Data Breach Response Plan

What is a data breach?

A data breach occurs when personal information (defined in section 6 of the Privacy Act 1988 (Cth)) is lost or subjected to unauthorised access, modification, use or disclosure or other misuse. Personal information is information or an opinion about an identified or reasonably identifiable individual. Data breaches may include (but are not limited to) unauthorised access by a third party, information accidentally being uploaded to a public website or a laptop or USB drive containing personal information being lost or stolen and can be caused by or exacerbated by a variety of factors, affect different types of personal information and give rise to a range of actual or potential harms to individuals, agencies or organisations.

Which data breaches are notifiable?

Not all data breaches require notification. The Notifiable Data Breaches (NDB) scheme only requires organisations to notify when there is a data breach that is likely to result in serious harm to any individual to whom the information relates. The purpose of this plan is to enable that assessment to be undertaken and for Ilim College to meet its reporting obligations. Where a data breach is assessed as having occurred then the Data Breach Response Team will take action immediately.

While every effort has been made to present all information accurately, Ilim College, its employees and related parties, accept no liability for, and do not indemnify against, any loss, damage or injury that may result from any actions taken based on the information contained in this document.

Data breach Response Plan

This data breach response plan outlines definitions, sets out procedures and clear lines of authority for Ilim College staff in the event that Ilim College experiences a data breach, or suspects that a data breach has occurred.

This response plan is intended to enable Ilim College to contain, assess and respond to data breaches in a timely fashion and to help mitigate potential harm to affected individuals. It sets out contact details for the appropriate staff in the event of a data breach, clarifies the roles and responsibilities of staff, and documents processes to assist Ilim College to respond to a data breach.

Response Team Membership

Team Member	Role	Description
Sait Kanacevic	Team Leader	
Husam Sidawi	Security Analyst	

Assessing Suspected Data Breaches

If any Ilim College staff member suspects or becomes aware of a data breach, this plan is activated and must be followed. The plan requires a reasonable and expeditious assessment to determine if the data breach is likely to result in serious harm. The following chart outlines the staff roles involved in assessing a data breach.

Ilim College experiences data breach or data breach suspected

The Data Breach was discovered by Ilim College staff member, OR Ilim College was alerted of the breach.

What should the Ilim College staff member do?

- Immediately notify IT Services of the suspected data breach.
- Record and advise IT Services of the time and date the suspected data breach was discovered, the type of personal information involved, the cause and extent of the breach, and the context of the affected information and the breach.

What should the IT Manager do?

- Determine whether a data breach has or may have occurred.
- Determine whether the data breach is serious enough to escalate to the Data Breach Response Team.
- If so, immediately escalate to the Data Breach Response Team.

Alert Ilim College Data Response Team Coordinator

- Coordinator convenes Response Team

Communications **Primary Contact** Glenn Ahern **Secondary Contact** Nejla Ayanlar	➡️	**Business Systems** **Primary Contact** Fatih Buyukyazici **Secondary Contact** Mehmet Erbasi	➡️	**ICT** **Primary Contact** Sait Kanacevic **Secondary Contact** Husam Sidawi

When Should IT Services Escalate A Data Breach to the Data Breach Response Team?

IT Services to use discretion in deciding whether to escalate to the Response Team.

Some data breaches may be comparatively minor, and able to be dealt with easily without action from the Data Breach Response Team.

In determining whether to escalate data breaches to the Response Team, IT Services should consider the following questions:

- Are multiple individuals affected by the breach or suspected breach?
- Is there (or may there be) a real risk of serious harm to the affected individual(s)?
- Does the breach or suspected breach indicate a systemic problem in Ilim College processes or procedures?
- Could there be media or stakeholder attention as a result of the breach or suspected breach?

If the answer to any of these questions is '**yes**', then it may be appropriate for IT Services to notify the Response Team.

IT Services to inform the Response Team Coordinator of minor breaches.

If IT Services decides not to escalate a minor data breach or suspected data breach to the Response Team for further action, IT Services should:

- send a brief email to the Response Team Coordinator Sait Kanacevic - IT Manager that contains the following information:
  - description of the breach or suspected breach
  - action taken by the IT Services or Ilim College officer to address the breach or suspected breach
  - the outcome of that action, and
  - IT Services view that no further action is required
- submit an IT Support request:
  - Use 'Other' category and subject line 'Data Breach':

Data Breach Response Process

There is no single method of responding to a data breach. Data breaches must be dealt with on a case-by-case basis, by undertaking an assessment of the risks involved, and using that risk assessment to decide the appropriate course of action.

