore, the handling of hard copy files remains an ongoing issue.</p> <p>Housing ACT has limited measures in place, in particular documented policies and procedures, to govern access to personal and sensitive information within hardcopy client files held in hardcopy storage rooms. This raises a medium privacy risk of unauthorised access to personal and sensitive information.</p>	<p>physical security policy containing procedures for the handling and storing of hardcopy personal information. The policy should:</p> <ul style="list-style-type: none"> include hard copy file handling procedures developed in response to the COVID-19 pandemic reside within CSD’s records management framework though be specific to Housing ACT’s activities and reflect the unique information handling practices of Housing ACT in relation to hard copy physical files. 	

