



Information Security Assessment for Electronic Voting and Counting System (EVACS)

Version 0.1

Published 14/08/2023

Contents

1	Introduction.....	3
1.1	Purpose.....	3
1.2	Background.....	3
1.3	Scope	5
1.4	Audience.....	5
2	Information Assets	6
2.2	Individual Records	7
2.3	Aggregate Records	7
3	Official Information Identification.....	9
4	Information Security Assessment.....	10
	Privacy Assessment Steps.....	10
	Information Classification Assessment	10
4.1	PIA Threshold Assessment (PTA).....	11
4.2	Data Matching	14
5	Privacy Impact Assessment	15
5.1	Sensitive Information	15
5.2	Territory Privacy Principles.....	16
6	Information Classification Assessment	21
6.1	System Information Classification	21
7.	Records management	22
8.	Approvals.....	23
	Appendix A: OFFICIAL Information Identification Flowchart	24
	Appendix B: ISA process flowchart.....	25
	Appendix C: Information Classification Assistance	26
	Actions for Classified Information with a Protective Marking	26

1 Introduction

1.1 Purpose

This document provides ACT Government data owners with two stages to assist the determination of the information security requirements of an ICT system (including cloud services):

- Privacy Impact Assessment - Threshold Assessment (PTA) and Privacy Impact Assessment (PIA)
- Information Security Assessment

The approach to the assessment of information security recommended in this document is modelled on the *Information Privacy Act (ACT) 2014*. This approach is recommended by the Office of the Australian Information Commissioner (OAIC) when assessing a Public Sector body's compliance under the Information Privacy Act [Guide to securing personal information](#), and related [Guide to undertaking privacy impact assessments](#). However, it cannot encompass all legislation with an enactment of secrecy that Directorates must respond to, such as:

- Health records falling under the *Health Records (Privacy and Access) Act 1997*

When handling information of this nature or under other legislation, Directorates must consult with their own legal advisors or the ACT Government Solicitors Office (GSO).

When completed and authorised, attach the assessments to any security risk assessment (High or Low Assurance) or Data Release request associated with Electronic Voting and Counting System (EVACS).

This document will help you do the following:

1. Identify what specific data is in the solution
2. Identify if the information is OFFICIAL or UNOFFICIAL
3. Identify if OFFICIAL information requires protective marking with an Information Management Marker (IMM)
4. Identify if Personal Information (PI) or Personal Health Information (PHI) is present
5. Identify any security measures taken
6. Identify links for data sharing between other solutions, systems, software, and agencies
7. Identify current record management practices
8. Acknowledgement and approval of this document by delegate.

1.2 Background

ICT Security has provided an interpretation of the ACT Information Security Guidelines in its Security Plan template since 2011. This document provides an updated approach which can be applied to any ICT system, not just those meeting the criteria for a Security Plan. The approach has the flexibility to also apply to data release requests.

Personal Information

What is Personal Information (PI)? PI is defined by the *Information Privacy Act 2014*, as meaning:

... 'information or an opinion about an identified individual, or an individual who is reasonably identifiable; whether the information or opinion is true or not, and whether the information or opinion is recorded in a material form or not'.

Common examples are an individual's name, signature, email address, home address, telephone number, date of birth, bank account details, employment details and commentary or opinion about a person.

ACT public sector agencies are responsible and accountable for the personal information (PI)¹ they collect, hold, store, use and disclose, even when the information is held by external service providers or contractors operating in Australia or overseas.

Health Information

For clinical systems, the handling personal health information (PHI)², the *Health Records (Privacy and Access) Act 1997* may be a consideration, in addition to the *Information Privacy Act*. However, given that health information requires a high standard of care and has specific legislation that governs its control, you should indicate how you are going to comply with the legislation in your assessment.

The ISA does not provide a detailed approach to handling PFI, however it may be useful to still model that assessment using the same approach as for the Information Privacy Act.

Privacy Impact Assessment - Threshold Assessments (PTAs)

The PTA will assist you to:

- determine if a full PIA is required;
- identify if other legislation is relevant to the handling of your data (e.g. s4, *Health Records (Privacy and Access) Act 1997*) and what, if any, additional steps or information handling or security requirements are needed; and
- and identify what other security matters may still apply i.e. any protected security classification needed (OFFICIAL: Sensitive – Personal Privacy, CABINET, etc) in order to protect the information (in addition to any IMM that may also apply).

It is best privacy practice to undertake a PTA when:

- undertaking a new project or business activity that collects personal or sensitive information, and
- when making changes to the way in which personal and sensitive information is collected, used or disclosed, stored and secured in existing projects or business activities.

Privacy Impact Assessments (PIAs)

A PIA is a systematic assessment of a project that identifies:

- whether the proposed treatment of personal information is compliant with the Information Privacy Act and Territory Privacy Principles (TPPs);
- the impact the project might have on the privacy of individuals; and
- sets out recommendations for managing, minimising or eliminating that impact.

¹ See the [Privacy in the ACT](#) section of the OAIC website for more information.

² Personal Health Information, of a consumer, means any personal information, whether or not recorded in a health record:

- Relating to the health, an illness or a disability of the consumer; or
- Collected by a health service provider in relation to the health, an illness or a disability of the consumer.

[s4, *Health Records (Privacy and Access) Act 1997*]

A PIA is more than a simple compliance checklist. It should ‘tell the full story’ of a project from a privacy perspective, going beyond compliance to also consider the broader privacy implications and risks, including whether the planned uses of personal information in the project will be acceptable to the community.

A large part of a project’s success will depend on whether it meets legislative privacy requirements and community privacy expectations. Privacy issues that are not properly addressed can impact on the community’s trust in an organisation or agency and undermine the project’s success.

To be effective, a PIA should be undertaken early enough in the development of a project that it is still possible to influence the project design or, if there are significant negative privacy impacts, reconsider proceeding with the project. Making a PIA an integral part of a project from the beginning means that you can identify any privacy risks early in the project and consider alternative, less privacy-intrusive practices during development, rather than later in the project when changes will be much more difficult and costly to implement.

1.3 Scope

An Information Security Assessment should be performed for all initiatives with ICT systems (including cloud services) that handle official Australian or ACT Government information, particularly those that form part of an ICT solution such as corporate applications or cloud services.

1.4 Audience

This self-assessment template should be completed by staff who are responsible for official information including but not limited to:

- Business system owners (SES-level executive with delegation to approve this assessment);
- Information custodians/data stewards;
- System managers;
- Project managers; and
- Embedded ICT managers.

