Data Breach Policy

Scope

This data breach policy applies to personal data held by NSW Land Registry Services (**NSW LRS**) and involved in a data breach or suspected data breach. Breaches of the following types of data, which would likely incur 'serious harm' may require notification:

- A device containing personal information is lost or stolen;
- A data repository containing personal information is compromised by an external party;
- personal information is mistakenly provided to the wrong person.

Purpose

This data breach policy is intended to enable NSW LRS to contain, assess and respond to data breaches in a timely fashion, and to help mitigate potential harm to affected individuals. It sets out:

- what constitutes a data breach;
- appropriate roles in the event of a data breach;
- the roles and responsibilities of staff; and
- documents and processes to assist NSW LRS to respond to a data breach.

Personal Information

Under the *Privacy Act 1988* (Cth) and the *Privacy and Personal Information Protection Act 1998* (NSW) (**PIPP Act**) personal information encompasses a broad range of information which includes:

- name;
- address;
- email address;
- phone number;
- ethnicity;
- religious or political beliefs or associations;
- age;
- sex;
- sexual orientation;
- marital status;

- education;
- financial;
- criminal;
- employment history; and
- others' opinion about the individual.

Examples of personal information according to the Office of the Australian Information Commissioner are:

- Information about a person's private or family life (name, contact details, date of birth, medical information, financial information, employment information, signature).
- Information about a person's working habits and practices (place of work, work location, work contact information, job title, work practices and salary).
- Commentary or opinion about a person (employment referee's comments about job applicant's career, performance, aptitude and attitudes, financial opinions about a person, opinion about individual attributes (gender, ethnicity), opinion about individual activities (tastes, preferences, online browsing history, online purchases)

Notifiable Data Breach Criteria

According to the Office of the Australian Information Commissioner the threshold at which a notifiable data breach or suspected data breach becomes reportable, is when the following three criteria are met:

- there is unauthorised access to or unauthorised disclosure of personal information, or loss of personal information, that an entity holds;
- it is likely to result in serious harm to one or more individuals; and
- NSW LRS has not been able to prevent the likely risk of serious harm with remedial action.

Likelihood of Serious Harm

The *Privacy Act 1988* (Cth) and the PIPP Act do not define serious harm but in terms of the notifiable data breaches schemes, serious harm to an individual may include serious physical, psychological, emotional, financial, or reputational harm. The likelihood of serious harm occurring is defined as “more probable than not” (rather than possible).

Compliance

The purpose is to comply with Commonwealth Privacy Legislation and NSW Privacy Legislation.

NSW LRS have implemented a number of cyber security measures to mitigate the risk of data breaches. NSW LRS has included the risk of a data breach within its enterprise risk register and established controls to mitigate this risk and its impact on NSW LRS' systems, data holdings and individuals.

In accordance with section 39 of the *Land and Property Information NSW (Authorised Transaction) Act 2016*, NSW LRS is deemed to be a public sector agency for the purposes of the PIPP Act in relation to the exercise of titling and registry functions. In the case of a data breach NSW LRS is authorised to disclose the information to the Registrar-General, and likewise the Registrar-General is authorised to disclose to NSW LRS. Disclosure between the Registrar-General and NSW LRS is required regardless of the type of data breach involved.

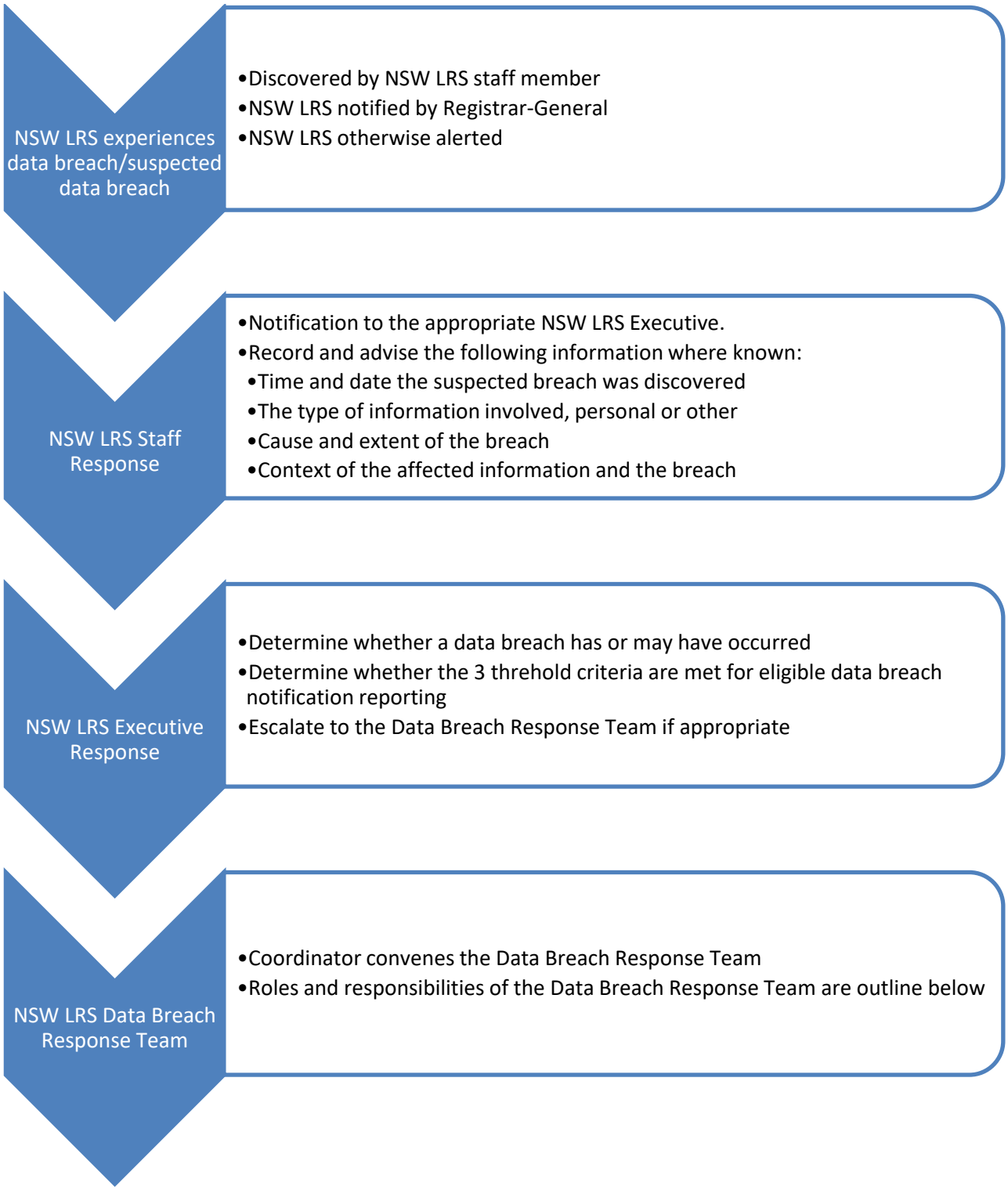
In the event that the threshold criteria for *Privacy Act 1988* (Cth) Notifiable Data Breaches scheme and the PIPP Act Mandatory Notification of Data Breach Scheme are met, the Office of the Australian Information Commissioner (**OAIC**) and the NSW Information and Privacy Commission should be notified.

