Head Office:
Level 6, 297 Diagonal Road
Oaklands Park, SA 5046.

Phone: (08) 8377 0101
Fax: (08) 8377 3911

Eighty9 Limited and its wholly owned subsidiaries Status Works Pty Ltd and Allied Services Worldwide Pty Ltd

DATA BREACH RESPONSE PLAN

Version Control			
Version	Date	Changes made	Changed by
1.0	16/06/21	Initial version	Scott Foody
1.1	4/11/21	Review	Scott Foody
1.2	09/03/23	Updated template, formatting, & company terminology	Savannah Bacon
1.3	15/03/2023	Added Scope – page 4 and amended terminology	Emma Farina
2.0	01/07/23	Update of Organisation details to Eighty9 Limited	Tahlia Yale

Table of Contents

PART A: Date Breach Reporting Procedures for the Organisation's Personnel

Objective

Eighty9 Limited and its wholly owned subsidiaries Status Works Pty Ltd and Allied Services Worldwide Pty Ltd, collectively and hereinafter referred to as "the Organisation" is committed to protecting the privacy of individuals, including clients, staff and stakeholders.

The purpose of this Data Breach Response Plan (**Plan**) is to enable us to:

(a) identify, contain, escalate, assess and respond to data breaches in a timely manner;
(b) proactively help mitigate and remediate potential harm to affected individuals;
(c) document its processes and data breach responses;
(d) identify the staff roles and responsibilities, delegations of authority and reporting lines in the event of a data breach and points of contact; and
(e) identify the staff responsible for managing the data breach response.

This Plan will assist the Organisation to meet its statutory obligations under the mandatory Notifiable Data Breaches scheme (NDB scheme) in Part IIIC of the Privacy Act that came into effect from 22 February 2018.

This Plan operates under the Privacy Policy and must be followed when assessing and responding to an actual or suspected data breach.

The Plan consists of the following sections:

Section	Description
Part A	Sets out the procedures for all staff who become aware of an actual or suspected data breach
Flowchart (Page 9)	Outlines the Phases for reporting and assessing data breaches
Part B	Sets out the assessment procedure for the Data Breach Response Group
Annex A	Data Breach Report Form
Annex B	Eligible Data Breach Assessment Form
Annex C	OAIC Notification Template
Annex D	Options for Notification Checklist

Scope

This policy applies to all Responsible Persons, employees and volunteers of the Organisation, hereinafter referred to as "our people".

Definitions

Personal information

Information or an opinion about an identified individual or an individual who is reasonably identifiable, whether the information is true or not, and whether the information is recorded in a material form or not. It includes all personal information regardless of its source and regardless of whether it is publicly available.

Data breach

This occurs when personal information is subjected to unauthorised access or disclosure, or where the information is lost and unauthorised access or disclosure is likely to occur.

Example: data breaches resulting from human error

- *Loss of our people's work laptop, USB or paper records that contain personal information held by* the Organisation *(e.g. left on a train, at the airport etc.)*

One of our people accidentally disclosing personal information to the wrong recipient (e.g. sending correspondence to the wrong student, publishing a link on our website which identifies all clients and their private information etc.)

Example: data breaches resulting from malicious activity

- *Hacking into* the Organisation's *email accounts, software or databases containing Personal Information*
- *Scams that trick an employee of* the Organisation *into releasing personal information*

Inappropriate or fraudulent use of a database containing personal information

Example: data breaches resulting from unforeseen circumstances

Unforeseen events that occur to a contractor who holds personal information on behalf of the Organisation *(e.g., YourDC) or if a cloud service provider suffers a data breach (e.g. MYOB, VETtrak)*

Eligible data breach

Is a data breach that is likely to result in serious harm to any of the individuals to whom the information relates.

The Organisation must notify the Office of the Australian Information Commissioner (**OAIC**) and affected individuals if:

(a) it has reasonable grounds to believe that an eligible data breach has occurred; or
(b) it is directed to do so by the OAIC (for instance if a data breach is reported directly to the OAIC by an affected individual and/or if the OAIC disagrees with Status' assessment that the incident is not an eligible data breach).

Key Points

- The Organisation's **people** must immediately report actual or suspected data breaches to their **Area Manager** using the **Data Breach Report** form.
- The **Area Manager** must take immediate action to contain the actual or suspect data breach, and provides the **Data Breach Report** to the **National Compliance Manager** (anysa.williams@status.net.au or 08 8377 0101).

- The **National Compliance Manager** must conduct a preliminary investigation and reports findings to the **Chief Information Officer**.
- If necessary, the **Chief Information Officer** convenes the **Data Breach Response Group** to assess the breach.
- If the **Chief Information Officer** (as recommended by the **Data Breach Response Group**) determines that an **eligible data breach** has occurred, the OAIC and affected individuals are notified by the **Chief Information Officer**.