2 Information Assets

Describe the fields of information that will be collected (e.g. are you collecting financial details; simply describing a process with the tool; collecting project information; storing attachments)

Using the table below, describe:

- the information assets;
- the information consumers;
- the intention to expose the information (e.g. to business unit only; whole directorate; will it be made public?)
- will consumers be able to access information themselves or will they be restricted to certain records?

Table 1: Information Assets

Information Assets Overview (describe in detail):	
Brief description of the project.	Provide description: Electronic Voting and Counting system.
What is the general purpose for which the information will be collected, used and disclosed?	Provide description: Information is collected in order to create an election in the system and then capture and count votes for ACT elections
What fields of information in the system are included? (list them)	Please list: Candidate names, party names, polling place names, vote preference data <i>Note: A 'field' is an area, option or flag in a form, or an answer that is required from an individual or organisation. These can sometimes be Personal Information, and sometimes are generic information. These are sometimes shared or generated from other systems. Please list all you think may apply.</i>
Authority under which personal information is collected³	<i>Who initially requested this system be created/procured and the data recorded/stored?</i> Briefly Describe: ACT Electoral Commission

³ Typically the business owner, e.g. the Director-General or CEO of the agency.

2.2 Individual Records

Individual records are any records the relate to an individual. This can be a complete or partial record like a contact card, a customer response, or a health record.

Table 2: Individual Records Table

1. Individual records	
1.1. Select all that apply to Electronic Voting and Counting System (EVACS):	<input checked="" type="checkbox"/> Individual records can be accessed by customers and users. <input type="checkbox"/> Individual records can be accessed only by users. <input type="checkbox"/> Individual records can be accessed by another system or solution. <input checked="" type="checkbox"/> Other stakeholders can access individual records (describe): <p style="margin-left: 20px;">Candidate and party names are public information. This same information is made public and accessible by the system to both users and customers.</p> <p style="margin-left: 20px;">Vote preference data is made public after the event but the data is not identifiable to the associated voter.</p>

2.3 Aggregate Records

Aggregate information is a collection of individual records. These can be partial or whole, for example, an extract of staff records from Chris21.

Aggregate data can also refer to a database that is used to run reports or statistics. For example, a database administrator with access to vehicle records in REGO, or a data analyst with access to datasets in a Data Lake.

Table 3: Aggregate Records Table

1. Aggregated/reporting data for Electronic Voting and Counting System (EVACS)	
1.1. Can reports or aggregate data be exported?	<input checked="" type="checkbox"/> Yes, Reports can be exported in the following ways): <ul style="list-style-type: none"> <input checked="" type="checkbox"/> To another system <input checked="" type="checkbox"/> As a PDF <input checked="" type="checkbox"/> As a spreadsheet <input type="checkbox"/> In an automated report <input type="checkbox"/> Via email to a user <input type="checkbox"/> Via email to a customer <input type="checkbox"/> Downloaded to a device <input type="checkbox"/> Other ways: Click or tap here to enter text. <input type="checkbox"/> Other: <p style="margin-left: 20px;">Click or tap here to enter text.</p> <input type="checkbox"/> No. No aggregate data cannot be exported or transferred from the system.

<p>1.2. Can users create reports?</p>	<p><input checked="" type="checkbox"/> Yes, some or all users can create reports based on aggregate data (beyond individual records). These reports:</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> include any or ALL fields with no restrictions. <input type="checkbox"/> are restricted to specific fields or records listed below: List: Click or tap here to enter text. <input type="checkbox"/> can be run to include any or ALL records in the system. <input type="checkbox"/> can be run on only a restricted number of records described below: <ul style="list-style-type: none"> <input type="checkbox"/> Customers are able to create reports based on their own records <input type="checkbox"/> Other (describe): Click or tap here to enter text. <p><input type="checkbox"/> Yes, some or all users can create reports with the following parameters: Click or tap here to enter text.</p> <p><input type="checkbox"/> No, users cannot create any reports based on aggregate data.</p>
<p>1.3. Describe any other functionality for handling data Electronic Voting and Counting System (EVACS) provides to users, customers, and/or other stakeholders:</p>	<ul style="list-style-type: none"> <input type="checkbox"/> Records are shared with other systems within ACT Government (Please also review Data Matching) <input type="checkbox"/> Records can be downloaded by other agencies (Please review Data Matching . <input checked="" type="checkbox"/> There is no other functionality for handling system data. <input type="checkbox"/> Other: Click or tap here to enter text.

3 Official Information Identification

Official Australian or ACT Government information⁴ is information owned, produced, stored or manipulated by a:

- Minister in their appointed capacity;
- Employee in the course of their employment; or
- Directorate, agency or organisation.

Official ACT Government Information is subject to the *Territory Records Act (2002)*.

The following statements will help determine if your system contains official Australian or ACT Government information (select all that apply):

Table 4: Statements to determine if your system contains official information

<input type="checkbox"/>	<p>This information represents a view of the Australian or ACT Government.</p> <p>I WILL need to complete and seek approval for the Information Security Assessment Sections (including the PIA Threshold Assessment) and Records Management sections of this document.</p>
<input checked="" type="checkbox"/>	<p>This information relates to Australian or ACT Government official business.</p> <p>I WILL need to complete and seek approval for the Information Security Assessment Sections (including the PIA Threshold Assessment) and Records Management sections of this document.</p>
<input checked="" type="checkbox"/>	<p>Unauthorised disclosure of this information could cause some form of damage to Australia’s national security, the Australian or ACT Government, commercial entities, or members of the public.</p> <p>I WILL need to complete and seek approval for the Information Security Assessment Sections (including the PIA Threshold Assessment) and Records Management sections of this document.</p>
<p>If you did not select any of the checkboxes, the information is considered UNOFFICIAL. The ACT Government does not require UNOFFICIAL information to have any protective marking.</p>	
<input type="checkbox"/>	<p>I have reviewed the legislation and information above and none of these are relevant to my system. I have asessed this system to be UNOFFICIAL.</p> <p>I WILL need to complete and seek approval for the Information Security Assessment Sections (including the PIA Threshold Assessment) to see if a Personal Impact Assesment is required, AND I WILL complete and review the Information Classification Assessment and Records Management Section of this document.</p>

⁴ See [Information Security Guidelines \(2017\)](#) for more information.

4 Information Security Assessment

An Information Security Assessment is performed on official Australian or ACT Government information and consists of two stages:

1. Privacy Assessment
2. Information Classification Assessment.

Privacy Assessment Steps

This Privacy Assessment has two parts. It starts with a PIA Threshold Assessment to determine if a Privacy Impact Assessment (PIA) needs to be conducted. Performing a PTA will help directorates determine if a PIA is required for a new project or if a new PIA needs to be carried out.

