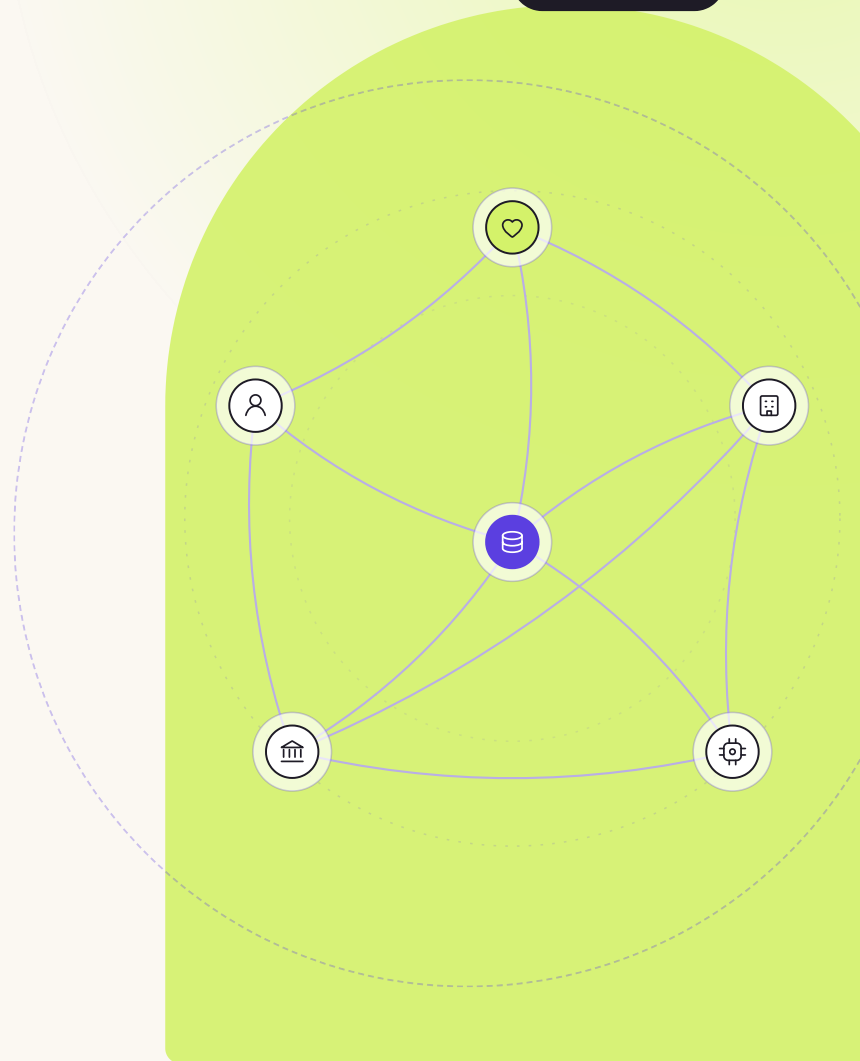




● **TEMPLATE OUTLINE · DATA GOVERNANCE**

Data classification starter

How to design a small, usable classification scheme for a private sector organisation, with the levels, criteria and handling rule headings to work through.

A classification scheme tells staff, in a word or two, how carefully a piece of information must be handled. Done well, it means people do not have to make a fresh judgement every time they save, share or send something. Done badly, it becomes a set of labels nobody applies.

This outline gives you the structure to design your own scheme. It is a starting point, not a finished policy: the levels, criteria and rules must reflect your information, your systems and your obligations.

First, check whether government markings apply to you

The Australian Government uses its own system under the Protective Security Policy Framework (PSPF), administered by the Department of Home Affairs and updated in annual releases. Its protective markings are **OFFICIAL**, **OFFICIAL: Sensitive**, **PROTECTED**, **SECRET** and **TOP SECRET**, with **UNOFFICIAL** used for information that is not part of official duties. Caveats and information management markers can be added in some cases.

The PSPF is mandatory for non-corporate Commonwealth entities. It does not apply to private organisations generally, but suppliers that handle Commonwealth information can be required by contract or direction to apply the relevant controls. If you supply government:

- ☐ Find out which markings the information you receive carries, and what your contract requires.
- ☐ Do not invent your own label that looks like a government marking. Keep your scheme visibly distinct.
- ☐ Map how government-marked information will be handled inside your systems, separately from your own levels.

State governments have their own frameworks, so check those too if you work with state agencies.