Key Roles and Responsibilities

Title	Role
The Organisation's Personnel (our people,titleholders, contractors, including personnel of controlled entities etc.)	• Report incidents immediately to their Area Manager • Complete the Data Breach Report and give to AreaManager • Participate in investigations as required
Area Managers or relevant line manager	• Receive Data Breach Reports from the Organisation's Personnel within their area • Contain breach, remediate harm, and preserve evidence • Forward Data Breach Report to the National Compliance Manager • Assist with investigations as required
National Compliance Manager	• Receive Data Breach Reports from Area Manager and alert Chief Executive Officer and Chief Information Officer of potential data breach • Conduct a preliminary investigation • Provide findings to Chief Information Officer • Participate as a member of the Data Breach Response Group • Record incidents in the Organisation's Risk Register
Chief Information Officer	• Receive preliminary investigation findings from National Compliance Manager • Accept or reject preliminary investigation findings • Determine the seriousness of the data breach • Decide whether to convene of the Data Breach Response Group, and whether to include additional members • Approve assessment by Data Breach Response Group • Make notifications as appropriate • Conduct post-action review
Data Breach Response Group	• Assess containment and/or remediation actions

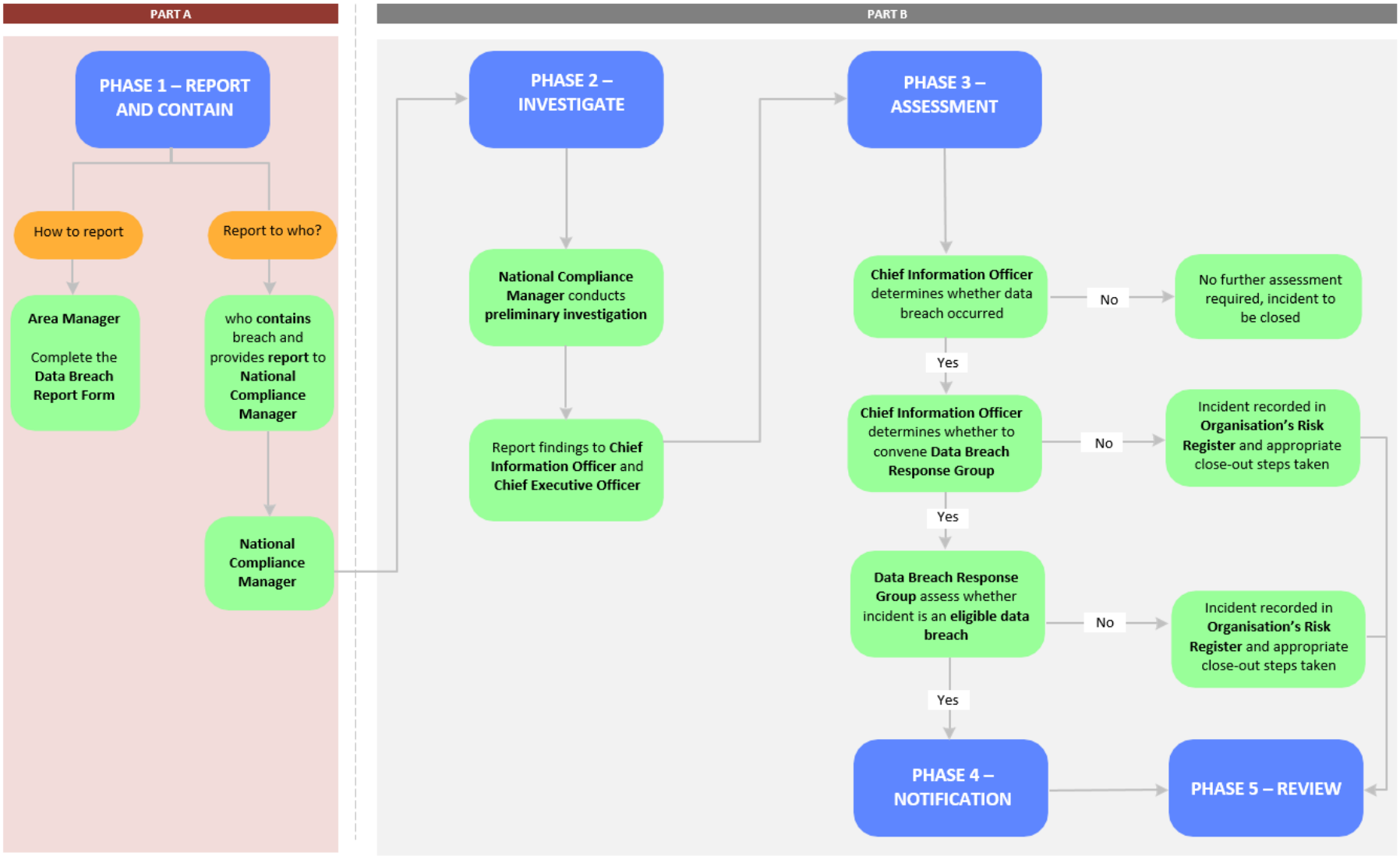
	• Assess preliminary investigation • Assess whether an eligible data breach has occurred • Assess notification requirements • Assist with post-action review

Timeframes

An actual or suspected data breach must be investigated and managed as soon as the Organisation becomes aware of the data breach, or suspects that it has occurred.