Not all processes will require a full PIA, and some may only require a brief PIA where there is little personal information being handled, or only minor changes to information handling practices.

The answer should also consider the risk of de-identified information becoming personal information if it can be matched with another dataset (or publicly available information), enabling individuals to be identified.

Information Classification Assessment

The Information Classification Assessment assists directorates in classifying their information and determining whether the information requires protective marking with an Information Management Marker (IMM).

4.1 PIA Threshold Assessment (PTA)

Table 5: PIA Threshold Assessment Decision

1. System Background	
1.1 Has a PIA been undertaken before?	<input type="checkbox"/> The PIA I have for this system is current AND I am able to provide a copy of it. <i>If you ticked this you do not need to complete this document. Please provide the previous PIA.</i>
<i>Tip: Answer and continue working down through the table unless you reach the bottom of the table OR have selected an answer that says to “skip” to a specific section.</i>	<input type="checkbox"/> Yes, one was previously carried out HOWEVER : <ul style="list-style-type: none"> <input type="checkbox"/> we no longer have a copy <input type="checkbox"/> there has been a change to legislation. <input type="checkbox"/> there has been a change to system functionality. <input type="checkbox"/> there are any changes to the information collected. <input type="checkbox"/> there has been a change to how the collected information will be used. <input type="checkbox"/> there has been a change to the environment in which the system operates. <input type="checkbox"/> there have been other changes and so needs updating. <input checked="" type="checkbox"/> No/I'm not sure.
1.2 Is this a new system?	<input type="checkbox"/> Yes, this system is new and/or replacing an old system. <i>If 'Yes': Skip to "2. Personal Information Description"</i>
1.3 Is this system undergoing changes in how personal information is being handled?	<input checked="" type="checkbox"/> No, nothing will change the way we are currently handling personal information. <input type="checkbox"/> No, there are changes and nothing will change the way we handle personal information BUT there are changes to how the system handles other kinds of information/data: Click or tap here to enter text. <input type="checkbox"/> Yes, it will modify an existing system in the following ways: Click or tap here to enter text.

2 Personal Information & Sensitivity Identification

2.1 Does this project collect any of the Personal Information?

Tip: See Glossary for definitions and help on Personal Information, Health Information, and Health Records.

*NOTE: If you tick any of these, you **must** complete the section on Sensitive Information, as well as complete the PIA.*

- Yes, it does as it collects:
 - Name, Home Address, AND/OR Contact phone number
 - Date of Birth
 - Health Information, PHI (e.g. dietary or allergy)
 - Emergency contact information
 - Employment details/Employee number
 - Information on race, religion, ethnicity, or identity
 - Other:
 - Click or tap here to enter text.

- No, it does not collect any of the above or any other Personal Information.
 - If 'No': Skip to "3. Conclusion" and finish the table.*

2.2 Identify any possible sensitivities of the personal information.

2.3 Note: Sensitivity may depend on the context of the individuals.

- This information is about children
- This information is about "at risk" people/group
- This information is a full/partial health record
- Other (please describe):
 - Click or tap here to enter text.

- No sensitivities present

2.4 What are the current privacy risk mitigations and practices in place?

- Provide a brief explanation of practices, training, and security implementations:
- We provide all users with training on best practices and their obligations regarding privacy.
 - All Users receive training on basic security.
 - Other:
 - Click or tap here to enter text.

3 Conclusion	
3.1 Based on the information above you conclude that:	<input checked="" type="checkbox"/> I have selected "NO" for question 2.1 and do <i>not</i> need to complete a PIA. I will complete the following Table Metadata section and will seek Approval from my delegate for this document. <input type="checkbox"/> I have answered 'YES' to at least one (1) of the questions above in regards to personal information and will require a Privacy Impact Assessment .
3.2 Does the project involve data matching of more than 5000 records annually?⁵	<input type="checkbox"/> Yes, and I will review the Data Matching section and create a Data Matching protocol. <input type="checkbox"/> No, the project involves data matching but at less than 5000 records annually. <input type="checkbox"/> No, this system does not share or match data with any other solution <input type="checkbox"/> I am unsure what this is (Please see Data Matching)
4 Metadata for this table	
4.1 Based on this threshold assessment, should a PIA be undertaken?	<input checked="" type="checkbox"/> No , the information I am proposing to collect, store, use or disclose does not include or contain personal information, and does not change an existing information handling practice. I do not need to undertake a PIA. Next steps: <ol style="list-style-type: none"> 1 Complete the Records management section 2 Complete Information Classification Assessment 3 Seek relevant Approvals 4 Keep this document as a record of the decision. <input type="checkbox"/> Yes , the information I am proposing to collect, store, use, or disclose does contain personal information and I will need to complete a Privacy Impact Assessment. Next steps: <ol style="list-style-type: none"> 1 Complete the Privacy Impact Assessment 2 Complete the Records management section 3 Complete Information Classification Assessment 4 Seek relevant Approvals 5 Keep this document as a record of the decision.
4.2 Name of person or team responsible for completing this privacy threshold assessment.	Jiv Sekhon, Elections Operations Manager
4.3 Date completed	14/08/2023

⁵ The OAIC provides guidelines around data matching. See the [Government data-matching](#) section of the OAIC website for more information.

4.2 Data Matching

Data matching refers to the sharing of data between multiple systems to correlate and cross-reference information. This can involve Personal Information and Identifiable Information as well as general sharing of de-identified data for reporting or statistics.

Other forms of data matching may include: exporting a copy of the database or manually extracting data to store it elsewhere for data matching purposes.

If the personal information is being collected for a data matching purpose and the number of records matched is over 5000 annually, either in one bulk data transfer or cumulatively via several smaller data transactions, then you will need to consider if you should prepare a Data Matching Protocol.

Special note: If the data matching exercise is only a pilot, and if you are proposing to ‘use/disclose’ the personal information matched to take an administrative or punitive action, then natural justice must be afforded and the individuals affected provided with sufficient and specific notice (even after the collection).

Table 6: Data Matching

Please complete the following by ticking all that apply	
<input type="checkbox"/>	This solution shares, matches, and/or uses information from another system as identified below:
	<input type="checkbox"/> This solution matches user data from an HR or other system: <ul style="list-style-type: none"> <input type="checkbox"/> Chris21 <input type="checkbox"/> Oracle eBusiness Suite <input type="checkbox"/> Other: Click or tap here to enter text.
	<input type="checkbox"/> This solution shares information to another system for data matching: <ul style="list-style-type: none"> <input type="checkbox"/> Other Click or tap here to enter text.
	<input type="checkbox"/> This solution uses information that is shared from another system: Click or tap here to enter text.
<input type="checkbox"/>	Other: Click or tap here to enter text.
<input checked="" type="checkbox"/>	This solution does NOT share or draw information from any other system.

