GOVERNMENT OF WESTERN AUSTRALIA

State Solicitor's Office

Information Breach Policy

Purpose

This policy establishes the State Solicitor's Office (SSO) framework for preventing, identifying, containing, assessing, notifying, and reviewing information breaches in accordance with the *Privacy and Responsible Information Sharing Act 2024* (WA) (PRIS Act).

Definitions

Information breach is an incident involving:

- **Unauthorised access** to information (i.e., someone sees or uses information without permission); or
- **Unauthorised disclosure** of information (i.e., information is shared with someone who shouldn't have it); or
- **Loss** of information in circumstances where unauthorised access or disclosure is likely.

Notifiable Information Breach is where there is unauthorised access, unauthorised disclosure, or loss of personal information which is likely to result in serious harm to any individual to whom the information relates.

Serious harm may include (but is not limited to) physical harm or intimidation, serious psychological or emotional harm, identity theft, financial loss, or reputational damage.

Policy Statement

The SSO is committed to safeguarding personal information and responding promptly and appropriately to information security incidents and information breaches, in accordance with applicable laws.

Scope

This Policy applies to all personal information:

- collected for the purposes of providing legal services to the Government of WA and State government departments and agencies.
- collected and held by us regarding our employees, contractors, and consultants.

It applies to all information handled by us, regardless of format (digital, physical, or verbal).

Principles

Our approach to managing information breaches is guided by the following principles:

Key principle:

- **Harm minimisation** – to prevent or reduce the risk of serious harm to affected individuals.

Supporting principles:

- **Protection** – safeguards, commensurate with the sensitivity of the information, level of risk, and potential impact, are implemented to prevent a breach.
- **Prompt action** – breaches are managed quickly to contain the extent of impact.
- **Transparency** – any notifiable information breach will be reported to the relevant authorities and affected individuals.
- **Continuous improvement** – review of incidents is conducted to improve security systems, information handling practices, and response procedures.

Breach Response

We manage information breaches in line with the following steps and record the relevant details in an Information Breach Register.

Contain Immediately, take all reasonable steps to contain the breach and mitigate any harm caused by the breach.

Assess Within 30 days, assess the breach to determine if a notifiable information breach has occurred. In determining whether an Information Breach is or would likely to result in Serious Harm, the following matters must be considered:

- Nature of the information.
- Sensitivity of the information.
- Security measures protecting the information and whether these were bypassed.
- Persons or kinds of persons who obtained or could obtain the information and their intention of causing harm.
- Nature of the harm that has resulted or could result.
- Other relevant matters, including any set out in privacy guidelines.

The written assessment must also consider any privacy guidelines issued by the Information Commissioner regarding such assessments.

Notify Unless an exception applies, and as soon as practical after determining a notifiable information breach has occurred, notify:

- Office of the Information Commissioner via the approved form.
- Affected individuals, in writing where possible, or where this is not practical, via a public notice for at least 12 months.

An exception may apply where:

- The notifiable information breach relates to multiple entities, and another entity has undertaken to notify the affected individuals.
- Compliance would be inconsistent with any applicable secrecy provision.
- There are reasonable grounds that compliance would result in a serious threat to the life, health, safety, or welfare of any individual.
- There are reasonable grounds that compliance would have a material adverse effect on the security of personal information held.

Where an exception is relied upon the Information Commissioner must be informed of that exception in addition to the result of each review, which must be conducted monthly for the duration the exception remains in effect.

Review Conduct a post-incident review to strengthen security and prevent future occurrences.

The swift identification, containment, and mitigation of harm of an information breach supports our wider commitment to strong privacy arrangements and effective legislative compliance.

Recordkeeping and Reporting

We maintain an **Information Breach Registe**r recording details of all reported information breaches; the kind of breach, steps taken to contain the breach and mitigate the risk, assessment outcomes, details of notifications made to the Information Commissioner and affected individuals, any remedial actions taken to prevent future breaches, and the estimated cost of the breach.

All records submitted or created in the management of information breaches will be managed in accordance with the *State Records Act 2000* and our Record Keeping Plan.

Interaction with Other Obligations

This policy operates alongside:

- The SSO Privacy Policy.
- Information security and records management policies.
- The *Legal Profession Uniform Law* (WA) and associated regulations and rules, Western Australian law, and any applicable non-publication or suppression orders made by a court or tribunal.

Review of this Policy

This policy will be reviewed annually to ensure ongoing compliance with:

- The PRIS Act.
- Guidance issued by the WA Information Commissioner.
- Changes in the SSO's systems, risks, or operating environment.