Suspected data breach	Confirmed eligible data breach
Assessment must be reasonable and expeditious. All reasonable steps to complete the assessment within 30 days of the date that the Organisation became aware of or suspected a data breach. This timeframe should be treated as the maximum timeframe for completing the assessment.	Notify the OAIC and affected individuals **as soon as practicable** after becoming aware of an eligible data breach.

The Organisation's Data Breach Response Plan - Flowchart



Note For further information about the steps in this Flowchart go to the relevant Phase in the Data Breach Response Plan

Phase 1: Report and Contain

1.1 *Procedure for Reporting Data Breaches*

If any of the Organisation's people becomes aware of an actual or suspected data breach, they must report it as soon as possible. The Organisation's people should immediately:

(a) record the details of the data breach in the **Data Breach Report Form** provided in **Annex A** (**Data Breach Report**);

(b) provide a copy of the **Data Breach Report** to their **Area Manager** either in person or by email; and

(c) otherwise keep the incident confidential except where it is necessary to disclose information about the incident in accordance with this Plan.

Upon receiving the **Data Breach Report**, the **Area Manager** must immediately:

(a) take action to contain the data breach, remediate harm, and preserve evidence;

(b) notify the **National Compliance Manager** of the incident and provide a copy of the completed **Data Breach Report** by emailing: loretteg@status.net.au; and

(c) otherwise keep the incident confidential except where it is necessary to disclose information about the incident in accordance with this Plan.

1.2 *Procedure for Containing Data Breaches and Remediating Harm*

The **Area Manager** is responsible for taking immediate action to contain the breach and remediate harm, including by seeking assistance from the appropriate business units or external suppliers as necessary.

Important: At any time, appropriate steps should be taken to reduce any potential harm to affected individuals. If remedial action is successful in preventing serious harm to affected individuals, notification may not be mandatory. However the Organisation's notification requirements will be determined in the relevant phase of this Plan.

Below are examples of containment / remedial steps that may be appropriate:

Example: If the data breach involves electronic records held on an ICT system:

- *Isolate the causes of the data breach in the relevant system, software or database*
- *Shut down the compromised system, software or database*
- *Reset log-in details and passwords for compromised devices, systems or databases*
- *Quarantine any compromised devices*
- *Activate the Organisations' Business Continuity Management Framework*

Example: If the data breach involves the loss of a device or physical files

- *Remotely disable the lost device*
- *Arrange a search of the site where the loss occurred by contacting any relevant authorities (e.g. the public transport authority if lost on a train, an airline if left on a plane etc.)*

Example: If the data breach involves the unauthorised disclosure of personal information to a third party

- *By email – recall the email from the recipient and/or ask the recipient not to read and to delete the email.*
- *By post – contact the recipient and ask them not to open or read the posted materials, and arrange for collection/return of the posted materials.*
- *By publication online – deactivate the link to the publication.*

1.3 *Preserving Evidence of a Suspected Data Breach*

The **Area Manager** must take any reasonable steps available to them to preserve and/or record evidence of an actual or suspected data breach.

Example:

- *Making a note of any other person/s who witnessed the incident.*
- *Recording the exact time of the incident.*
- *If a cyber-attack has occurred – recording the details of any pop-up message or email you receive in relation to the cyber-attack.*
- *If there has been accidental disclosure of personal information to the wrong person – retaining copies of any emails or file notes relating to the incident, and storing them on the Organisations' record keeping system.*

For Phases 2 – 5 see Part B of this Plan

PART B: Data Breach Management Procedures for Internal

Phase 2: Investigate

2.1 *Procedure for investigating reported Data Breaches*

The **National Compliance Manager** must review any report of an actual or suspected data breach as soon as reasonably practicable. Upon reviewing the **Data Breach Report**, the **National Compliance Manager** must:

(a) notify the **Chief Executive Officer** and **Chief Information Officer** that a **Data Breach Report** has been received;
(b) assess what containment and/or remediation actions have already been undertaken by the **Area Manager** (if any), and whether any further actions are required; and
(c) undertake any preliminary investigations necessary to confirm the report and/or seek any clarification or additional detail as necessary.

Important: At any time, appropriate steps should be taken to reduce any potential harm to affected individuals. If remedial action is successful in preventing serious harm to affected individuals, notification may not be mandatory. However the Organisation's notification requirements will be determined in the relevant phase of this Plan.