5 Privacy Impact Assessment

The *Information Privacy Act (ACT) 2014* applies to ACT Public Sector Agencies and gives a set of 13 Territory Privacy Principles (TPPs) which must be adhered to by Directorates with business systems that handle personal information.

If a PTA has determined that a Privacy Impact Assessment (PIA)⁶ should be completed to determine which, if any, of the below Sensitive Information criteria and TPPs apply.

The format below is not prescriptive but is an example of how a system specific PIA might be performed. Directorates are encouraged to seek privacy advice from legal advisors and, if required, engage external consultants to perform a PIA.

PIAs are living documents and can be updated, or regularly reviewed to ensure a projects privacy obligations are being met throughout the life of a project or program.

A PIA will not require review unless a change occurs to:

- legislation regarding the handling or kind of personal information to be collected, used or disclosed;
- system functionality;
- the kind of personal information collected
- the use or disclosure of information; or
- change in the environment in which the information is used.

5.1 Sensitive Information

‘Sensitive information’ is a subset of personal information. It is considered present if it meets at least one of the following criteria.

Table 7: Sensitive Information checklist

<input type="checkbox"/>	Information or an opinion (that is also personal information or information that indicates) about an individual's:
	<input type="checkbox"/> racial or ethnic origin
	<input type="checkbox"/> political opinions
	<input type="checkbox"/> membership of a political association
	<input type="checkbox"/> religious beliefs or affiliations
	<input type="checkbox"/> philosophical beliefs
	<input type="checkbox"/> membership of a professional or trade association
	<input type="checkbox"/> membership of a trade union; or
	<input type="checkbox"/> sexual orientation or practices, or
	<input type="checkbox"/> criminal record
<input type="checkbox"/>	Genetic information about the individuals
<input type="checkbox"/>	Biometric information about the individual that is to be used for the purpose of automated biometric verification or biometric identification; or a biometric template that relates to the individual.
<input type="checkbox"/>	Other (describe): Click or tap here to enter text. NOTE: Health information is governed by its own Act and should be given additional considerations and protects similar to ‘sensitive information’.

⁶ See the OAIC [Guide to undertaking privacy impact assessments](#)

Inappropriate handling of sensitive information can have adverse consequences for an individual or those associated with the individual. Sensitive information consequently needs a higher level of protection under the TPPs than other personal information (see TPP 11).

5.2 Territory Privacy Principles

This PIA will assist with identifying how compliant Electronic Voting and Counting System (EVACS) is with the applicable TPPs⁷.

Open and Transparent Management of Personal Information (TPP 1)

<input type="checkbox"/>	The system provides customers with a privacy statement explaining how their information will be used.
<input type="checkbox"/>	The system provides customers with a link to an approved directorate Privacy Policy.
<input type="checkbox"/>	The system provides customers with a mechanism for contacting the directorate Privacy Officer for questions or complaints.
<input type="checkbox"/>	Other (describe): Click or tap here to enter text.
<input type="checkbox"/>	N/A, this system does not collect PI.

Anonymity and Pseudonymity (TPP 2)

The ways in which individuals can interact with the system without identifying themselves or by using pseudonyms are (select all that apply):

<input type="checkbox"/>	N/A This Principle is not applicable, because we are required by law to deal with individuals who have identified themselves.
<input type="checkbox"/>	This Principle is not applicable, because it is impracticable to deal with individuals who have not identified themselves or who have used a pseudonym.
<input type="checkbox"/>	The system provides the option of leaving contact details if the individual wants us to contact them, or to not leave any contact details, if they do not want us to get back to them.
<input type="checkbox"/>	Other (describe): Click or tap here to enter text.

Collection of Solicited Information (TPP 3), Quality (Accuracy and Completeness) of Personal Information (TPP 10), and Correction of Personal Information (TPP 13)

The procedures used to ensure that personal information collected is kept accurate, up-to-date and complete are (select all that apply):

<input type="checkbox"/>	Every time a customer presents at the counter, staff ask for confirmation of data: name, address, phone number etc.
<input type="checkbox"/>	The only personal data in the system is mastered from another system and downloaded from this system whenever a new record (requiring personal information) is created.
<input type="checkbox"/>	At the counter, customers are requested to verify current data on the system.

⁷ See the [Territory Privacy Principles](#) section of the OAIC website for more information.

<input type="checkbox"/>	Personal information is stored against a public enquiry or against an accident as a “point in time” record i.e. the information stored is intended to be an accurate record as at the time of the request/incident, and not intended to be an on-going reflection of the current attributes of the person involved.
<input type="checkbox"/>	Customers/users of this system are responsible for keeping their information up to date by submitting change of circumstances forms/calling the counter/updating from the account information page/etc
<input type="checkbox"/>	Other (describe): Click or tap here to enter text.
<input type="checkbox"/>	N/A

Dealing with Unsolicited Personal Information (TPP 4)

The procedures used to destroy or de-identify unsolicited personal information are (select all that apply):

<input type="checkbox"/>	The system has no free text fields so there is no scope to enter (and record) unsolicited personal information.
<input type="checkbox"/>	When a person fills in a form on the system, we have clearly marked response boxes, to minimise the chance that a person will enter information we do not need.
<input type="checkbox"/>	We have a written policy that tells our staff members that if they find an individual has entered unrequested personal information the staff member is to refer that to the supervisor.
<input type="checkbox"/>	The supervisor will either delete or redact the information if it is not the sort of information that the Directorate ever collects, if it is lawful to do so under the Territory Records Act, and make a log entry to record that he/she has edited the record.
<input type="checkbox"/>	The supervisor will leave the information untouched if it is the sort of information that the Directory does collect and if it is part of a Territory Record.
<input type="checkbox"/>	Other (describe): Click or tap here to enter text.
<input type="checkbox"/>	N/A

Notification of the Collection of Personal Information (TPP 5)

The procedures used to notify individuals that their personal information has been collected are (select all that apply):

<input type="checkbox"/>	The system requires a customer to acknowledge that they have read our “Territory Privacy Principle 5 - Notification of Collection of Personal Information” (which directs the individual to our Privacy Policy that explains how we collect, use, share and store personal information, and how a user may access/correct it).
<input type="checkbox"/>	A standard message is played to all callers: “your call may be recorded for training purposes”
<input type="checkbox"/>	Other (describe): Click or tap here to enter text.
<input type="checkbox"/>	N/A

Use or Disclosure for the Primary Purpose Collected (TPP 6), Security of Personal Information (TPP 11), and Access to Personal Information (TPP12)