Design principles

- **Keep it small.** Three or four levels is usually enough. More levels create hesitation and inconsistent labelling.
- **Classify by impact.** Ask what would happen if the information were disclosed, altered or lost, not who created it.
- **Make the default sensible.** Most information should land on one everyday level without thought.
- **Tie each level to rules.** A label that does not change how information is handled is decoration.
- **Remember personal information.** The Privacy Act obligations under APP 11 apply whatever label you choose. Classification is one way to show the reasonable steps you take.

Suggested level structure

Use your own names. Common patterns are below, with the questions that should decide each level.

Level 1: Public

- Has it been approved for release, or is it already published?
- Would disclosure cause no harm at all?

Level 2: Internal

- Is it routine business information intended for staff and trusted contractors?
- Would disclosure cause minor inconvenience or embarrassment, but no real harm to people or the business?

Level 3: Confidential

- Does it include personal information, client information or commercially sensitive material?
- Could disclosure cause harm to individuals, breach a contract, or damage the business?
- Is access limited to people who need it for their role?

Level 4: Restricted (optional)

- Does it include sensitive information (such as health information), identity documents, financial account details, credentials, legal advice or board-level material?
- Could disclosure cause serious harm to individuals, significant financial loss, or regulatory consequences?
- Would it need to be reported as a breach if exposed?

Criteria to define for every level

- Examples of typical information at that level, drawn from your own records
- Who may assign and change the level, usually the data owner
- What to do when a document mixes levels (normally the highest applies)
- When a level should be reviewed or downgraded

Handling rule headings

For each level, write short rules under these headings:

1. **Labelling.** Whether and how the level is shown in documents, emails and systems.
2. **Storage.** Approved locations and systems, and where it must never be kept.
3. **Access.** Who can see it, and how access is approved and reviewed.
4. **Sharing and transmission.** Internal sharing, external sharing, email, file transfer and encryption.
5. **Suppliers.** What contractual and security requirements apply before a supplier can hold it.
6. **AI tools.** Whether it may be entered into any AI tool, and which tools are approved.
7. **Printing and physical copies.** Whether permitted, and how stored and destroyed.
8. **Remote work and devices.** Personal devices, travel and working in public places.
9. **Retention and disposal.** How long it is kept and how it is destroyed or de-identified.
10. **Incidents.** How to report suspected loss or exposure, and how quickly.

Before you roll it out

- ☐ Test the levels on 20 real documents. If people disagree on more than a few, refine the criteria.
- ☐ Check the rules can be followed in your actual systems.
- ☐ Assign a named owner for the scheme.

Next step

The hardest part of classification is usually agreeing the criteria and making the rules work in existing systems. Lexora's data governance framework work can help you test a draft scheme against your own information and obligations.

General information, not legal advice. Your classification scheme and any government contract requirements should be confirmed for your circumstances.

Sources

1. Australian Government Style Manual, Security classifications and protective markings
<https://www.stylemanual.gov.au/node/93>
2. Department of Home Affairs, PSPF Release 2026 now available
<https://www.protectivesecurity.gov.au/node/983>
3. Department of Defence, Assessing and protecting official information guide (2025)
<https://www.defence.gov.au/sites/default/files/2025-04/Assessing-Protecting-Official-Information-Guide.pdf>
4. King & Wood Mallesons, The Protective Security Policy Framework has been updated, what's new (September 2025)
<https://www.mallesons.com/au/en/insights/latest-thinking/the-protective-security-policy-framework-has-been-updated-whats-new>
5. OAIC, Australian Privacy Principles guidelines, Chapter 11 (APP 11 security of personal information)
<https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-11-app-11-security-of-personal-information>



Better governance. *Greater confidence.*

Lexora is an Australian-first advisory business. We help organisations understand their privacy, data and AI obligations, assess risk, build governance frameworks and put practical controls in place.

OUR PRACTICES

Privacy & Data Protection

AI Governance & Responsible AI

Data Governance

Regulatory Readiness & Compliance

WAYS TO START

Privacy Health Check

AI Governance Readiness Assessment

Data Governance Review

Regulatory Readiness Consultation

DISCUSS YOUR GOVERNANCE NEEDS

lexoraai.com.au

info@lexoraai.com.au

More free guides: lexoraai.com.au/resources

This guide is general information, current at the date shown. It is not legal advice and does not take account of your circumstances. Lexora is not a law firm. Check the primary sources before relying on any date or requirement. © 2026 Lexora. You are welcome to share this guide unaltered, with this page attached.