Once the **National Compliance Manager** has reviewed the **Data Breach Report** and undertaken their preliminary investigation to confirm the incident, they must make an initial assessment of:

(a) whether the reported incident is not a data breach (such that further investigation is not required);
(b) whether the reported incident is a data breach (such that a further investigation is required); and
(c) if there is a data breach, give an initial risk rating using the Organisations' Risk Matrix having regard to relevant issues including (if known):
    (i) number of individuals affected by the breach or suspected breach;
    (ii) type of personal information;
    (iii) likelihood of serious harm to affected individuals;
    (iv) the breach or suspected breach indicates a systematic problem in the Organisations' processes or systems;
    (v) media or stakeholder attention as a result of the breach or suspected breach; or
    (vi) whether remedial actions have successfully prevented harm to affected individuals.

2.2 *Reporting and Escalation*

The **National Compliance Manager** must provide the findings of the preliminary investigation to the **Chief Executive Officer** and **Chief Information Officer** as soon as possible.

Phase 3: Assessment

3.1 *Procedure for escalation to the Data Breach Response Group*

The **Chief Information Officer** will assess the preliminary investigation findings to determine whether to convene the **Data Breach Response Group**. The **Chief Information Officer** may request further information from the **National Compliance Manager** if reasonably required to make a determination.

If the **Chief Information Officer**:

(a) determines the incident is not a data breach, the incident will not be escalated to the **Data Breach Response Group**, and the **Chief Information Officer** must direct the **Area Manager** or **National Compliance Manager** to undertake any action that is reasonably necessary to close-out the incident appropriately;

(b) determines the incident is a data breach and suspects that serious harm is at least *possible* (as per the likelihood scoring system in the Organisation's Risk Matrix), it should be escalated to the **Data Breach Response Group** for further assessment (see section 3.3); or

(c) determines the incident is a data breach and determines that serious harm is at most *unlikely* (as per the likelihood scoring system in the Organisation's Risk Matrix):

  (i) the incident should not be escalated to the **Data Breach Response Group**;

  (ii) the **Chief Information Officer** will direct the **National Compliance Manager** to record the incident in the Organisation's Risk Register; and

  (iii) the **Chief Information Officer** may direct the **Area Manager** or **National Compliance Manager** to undertake any action that is reasonably necessary to close-outthe incident appropriately, which may include giving voluntary notification to affected individuals and / or OAIC.

3.2 *Members of the Data Breach Response Group*

The **Data Breach Response Group** comprises the following permanent members:

Position Title
Chief Information Officer (Convenor) (or nominee)
Chief Executive Officer (or nominee)
National Compliance Manager (or nominee)
National Operations Managers (or nominee)

The **Chief Information Officer** may co-opt additional members onto the **Data Breach Response Group** or engage external providers to assist in containment or investigation of the breach, depending on the nature or severity of the data breach:

Branch / Office	Requirement	Position Title
Human Resources	Where data breach involves our people (as affected individuals or involved in the breach)	Executive Director – HR
IT	Where data breach involves ICT systems (e.g. unauthorised access to a database, a cyber-attack etc.)	Chief Information Officer
Media & Corporate Relations	Where data breach affects a large number of individuals or is serious, and therefore likely to attract publicity	Chief Executive Officer
Student Services	Where data breach affects a large number of students and it is likely they will want to contact the Organisation	Executive Director – Training Services
Insurance	Where data breach will potentially be covered by insurance held by the Organisation (e.g. cyber	Executive Director – Finance

	insurance or insurance against theft or damage to physical property)	
Records Services	Where data breach affects records of the Organisation	Chief Executive Officer
External Supplier	Where data breach involves a third party supplier or contractor of the Organisation	Subject to nature of data breach
External service providers	Legal services (e.g. if the Organisation requires specialist / legal advice) IT (e.g. if the Organisation requires additional assistance with a data breach involving ICT systems) Accounting or auditing services (e.g. if the Organisation requires additional assistance with a data breach involving financial information) Public relations services (e.g. if the Organisation requires advice on how to manage media enquiries, possible reputational damage etc.)	Note: External service providers must be preapproved by the Chief Executive Officer prior to engagement to ensure costs are covered by insurance

3.3 *Procedure for Conducting Assessment of Data Breach*

If a determination is made in accordance with 3.1(b), the **Chief Information Officer** must convene a meeting of the **Data Breach Response Group** **as soon as possible**.

The **Data Breach Response Group** is responsible for assessing and determining whether:

(a) the data breach is likely to result in serious harm to the affected individual or individuals;

(b) mandatory notification to the OAIC and affected individuals is required; or

(c) if notification is not mandatory, voluntary notification to the OAIC and/or affectedindividuals is desirable.

In conducting the assessment, the following issues must be considered:

(d) the **type** of Personal Information involved;

(e) the **context** of the affected information and the breach;

(f) the **cause and extent** of the breach; and

(g) the **risk of serious harm** to affected individuals.

The **Data Breach Response Group** must meet in person or via secure teleconference. The **Data Breach Report** and the results of the preliminary investigation (including any containmentand/or remediation steps taken) must be tabled at the first meeting of the **Data Breach Response Group.**

The **Data Breach Response Group** must complete the **Eligible Data Breach Assessment Form (Annex B)**. In all cases, the assessment should be conducted expeditiously and completed within 30 days of the date that the data breach occurred.