The following procedures ensure that personal information is used for the lawful purpose for which it was collected or the primary purpose of collection (select all that apply):

<input type="checkbox"/>	Regularly instructing all persons with access that they are bound under the <i>Information Privacy Act (ACT) 2014</i> , which forbids unauthorised use, modification or disclosure to parties not entitled to receive it.
<input type="checkbox"/>	Checking that information collected or used complies with the Information Privacy Act or other applicable legislation governing the information i.e. secrecy provisions, or the Health Records (Privacy and Access) Act.
<input type="checkbox"/>	All requests for information are accepted only if they approved by the appropriate delegate. Please note the delegate will differ for some Directorates: <ul style="list-style-type: none"> • If the information belongs to the Health Directorate <ul style="list-style-type: none"> - refer to the Health Directorate policy. • For all other Directorates <ul style="list-style-type: none"> - either the Business System Owner of the system from which the data originated; or - a decision maker under the <i>Freedom of Information Act 2016</i>.
<input type="checkbox"/>	All requests for de-identified information for the purpose of research must be approved by the following. Please note this will differ for some Directorates: <ul style="list-style-type: none"> • If the information belongs to the Health Directorate <ul style="list-style-type: none"> - as per the Health Directorate policy. • For other Directorates (insert positions of delegated data stewards): Click or tap here to enter text.
<input type="checkbox"/>	All Production data used in non-production environments have privacy-related items de-identified. <i>See also: Use or Disclosure of Personal Information in Non-Production Environments (TPP6)</i>
<input type="checkbox"/>	Other (describe): Click or tap here to enter text.
<input type="checkbox"/>	N/A

Use or Disclosure of Personal Information in Non-Production Environments (TPP6)

Personal information is used in the following non-Production environments^{8,9}:

<input type="checkbox"/>	No personal information is used in non-Production environments.
<input type="checkbox"/>	PI is used in ACTTST or Training <ul style="list-style-type: none"> <input type="checkbox"/> The Business System Owner approved the use of PI for this secondary purpose (attach written evidence to this Information Security Assessment). <input type="checkbox"/> The target environment is secured to the same standard as ACTGOV, including access control, logging and monitoring, auditing, password and encryption standards.

⁸ **Development and Vendor access to PI**

Advice from the Privacy Commissioner and the Government Solicitor’s Office is that Privacy-related information **SHALL NOT** be used in its raw form in a Development environment.

If production information is to be used in a DEV or vendor environment, then it **MUST** be de-identified (that is: the personal information has been replaced with artificial data from which the identity of the individuals cannot be ascertained). This is a ruling of the ACT Attorney-General. Penalties are described in the Information Privacy Act (ACT) 2014.

⁹ **Test and Training**

<input type="checkbox"/>	PI is used in ACTDEV or any vendor non-Production environment <input type="checkbox"/> The data is de-identified using methods approved by ICT Security before exporting from Production.
<input type="checkbox"/>	Other (describe): Click or tap here to enter text.
<input type="checkbox"/>	N/A

Cross-Border Disclosure of Personal Information (TPP 8)

Data sovereignty is an ongoing concern for ACT Government. Differing legal frameworks and potential inability to enforce contractual terms between the ACT Government, off-shore provider and/or off-shore country where the information is being handled.

The ability of the ACT Government or affected citizens to enforce legislation, public regulations or contract terms to off-shore providers and countries outside of borders of Australia could be limited.

The following procedures ensure that personal information is not disclosed to overseas recipients (select all that apply):

<input type="checkbox"/>	Not applicable. No information held in this application is transmitted abroad.
<input type="checkbox"/>	The Directorate’s intention is that no personal information held in the database will be transmitted/disclosed cross border. Should the need arise, the Directorate will release personal information only to organisations for which the Business System Owner has provided written authorisation after seeking advice of the Directorate’s legal staff.
<input type="checkbox"/>	Other (describe): Click or tap here to enter text.
<input type="checkbox"/>	N/A

Security of Personal Information (Prevention of Unauthorised Use, TPP 11)

The following procedures guard personal information against interference, misuse and loss and unauthorised access, modification and disclosure¹⁰ (select all that apply):

<input type="checkbox"/>	Active monitoring of audit trails, to track activity in the system.
<input type="checkbox"/>	Restricting users of the system to just ACT Government staff - who are vetted and informed of their responsibilities upon employment.
<input type="checkbox"/>	Employing individual usernames and passwords to restrict access to the application.
<input type="checkbox"/>	Employing role-based permissions to restrict read-access and write-access to staff who have a need to see or to change that data.

Production data containing personal data can ONLY be used in a TEST or TRAINING environment if the business owner deems it as an appropriate secondary purpose AND data held in Test is protected from misuse, interference or loss, and from unauthorised access, modification or disclosure.

Production data containing personal data covered under the *Information Privacy Act 2014* can be used in a Test or Training environment only if the business owner explicitly deems it as an appropriate secondary purpose AND data held in Test is protected from misuse, interference or loss, and from unauthorised access, modification or disclosure. (In practice, that means being secured to a comparable standard to that applied in Production). If both conditions are met, the information may be used in Test as the compliance risks have been treated/accepted. If either of the sign offs are missing, then it **SHALL NOT** be used in TEST.

¹⁰ See GSO privacy advice for SSICT managed cloud environments for advice on privacy in cloud environments (AWS, Azure), especially regarding TPP11 considerations on ‘disclosure’.

<input type="checkbox"/>	Access is restricted by way of fixed IP addresses to gain access to the server and username and passwords to gain access to the database. If officers leave their workspace they are required to log out of the system. Physical access to servers is restricted by swipe cards access.
<input type="checkbox"/>	Regularly instructing all persons with access that they are bound by the <i>Information Privacy Act 2014</i> , which forbids unauthorised use, modification, or disclosure to parties not entitled to receive it.
<input type="checkbox"/>	Other (describe): Click or tap here to enter text.
<input type="checkbox"/>	N/A

TPP Conclusion

Based on the above answers, use the following table to show which TPPs apply to Electronic Voting and Counting System (EVACS):

Table 8: Territory Privacy Principles checklist

<input type="checkbox"/>	TPP 1 - open and transparent management of personal information
<input type="checkbox"/>	TPP 2 - anonymity and pseudonymity
<input type="checkbox"/>	TPP 3 - collection of solicited personal information
<input type="checkbox"/>	TPP 4 - dealing with unsolicited personal information
<input type="checkbox"/>	TPP 5 - notification of the collection of personal information
<input type="checkbox"/>	TPP 6 - use or disclosure of personal information
<input type="checkbox"/>	TPP 8 - cross-border disclosure of personal information
<input type="checkbox"/>	TPP 10 - quality of personal information
<input type="checkbox"/>	TPP 11 - security of personal information
<input type="checkbox"/>	TPP 12 - access to personal information
<input type="checkbox"/>	TPP 13 - correction of personal information

6 Information Classification Assessment

6.1 System Information Classification

This process is mandatory for ALL official Australian or ACT Government information regardless of whether a PIA has been performed.