There are four key steps to consider when responding to a breach or suspected data breach.

- STEP 1: Contain the breach and do a preliminary assessment
- STEP 2: Evaluate the risks associated with the breach
- STEP 3: Notification
- STEP 4: Prevent future breaches

The Response Team should ideally undertake steps 1, 2 and 3 either simultaneously or in quick succession. Refer to the detailed checklist at the end

of this plan.

Depending on the breach, not all steps may be necessary, or some steps may be combined. In some cases, it may be appropriate to take additional steps that are specific to the nature of the breach. The checklist at the end of this plan is intended to guide the Response Team in the event of a data breach and alert the Response Team to a range of considerations when responding to a data breach.

Evaluating A Serious Risk of Harm to An Individual

In evaluating whether there is a serious risk of harm to an individual whose information is the subject of a data breach, the Response Team must consider:

- what type of personal information is involved (and in particular, whether it is sensitive information);
- whether there are any protections that would prevent the party who receives (or may have received) the personal information from using it (for example, if it is encrypted);
- the nature of the harm that could arise from the breach, for example whether an individual was reasonably likely to suffer:
  - identity theft;
  - financial loss;
  - a threat to their physical safety;
  - a threat to their emotional wellbeing;
  - loss of business or employment opportunities;
  - humiliation, damage to reputation or relationships; or
  - workplace or social bullying or marginalisation;
- what steps have been taken to remedy the breach (and how certain Ilim College is that they are effective).

Notifying the Office of Australian Information Commissioner (OAIC)

- In the event that the Response Team decides there has been a data breach and there is a real risk of serious harm to affected individuals the Response Team must prepare a statement that includes:

- Ilim College's contact details;

- a description of the data breach;

- the kind of information concerned; and

- recommendations about the steps that individuals should take in response to the eligible data breach that the entity has reasonable grounds to believe has happened.

The statement must be submitted to OAIC via email to enquiries@oaic.gov.au as soon as reasonably practical.

Notifying the Individuals Affected

As soon as reasonably practical after Ilim College has submitted the statement to the OAIC, Ilim College must:

- if practical, take reasonable steps to notify the contents of the statement to each of the individuals to whom the information relates; or

- if practical, take reasonable steps to notify contents of the statement to each of the individuals who are at risk from the eligible data breach.

If it is not practical to undertake either of the above, the Response Team must ensure a copy of the statement is published on Ilim College's website and reasonable steps are taken to publicise the contents of the statement (for example, by notifying its members).

Records Management

Documents created by the Response Team should be saved in the following Google Drive location:

- IT Services > Data Breaches

Checklist

☐	Convene a meeting of the data breach Response Team
☐	Immediately contain breach: • IT to implement the ICT Incident response plan if necessary • Building security to be alerted if necessary
☐	Inform IT Manager, provide ongoing updates on key developments
☐	Ensure evidence is preserved that may be valuable in determining the cause of the breach, or allowing Ilim College to take appropriate corrective action
☐	Consider developing a communications or media strategy to manage public expectations or media interest

☐	Conduct initial investigation, and collect information about the breach promptly, including: • the date, time, duration and location of the breach • the type of personal information involved in the breach • how the breach was discovered and by whom • the cause and extent of the breach • a list of the affected individuals, or possible affected individuals • the risk of serious harm to the affected individuals • the risk of other harms
☐	Determine whether the content of the information is important
☐	Establish the cause and extent of the breach
☐	Assess priorities and risk based on what is known.
☐	Keep appropriate records of the suspected breach and actions of the Response Team, including the steps taken to rectify the situation and the decisions made

☐	Determine who needs to be made aware of the breach (internally and potentially externally) at this preliminary stage
☐	Determine whether to notify affected individuals – is there a real risk of serious harm to the affected individuals?
☐	Consider whether others need to be notified, including police, Australian Privacy Commissioner, or other agencies or organisations affected by the breach, or where Ilim College is contractually required, or required under the terms of an MOU to notify specific parties
☐	Fully investigate the cause of the breach

☐	Report to Executive on outcomes and recommendations: • update security and response plan if necessary • make appropriate changes to policies and procedures if necessary • revise staff training practices if necessary • consider the option of an audit to ensure necessary outcomes are affected