The **Chief Information Officer** will be responsible for determining whether an **eligible data breach** has occurred, based on the **Data Breach Response Group's** assessment and recommendation.

Important: The obligation to notify the OAIC and affected individuals as soon as reasonably practicable is triggered when the Organisation determines that an **eligible data breach** has occurred.

The 30 day assessment timeframe is the **maximum** timeframe for completing the risk assessment. It is possible that the obligation to notify could be triggered within 1-2 days of the data breach occurring.

3.4 *Non-eligible Data Breaches*

If during Phase 3, the **Chief Information Officer** determines the data breach is *not* an **eligible data breach**, the **Chief Information Officer** will direct the **National Compliance Manager** to record the incident in the Risk Register (if appropriate), and the **Chief Information Officer** may direct the **Area Manager** or **National Compliance Manager** to undertake action that is reasonably necessary to close-out the incident appropriately.

The close-out actions may include giving voluntary notification to the OAIC and/or affected individuals in accordance with notification procedures set out in Phase 4 based on a recommendation by the **Data Beach Response Group** having regard for the nature and circumstances of the incident.

Once close-out steps have been carried out (if any) Phase 5 should be completed as appropriate.

3.5 *Record Keeping and Evidence Preservation*

The **Data Breach Response Group** must keep records of all steps taken in response to the data breach and decisions made in connection with it. This includes:

(a) keeping a record of all steps taken during the preliminary investigation and subsequent assessment of the reported data breach; and

(b) ensuring that any relevant evidence of the data breach (such as computer imaging, forensic investigation or other investigative processes) is preserved and stored securely.

The information may be required by forensic investigators, legal advisors, law enforcement and regulators, as well as for use in preparing notifications to and communications with affected individuals and the OAIC and any other regulator or relevant entities.

Evidence and records must be sufficient to demonstrate to the OAIC, where required, the reasonable steps taken to comply with statutory and other legal obligations.

Where the assessment by the **Data Breach Response Group** is for the purpose of obtaining legal advice:

(c) all documents, written communications, reports, notes or advice relating to the data breach must be marked "*Confidential and Subject to Legal Professional Privilege*"; and

(d) no other reports, forms or other documents relating to the data breach will be prepared except those which are required or requested by the **Chief Executive Officer** (or nominee).

Phase 4: Notification

4.1 *Notification*

If during Phase 3, the **Chief Information Officer** determines the data breach to be an **eligible data breach**, the Organisation must give notification to the **OAIC and all affected individuals** about the data breach.

The statutory timeframe for **eligible data breach** notification is **as soon as practicable after the Organisation becomes aware of the eligible data breach**. The OAIC understands that this timeframe will vary depending on the Organisation's circumstances. Factors such as the time, effort, or cost required to prepare the eligible data breach notification will also be relevant.

There may also be other notifications which would be appropriate in the particular circumstances (e.g. notifying insurers, the police, cybercrime agencies etc.) – see 4.4.

Important: At any time, steps should be taken to reduce any potential harm to affected individuals. If remedial action is successful in preventing serious harm to affected individuals, notification may not be mandatory. However the Organisations' notification requirements will be determined in the relevant phase of this Plan.

4.2 *Procedure for Notifying the OAIC*

The **Chief Information Officer** or a nominated member of the **Data Breach Response Group** must prepare a draft **notification to the OAIC** using the **OAIC Notification Template (Annex C)**, completed online at:
https://forms.business.gov.au/smartforms/servlet/SmartForm.html?formCode=OAIC-NDB

It is mandatory to include the following information in Part A of the OAIC Notification:
(a) the identity and contact details of the Organisation;
(b) a description of the eligible data breach;
(c) the kind or kinds of Personal Information affected by the breach; and
(d) the Organisation's recommendation as to the steps that individuals should take to protect their position in response to the data breach.

It is optional to include the following additional information in Part B of the OAIC Notification:
(e) additional details about the circumstances of the breach;
(f) number of individuals affected;
(g) additional information about the steps taken to respond to the breach; and
(h) any other information that might be relevant to assist OAIC in considering the appropriate response to the notification.

The notification to the OAIC must be **approved by the Chief Information Officer** prior to being sent.

The notification must be sent to the OAIC by the notifiable Data Breach Form on the OAIC website:
https://forms.business.gov.au/smartforms/servlet/SmartForm.html?formCode=OAIC-NDB

Once the **Chief Information Officer** (or nominee) has submitted the notification to the OAIC, the record of the OAIC's acknowledgement of receipt of the eligible data breach statement and reference number must be recorded and sent to the **National Compliance Manager**. Following submission of the notification to the OAIC the **Chief Information Officer** (or nominee) should contact the OAIC by telephone to confirm it has been received.

4.3 *Procedure for Notifying Affected Individuals*

If there has been an **eligible data breach**, the **Data Breach Response Group** is responsible for assessing the options available for notifying affected individuals of the data breach, using the **Options for Notification Checklist (Annex D)**.