In accordance with the ACT PSPF¹¹, directorates must apply safeguards so that:

- information is classified and labelled with a protective marking as required;
- only authorised people, using approved processes, have access to the information;
- information is only used for its official purpose, retains its content integrity, and is available to satisfy operational requirements; and
- information is properly managed and protected in accordance with the Cyber Security Policy¹².

Before completing the following table

Reference the information you have on your system, how it will be used, and refer to the help section in [Appendix C: Information Classification Assistance](#).

Table 9: Electronic Voting and Counting System (EVACS) Information Classification

Information Classification (Tick all that apply)		
Classification/IMM of Electronic Voting and Counting System (EVACS) ¹³		Impact of unauthorised disclosure
<input checked="" type="checkbox"/>	OFFICIAL	No significant damage to National Security/Government/Commercial/public
<input checked="" type="checkbox"/>	OFFICIAL: Sensitive	Breach other secrecy provisions or enactments. Damage to Government/Commercial/public as determined by directorate
<input type="checkbox"/>	OFFICIAL: Sensitive - Legislative Secrecy	Breach of sensitive audit information
<input type="checkbox"/>	OFFICIAL: Sensitive - Legal Privilege	Breach of legal professional privilege
<input type="checkbox"/>	OFFICIAL: Sensitive - Personal Privacy	Reveal sensitive personal information and breach <i>Information Privacy Act (ACT) 2014</i> . For examples, see Sensitive personal information and Health information
<input type="checkbox"/>	CABINET Caveat	Reveal the deliberations or decisions of Cabinet
<input type="checkbox"/>	Protected	Severe damage to National Security/Government/Commercial/public

¹¹ See [ACT Government Protective Security Policy Framework \(2017\)](#)

¹² See [Cyber Security Policy](#) for more information

¹³ See the [ACT Information Security Guidelines](#) for classification and handling requirements of each IMM.

7. Records management

The Territory Records Act 2002 ¹⁴ requires the Chief Officer of a Directorate to be responsible for the access to and accountability of all corporate records owned by that agency.

If the Chief Officer of an agency at any time loses control of corporate records, then they are in violation of the Territory Records Act.

If a system has a large dataset of personal information, the system owner needs to ensure that the host (whether Shared Services or Cloud Service provider) does not re-use it for other purposes. The ACT Government business needs to be in control of the information including when using third party services. Of further concern is the disposal of records in a cloud arrangement data may remain visible on reallocated/disposed-of data storage devices.

The Territory’s contractual agreement with the Vendor should include terms to require secure reallocation/disposal of resources at the end of life of the service.

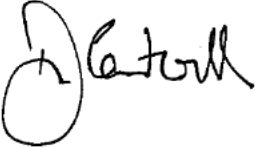
Table 10: Records Management Requirements

Please read the following and tick all that apply.	
<input checked="" type="checkbox"/>	I have read the above and understand our records management obligations.
<input checked="" type="checkbox"/>	The Territory’s contractual agreement with the Vendor include terms to require secure reallocation/disposal of resources at the end of life of the service.
<input type="checkbox"/>	I don’t understand and will contact the Territory Records Office to find out what I need to do to be compliant.

¹⁴ See [Territory Records Act 2002](#)