After NSW LRS becomes aware of a data breach/suspected sensitive data leak:

- the OAIC requires the OAIC to be notified as soon as practicable and the Information and Privacy Commission NSW requires the Privacy Commissioner to be notified immediately.
- the OAIC and the Information and Privacy Commission NSW require assessments of data breaches/suspected data breaches to be completed within 30 days.

Additional notifications to police, law enforcement, professional or regulatory bodies and other agencies or organisations may be required depending on the data involved in the breach.

Plan Overview



Escalation to the Data Breach Response Team

Some data breaches will not require the convening of the Data Breach Response (**DBR**) Team. If serious harm is unlikely, or if NSW LRS can take remedial steps that will stop serious harm, then the DBR Team may not need to be convened and the issue may not be a reportable breach.

In assessing when to convene the DBR Team the following questions should be considered regarding the breach / suspected breach:

- is there a real risk of serious harm to the affected individual or individuals?
- does the breach indicate a systemic problem with NSW LRS processes or procedures?
- are the recommended remedial actions unlikely to prevent serious harm?

If the answer to any of the above is 'yes' then the Data Breach Response Team shall be convened.

Risk Assessment of Data Involved

A guide to assessment of the risk to NSW LRS by reference to the data involved can be described as follows:

Data Involved	Risk Assessment	Risk Assessment To be performed by:
Publicly available data	Low	Business Unit General Manager and reviewed by General Manager Corporate Services
Personal information	High	General Manager Corporate Services
Suppressed personal information	Extreme	General Manager Corporate Services
Financial and personal information	High	Chief Financial Officer and General Manager Corporate Services

IMPORTANT NOTE:

This activity must be completed by NSW LRS in order to assess the potential impact to NSW LRS, however a “Low” risk to NSW LRS does not equate to a lower likelihood of serious harm to the individual(s) involved.

Data Breach Response

Data breaches or suspected data breaches must be dealt with on a case-by-case basis. A risk assessment should be performed and based on that assessment the appropriate course of action determined.

The four steps to consider when responding to a breach or suspected breach:

1. Contain the breach and perform a preliminary assessment
2. Perform a risk assessment
3. Notify internal and external stakeholders
4. Prevent future breaches

If the breach is deemed to require notification (data breach meets the criteria, i.e. data breach is likely to result in serious harm to any of the individuals to whom the information relates), then the data breach notification must be made including recommendations about the steps the individuals should take in response. Direct notification is recommended, either by phone, letter, email or in person. All notification shall be escalated and subject to approval of NSW LRS Executive and/or Chief Executive Officer, this includes website, notices, media etc. and should only occur without direct contact, when direct notification could result in further harm, or contact information is not known. It may be appropriate to use multiple methods of communication in response to a data breach.

Further information for responding to a data breach can be found on the Office of the Australian Information Commissioner (OAIC) website.

All records associated with a data breach / suspected data breach should be stored in the official records management system. NSW LRS maintains an internal register of eligible data breaches.

Root Cause Analysis

Root cause analysis shall be performed on all data breaches/suspected data breaches. Based on the outcomes of the analysis additional processes may be initiated, including but not limited to:

- People and Change Disciplinary Process;
- ICT Problem Management Process;
- ICT Change Management Process;
- Document Review Process.

Continuous Improvement

This plan should be tested and reviewed annually, or sooner in response to business, risk or legislative change.