The **Chief Information Officer** or a nominated member of the **Data Breach Response Group** must then prepare a draft **notification to affected individuals**. The notification to affected individuals must include:

(a) how and when the data breach occurred;
(b) the types of Personal Information involved in the data breach;
(c) what the Organisation has done or will be doing to reduce or eliminate the risk of harm brought about by the data breach;
(d) any assurances (if applicable) about what data has not been disclosed (i.e. if a breach only affects an individual's basic identity or contact information, but not their financial information or any sensitive information);
(e) what steps the individuals can take to protect themselves and what the Organisation will do to assist people to do this (if applicable);
(f) contact details for the Organisation for questions or requests for information or assistance (e.g. helpline numbers, e-mail addresses or websites);
(g) whether the Organisation has notified the OAIC about the data breach; and
(h) how an individual can lodge a privacy complaint with the OAIC.

The notification to affected individuals must be **approved and signed by the Chief Information Officer** prior to being sent out to the relevant persons.

Once approved, the **Chief Information Officer** is responsible for sending out the notification to individuals and/or delegating the responsibility to the appropriate business unit.

The **Chief Information Officer** must keep a record of:

(a) the date, time and method of notification to each individual; and
(b) any confirmation of receipt of the notification received from an individual (unless the data breach involves a very large number of individuals, and it would be impractical to do so).

4.4 *Procedure for Making Additional Notifications*

The **Data Breach Response Group** must also consider whether any of the following persons need to be made aware of the actual or suspected data breach:

Category	Notification trigger
Internal people	If the breach is likely to be reported on in the media, or if there are widespread discussions of it between our people
Insurance company	If the breach involves unauthorised access, use or disclosure of electronic records (i.e., hacking, online scams, malware, physical theft of devices containing electronic records etc.)
Law enforcement agency	If the breach involves theft or other criminal activity, it will generally be appropriate to notify police
Third party service providers	If the breach involves or affects a third-party service provider's facilities, infrastructure or personnel

Category	Notification trigger
Regulators ○ **ASIC** ○ **ATO**	If the breach involves financial information, notification may be appropriate
Specialist advisors ○ **Legal** ○ **Public relations** ○ **Forensic IT**	If the Organisation requires independent legal advice, IT investigations, or a PR strategy ***Note:* Specialist advisors must be preapproved by Finance prior to engagement to ensure costs are covered by the Insurer**
Cybercrime support networks ○ **The Australian Cybercrime Online Reporting Network** ○ **The Computer EmergencyResponse Team (CERT)** ○ **Australia Cyber Security Centre**	If the data breach involves unauthorised access, use ordisclosure of electronic records (i.e. hacking, online scams etc.)

If the **Data Breach Response Group** determines that additional notification is desirable, approval must be obtained from the **Chief Information Officer** before such notification is made.

4.5 *Additional Considerations*

The **Data Breach Response Group** should also consider the following factors:

(a) If law enforcement authorities are involved, check with them whether notification shouldbe withheld or delayed to avoid compromising the investigation; and

(b) If the data breach is likely to attract publicity, the Board must be briefed so as to co-ordinate the timing and prepare content for any media release or statement. All media or public enquiries relating to the data breach must be referred to the **Executive Chairman** and responses should be approved by the **Chief Information Officer** (or nominee) prior to release.

Phase 5: Review

5.1 *Procedure for Conducting Post Breach Review*

The **Chief Information Officer** (or nominee) is responsible for conducting a post-breach review and assessment, once the immediate consequences of the data breach have been dealt with.

In conducting the review, the **Chief Information Officer**:

(d) should seek informal input and assistance from other members of the **Data Breach Response Group** and other business units, as required;

(e) must

(i) complete any further investigations as necessary or desirable;

(ii) determine whether any data handling or data security practices led or contributed to the relevant data breach;

(iii) consider whether there are any further actions that need to be taken as a result of the relevant data breach, such as:
  (A) updating security measures;
  (B) reviewing and updating this data breach response plan;
  (C) making appropriate changes to practices, systems, other processes, policies and procedures;
  (D) revising the Organisation's internal training practices;
  (E) reviewing external vendors' security/contract terms and ongoing engagement; and
  (F) considering undertaking an audit to ensure necessary outcomes are implemented.

(f) then as soon as reasonably practicable:
  (i) update the Organisation's Risk Register and / or Non-compliance Register as appropriate; and
  (ii) provide a written report to the Audit, Compliance & Risk Committee with their findings and recommendations for further actions.