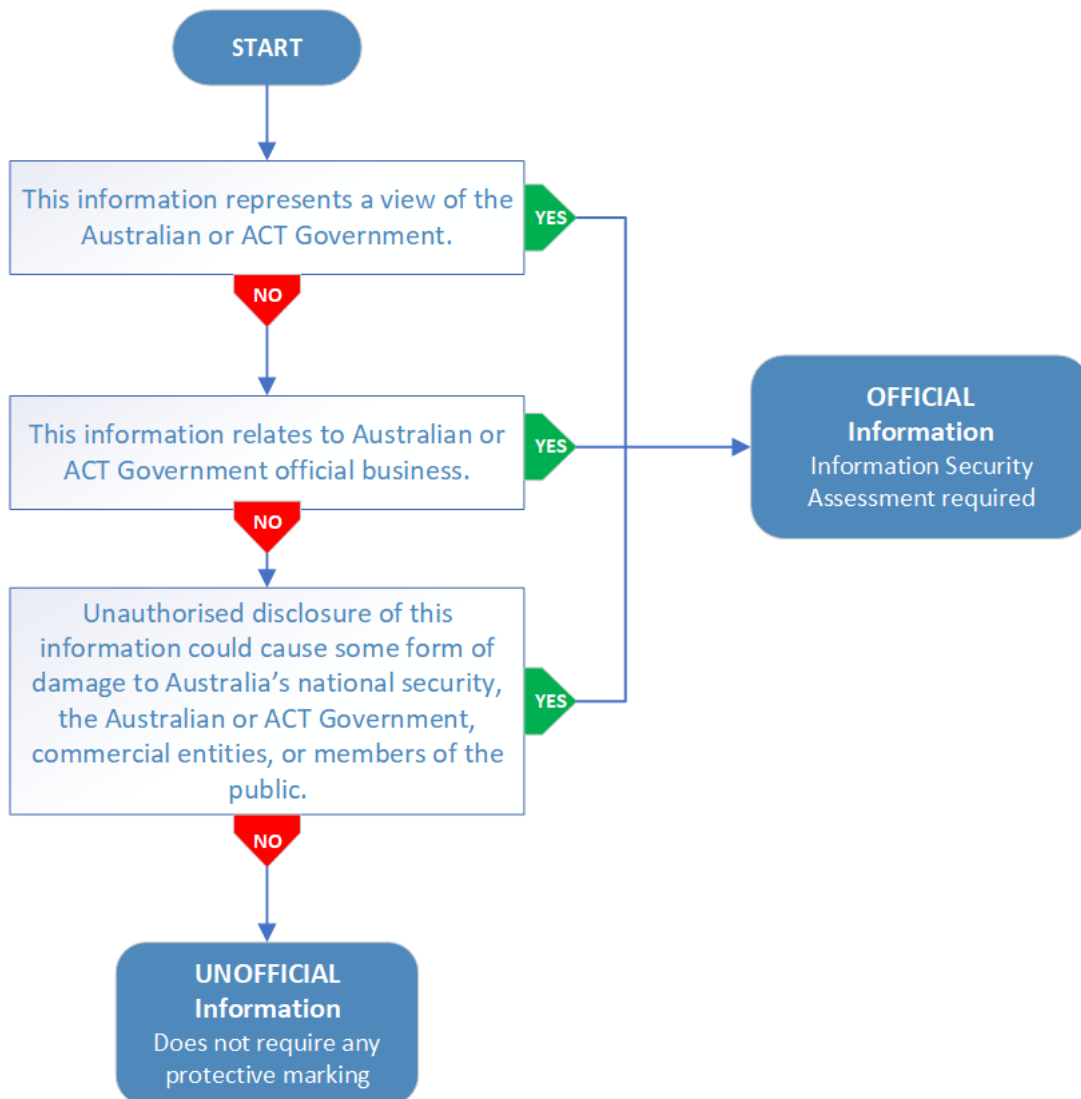
8. Approvals

Table 11: Document approvals

Name of System Manager	Jiv Sekhon	Phone	6205 0046
Name of Business System Owner	Damian Cantwell Electoral Commissioner ACT Government Telephone: 6205 0236 Email:		
Decision	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DECLINE		
Signature of Business System Owner		Date	15/08/2023
Comments			

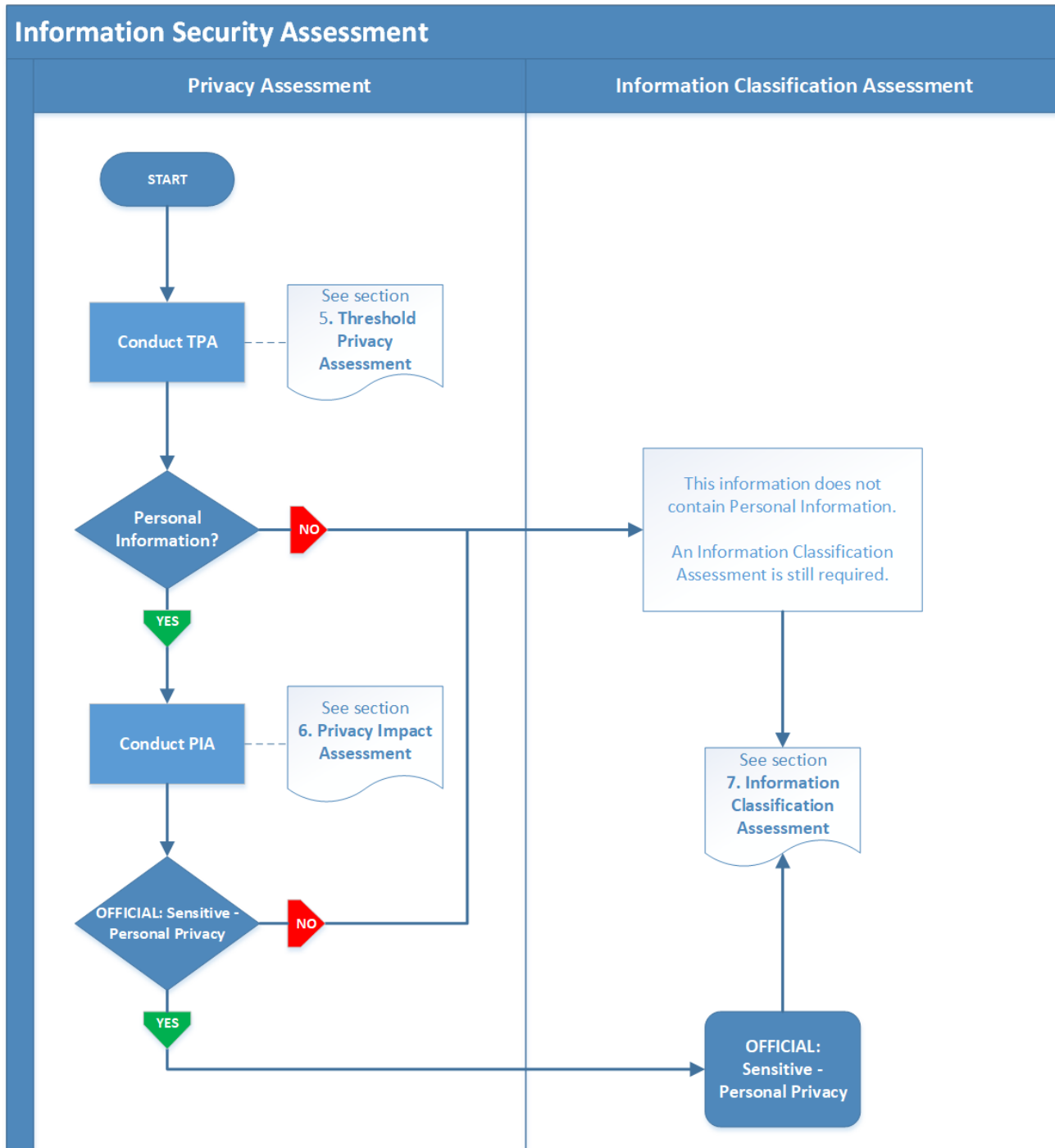
Appendix A: OFFICIAL Information Identification Flowchart

Figure 1: Official information process flow



Appendix B: ISA process flowchart

Figure 2: Information Security Assessment process flow



Appendix C: Information Classification Assistance

Actions for Classified Information with a Protective Marking

The following activities should be carried out for information classified with a protective marking.

IMPORTANT: ICT Security recommends documenting these business activities in a Standard Operating Procedure (SOP) for the system or service.

1. Where feasible, mark the information with the IMM so that consumers of the information understand the security with which it must be handled.
2. Apply the Principle of need-to-know, which requires the restricting of an individual's access to only the information they require to fulfil the duties of their role.
 - a. All ICT systems holding information with a protective marking must force users to authenticate with a unique and attributable identity.
 - b. Authentication must comply with the ACT Government Password Standard.
 - c. Authentication attempts must be logged and periodically audited by the system manager.
3. Apply the Principle of least privilege, which requires that an individual should only be able to access the information and resources they require for legitimate reasons.
 - a. Roles and permissions must be defined within the system and authorised by the system manager in a documented request (electronic or paper).
4. Apply the Principle of separation of duties, which requires that the person who authorises and/or audits user access is not also the person or team who provisions user access.
5. Cyber Security awareness training and understanding of the ICT Acceptable Use Policy to ensure those who handle the information follow the requirements to protect the information appropriately.
6. Extra protective measures such as:
 - a. Those derived from the Cyber Security Policy¹⁵ on a risk assessment basis.
 - b. Typically, the Business System Owner is required to seek strategic security advice from the IT Security Advisor (ITSA), to determine the appropriate security controls.
 - c. Apply the appropriate technical controls around classified documents with a protective marking as per the PSPF Information Security Guidelines¹⁶ including:
 - i. Preparation and Handling.
 - ii. Removal of documents or files.
 - iii. Auditing.
 - iv. Copying, storage and destruction.

¹⁵ See [Cyber Security Policy](#) for more information.

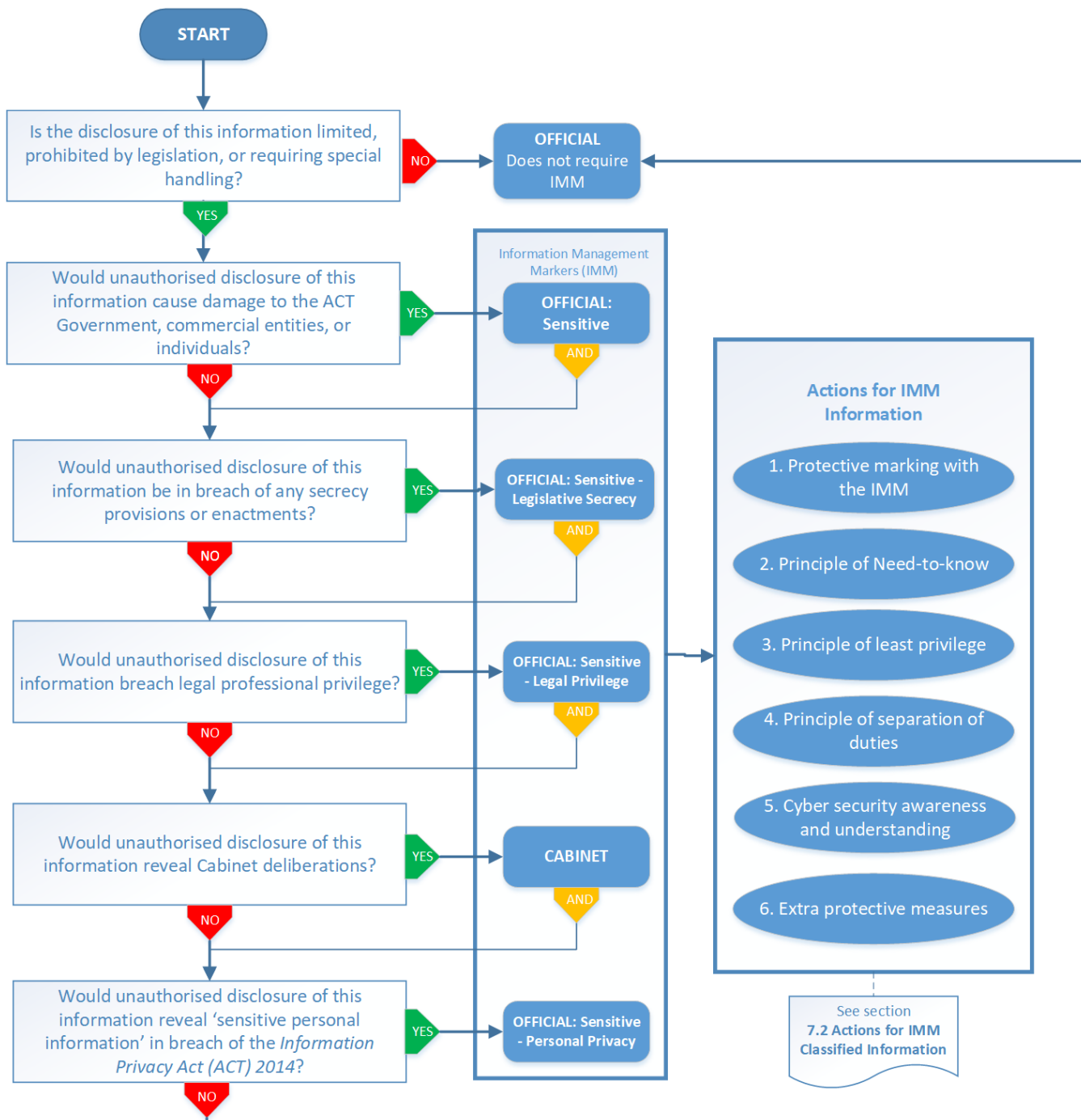
¹⁶ See p14 of the [ACT Government Protect Security Information Security Guidelines \(2017\)](#) for more information.

Mapping of Dissemination Limiting Markers 2014 to Information Management Markers 2020

2014 DLMs	IMMs as of 03 August 2020
UNOFFICIAL*	UNOFFICIAL*
UNCLASSIFIED	OFFICIAL
UNCLASSIFIED For-Official-Use-Only	OFFICIAL: Sensitive
UNCLASSIFIED Sensitive	OFFICIAL: Sensitive - Legislative Secrecy
UNCLASSIFIED Sensitive: Personal	OFFICIAL: Sensitive - Personal Privacy
UNCLASSIFIED Sensitive: Legal	OFFICIAL: Sensitive - Legal Privilege
UNCLASSIFIED Sensitive: Auditor-General	OFFICIAL: Sensitive - Legislative Secrecy
UNCLASSIFIED Sensitive: Cabinet	CABINET Caveat

*Used for personal correspondence, not business systems

Figure 3: Information Classification Assessment process flow



Glossary

Table 12: Glossary

Term	Definition
ACT Government	ACT Government
ACT PSPF	ACT Government Protective Security Policy Framework
IMM	Information Management Marker
ISA	Information Security Assessment
PHI	Personal Health Information
PI	Personal Information
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information Note: Territory and Commonwealth legislation does not use the term 'personally identifiable information' (PII), using instead 'personal information' (PI). For the purpose of this ISA and compliance with legislation, any instances of the term 'PII' should be read as meaning the definition of 'PI' under the legislation.
PTA	PIA Threshold Assessment

Metadata

Table 13: Document metadata

Owner:	Chief Information Security Officer, ACT Government
Document location:	https://actgovernment.sharepoint.com/teams/CyberStrategyandGovernance/Shared Documents/General/Templates/[Client] [System] Information Security Assessment.docx
Review cycle:	This document should be reviewed every 24 months or when significant changes occur in the business, technology or security environment
Document version:	Information Security Assessment version 0.1

Note: This is a *controlled* document. Any documents appearing in paper form are not controlled and should be checked against the WIRE version prior to use.

Document Revisions

Table 14: Document revision history

Version	Published	Amendment details	Author/s	Approval