Below are some examples of further actions that could be considered in particular situations:

Example: If the data breach was caused by the conduct of our people, could the Organisation:

- *provide any internal training to prevent the data breach from re-occurring*
- *provide any once-off or regular internal reminders to our people to prevent the data breach from re- occurring*
- *provide any additional oversight or supervision of our people, to prevent the data breach from re-occurring*
- *increase its auditing or monitoring of our people to prevent the data breach from re-occurring*
- *change any internal policies or procedures to prevent the data breach from re-occurring*
- *introduce any new controls or restrictions on access for our people to prevent the data breach from re-occurring*

Example: If the data breach involved a security breach by a third party, could Status:

- *improve its IT security in any way*
- *improve its building security in any way*
- *apply any additional security protections to protect the Personal Information (e.g. encryption, use of pseudonyms)*
- *increase its security surveillance in any way*
- *give any directions to its people or contractors that would prevent the security breach from re-occurring*
- *change any IT or building security policies or procedures to prevent the data breach from re-occurring*
- *introduce any new access restrictions to prevent the data breach from re-occurring*

ANNEX A – Data Breach Report Form

Part A – Persons Details	
Full Name:	
Position Title and Business Unit:	
Phone Number:	
Email Address:	
Part B – Incident Details	
Date and time of the data breach:	
Location of the data breach:	
Description of the data breach (ie. what happened, what types of personal information involved):	
How was the breach detected?	
How many individuals does the data breach affect?	1 2 – 10 11 – 100 101 – 1,000 1,001 – 10,000 10,001 – 100,000 100,001 or more
What systems (eg devices, email accounts, databases, worksites etc.) have been affected by the breach (if known)?	
Attach any evidence of the breach (eg. computer logs, screenshots, relevant emails etc.):	
Part C - Declaration	
Date:	Signature:

ANNEX B – Eligible Data Breach Assessment Form

The Organisation must 'carry out a reasonable and expeditious assessment of whether there are reasonable grounds to believe that relevant circumstances amount to an eligible data breach', as per The Privacy Act 1988 (s 26WH(2)(a)).

The amount of time and effort spent on this assessment should be proportionate to the likelihood, and apparent severity, of the breach.

Eligible Data Breach Assessment should be a three-stage process:

Initiate

The Organisation should decide whether an assessment is necessary, and subsequently decide which person(s) or group(s) will be responsible for this assessment if deemed necessary.

Investigate

Relevant information to the breach should be gathered as quickly as possible. Such information could include: who may have had access to the information, what personal information could have been affected and what are the likely impacts of this breach. Depending on the breach, a foundation for this investigation can be built from the data included in the Data Breach Report Form (Annex A)

Evaluate

At the conclusion of the investigation, it can be determined whether the identified breach is an eligible data breach or not. The OAIC determines a breach is classified as an eligible data breach if the following three criteria are satisfied:

1. there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds
2. this is likely to result in serious harm to one or more individuals, and
3. the entity has not been able to prevent the likely risk of serious harm with remedial action

More information can be obtained via the OAIC website: https://www.oaic.gov.au

ANNEX C – OAIC Notification Template

The OAIC Notification Template can be found and submitted online at the following address:

https://forms.business.gov.au/smartforms/servlet/SmartForm.html?formCode=OAIC-NDB

ANNEX D – Options for Notification Checklist

Once the Organisation has identified there has been an eligible data breach, the Organisation must:

- Make a decision about which individuals to notify
- Prepare a statement for the Commissioner, and
- Notify individuals of the contents of this statement

There are three options for notifying individuals at risk of serious hard, depending on what is 'practicable' for the Organisation

Notification Options

Option 1 — Notify all individuals

If it is practicable, an entity can notify each of the individuals to whom the relevant information relates (s 26WL(2)(a)). That is, all individuals whose personal information was part of the eligible data breach.

This option may be appropriate, and the simplest method, if an entity cannot reasonably assess which particular individuals are at risk of serious harm from an eligible data breach that involves personal information about many people, but where the entity has formed the view that serious harm is likely for one or more of the individuals.

The benefits of this approach include ensuring that all individuals who may be at risk of serious harm are notified, and allowing them to consider whether they need to take any action in response to the eligible data breach.

Option 2 — Notify only those individuals at risk of serious harm

If it is practicable, an entity can notify only those individuals who are at risk of serious harm from the eligible data breach (s 26WL(2)(b)).

That is, individuals who are likely to experience serious harm as a result of the eligible data breach. If an entity identifies that only a particular individual, or a specific subset of individuals, involved in an eligible data breach is at risk of serious harm, and can specifically identify those individuals, only those individuals need to be notified.

The benefits of this targeted approach include avoiding unnecessary distress to individuals who are not at risk, limiting possible notification fatigue among members of the public, and reducing administrative costs, where it is not required by the NDB scheme.

Option 3 — Publish notification

If neither option 1 or 2 above are practicable, for example, if the entity does not have up-to-date contact details for individuals, then the entity must:

- publish a copy of the statement on its website if it has one
- take reasonable steps to publicise the contents of the statement (s 26WL(2)(c))

It is not enough to simply upload a copy of the statement prepared for the Commissioner on any webpage of the entity's website. Entities must also take proactive steps to publicise the substance of the eligible data breach (and at least the contents of the statement), to increase the likelihood that the eligible data breach will come to the attention of individuals at risk of serious harm.

While the Privacy Act does not specify the amount of time that an entity must keep the statement accessible on their website, the Commissioner would generally expect that it is available for at least 6 months.

Methods of Notification and Content of Notifications

Options 1 (Notify all individuals) and 2 (Notify only those individuals at risk of serious harm)

Options 1 and 2 above require that entities take 'such steps as are reasonable in the circumstances to notify individuals about the contents of the statement' that the entity prepared for the Commissioner (s 26WL(2)(a) and (b)).

The entity can use any method to notify individuals (for example, a telephone call, SMS, physical mail, social media post, or in-person conversation), so long as the method is reasonable. In considering whether a particular method, or combination of methods is reasonable, the notifying entity should consider the likelihood that the people it is notifying will become aware of, and understand the notification, and weigh this against the resources involved in undertaking notification.

An entity can notify an individual using their usual method of communicating with that particular individual (s 26WL(4)). For example, if an entity usually communicates through a nominated intermediary, they may also choose to notify through this intermediary.

The entity can tailor the form of its notification to individuals, as long as it includes the content of the statement required by s 26WK. That statement (and consequently, the notification to individuals) must include the following information:

1. the identity and contact details of the entity (s 26WK(3)(a))
2. a description of the eligible data breach that the entity has reasonable grounds to believe has happened (s 26WK(3)(b))
3. the kind, or kinds, of information concerned (s 26WK(3)(c))
4. recommendations about the steps that individuals should take in response to the eligible data breach (s 26WK(3)(d))

Decisions about the appropriate types of recommendations will always be dependent on the circumstances of the eligible data breach. This may include choosing to tailor recommended steps around an individual's personal circumstances, or providing general recommendations that apply to all individuals. In some circumstances, the entity may have already taken some protective steps, reducing the necessity for action by affected individuals. The entity may choose to explain these measures in the notice to individuals as a part of their recommendation. For example, a bank may notify an individual that it has suspended suspicious transactions on their account and recommended steps may be limited to suggesting the individual monitor their accounts and notify the bank immediately of any other suspicious transactions.

Option 3 (Publish notification)

Option 3, which can only be used if options 1 or 2 are not practicable, requires an entity to publish a copy of the statement prepared for the Commissioner on its website, and take reasonable steps to publicise the contents of that statement.

An entity should consider what steps are reasonable in the circumstances of the entity and the data breach to publicise the statement. The purpose of publicising the statement is to draw it to the attention of individuals at risk of serious harm, so the entity should consider what mechanisms would be most likely to bring the statement to the attention of those people.

A reasonable step when publicising an online notice, might include:

- ensuring that the notice is prominently placed on the relevant webpage, which can be easily located by individuals and indexed by search engines
- publishing an announcement on the entity's social media channels
- taking out a print or online advertisement in a publication or on a website the entity considers reasonably likely to reach individuals at risk of serious harm

In some cases, it might be reasonable to take more than one step to publicise the contents of the statement. For example, if a data breach involves a particularly serious form of harm, or affects a large number of individuals, an entity could take out multiple print or online advertisements (which could include paid advertisements on social media channels), publish posts on multiple social media channels, or use both traditional media and online channels.

The approach to publicising the statement may depend on the publication method. For example, where space and cost allows, an entity may republish the entirety of the information required to be included in the statement. Another option, if the available space is limited, or the cost of republishing the entire statement would not be reasonable in all the circumstances, would be to summarise the information required to be included in the statement and provide a hyperlink to the copy of the statement published on the entity's website. Entities should keep in mind the ability and likelihood of individuals at risk of serious harm being able to access the statement when determining the appropriateness of relying solely on such an approach.

If option 3 is chosen, entities should take care to ensure that the online notice does not contain any personal information. While it may help if entities provide a general description of the cohort of affected individuals, this description should not identify any of the affected individuals or provide information that may make an individual reasonably identifiable. For example, it may be appropriate for an online retailer to publicise that individuals who made transactions in the year 2013 may be affected, but it would not be appropriate for the retailer to publicise the names associated with any compromised transaction data.

Timing of notification

Entities must notify individuals as soon as practicable after completing the statement prepared for notifying the Commissioner (s 26WL(3)).

Considerations of cost, time, and effort may be relevant in an entity's decision about when to notify individuals. However, the Commissioner generally expects entities to expeditiously notify individuals at risk of serious harm about an eligible data breach unless cost, time, and effort are excessively prohibitive in all the circumstances.

If entities have notified individuals at risk of serious harm of the data breach before they notify the Commissioner, they do not need to notify those individuals again, so long as the individuals were notified of the contents of the statement given to the Commissioner. The scheme does not require that notification be given to the Commissioner before individuals at risk of serious harm, so if entities wish to begin notifying those individuals before, or at the same time as notifying the Commissioner, they may do so.

*Notification content taken directly from the OAIC website:
https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/part-4-notifiable-data-breach-ndb-scheme#notifying-individuals-about-an-eligible-data-breach

Approved by: Gary Hatwell Signature:  Date: 1/7/2023