SAAFE Limited Data Breach Response Plan

1. Policy statement

1.1 SAAFE Limited ABN 89 663 720 278 (**SAAFE**) is committed to complying with the *Privacy Act 1988* (Cth) (**Privacy Act**), including the provisions relating to mandatory notifications of data breaches.

1.2 This Data Breach Response Plan (**Response Plan**) sets out procedures and clear lines of authority for the persons involved in CRC SAAFE in the event that SAAFE experiences a data breach (or suspects that a data breach has occurred).

1.3 This Response Plan is intended to enable SAAFE to contain, assess and respond to data breaches in a timely fashion, 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 SAAFE to respond to a data breach. It has been informed by the Data Breach Response Plan of the Office of the Australian Information Commissioner (**OAIC**).

2. Application

2.1 Staff

(a) All persons who handle personal information in connection with CRC SAAFE are responsible for ensuring that they comply with this Response Plan.

(b) Persons involved with CRC SAAFE or SAAFE from other organisations may also be required to follow this Response Plan.

2.2 Data breaches

(a) A data breach occurs when personal information is lost or subjected to unauthorised access, modification, use or disclosure or other misuse. These events could be the result of malicious activity, such as hacking, or arise inadvertently.

(b) By way of example, there will be a personal data breach where personal information is:

(i) lost, including the loss of paper records or devices on which personal data is stored such as laptops, mobile devices or USBs; or

(ii) stolen, including theft of hard copy materials or devices containing personal information; or

(iii) accessed by an unauthorised third party, including by way of hacking attempts, or virus or other malicious malware attacks; or

(iv) obtained by deception; or

(v) made vulnerable as a result of compromised user account (eg disclosure of user login details through phishing); or

(vi) deliberately published/leaked on a public forum without authorisation; or

(vii) disclosed to an incorrect recipient, or disclosed to a third party without authorisation; or

(viii) altered without permission; or

(ix) otherwise accidentally lost or destroyed.

(c) Certain data breach events give rise to mandatory reporting obligations under the Privacy Act. These are referred to as an '**Eligible Data Breach**'.

(d) An Eligible Data Breach arises when all three of the following criteria are satisfied:

(i) there is '**unauthorised access**' to, '**unauthorised disclosure**' of, or a '**loss**' of, personal information that is held by SAAFE; and

(ii) that access, disclosure or loss is likely to result in '**serious harm**' to any of the individuals to whom the information relates; and

(iii) SAAFE has not been able to prevent the likely risk of serious harm with remedial action.

(e) This Response Plan applies to *all* data breach events, whether it is an Eligible Data Breach or not, but some of the steps in this Response Plan will apply only in the event of an Eligible Data Breach.

2.3 Personal information

(a) Under the Privacy Act, 'personal information' is defined to mean any information or opinion, whether or not true, about an individual who is identified or reasonably identifiable.

(b) An individual may be identifiable without being named, for example if a combination of traits could be used to identify the person involved.

(c) Personal information can also include:

(i) sensitive information, about matters such as race, religion and sexuality, health, genetics, and biometrics;

(ii) health information, about matters such as an individuals symptoms/diagnosis and genetic information; and

(iii) credit-related information.

3. Steps when a data breach is suspected

3.1 Step 1: Discovery

(a) A data breach is:

(i) discovered or suspected by a SAAFE staff member or contractor (**Staff**);

(ii) discovered or suspected by a CRC SAAFE partner or Project partner (**Partner**) or its staff members or contractors (**Partner Staff**);

(iii) is otherwise brought to SAAFE's attention.

3.2 Step 2: Containment

(a) Where any data breach is discovered or suspected, regardless of seriousness of the breach, Staff and Partner Staff must first ensure that they take any steps immediately available to them to:

(i) contain any possible data breach; and

(ii) preserve any evidence that may be valuable in identifying the cause of the breach, or that would enable SAAFE to address the risks posed to affected individuals or SAAFE as a result of the breach.

(b) Examples of containment/remedial steps that may be appropriate include:

(i) applying (or re-applying) access restrictions;

(ii) shutting down any compromised systems, software or databases;

(iii) quarantining any compromised devices;

(iv) remotely disabling any lost devices;

(v) contacting any unintended recipients of personal information and recalling the relevant personal information (or verifying that the recipient has destroyed the personal information) if possible; or

(vi) deactivating any links to unauthorised publications of personal information.

(c) If in doubt, contact the Privacy Officer to discuss the steps required.

3.3 Step 3: Internal reporting

(a) The relevant person must immediately notify:

(i) in the case of Staff, their line manager; and

(ii) in the case of Partner Staff:

(A) who are involved in a CRC SAAFE Project, the Project Leader; or

(B) otherwise, the representative in their organisation who is responsible for receipt of notices in relation to CRC SAAFE,

of the suspected data breach (**Manager**).

(b) This should include advising of:

(i) the time and date the suspected breach was discovered;

(ii) the type of personal information involved;

(iii) the cause and extent of the breach;

(iv) the context of the affected information and the breach; and

(v) any steps that have already been taken to contain the breach.

3.4 Step 4: Managerial assessment

(a) To the extent that there is any ambiguity as to whether a data breach has in fact occurred, the Manager must first seek to determine this question. If this cannot be promptly answered conclusively, the matter should be referred to the Data Breach Response Team (**Response Team**) for further investigation.

(b) Once a data breach has been identified, the Manager must promptly determine whether the data breach is serious enough to escalate to the Response Team, as per the considerations discussed below at 4.1.

(c) If so, the matter must be immediately escalated to the Privacy Officer, acting as **Response Team Coordinator**.

(d) If not, the incident must still be reported, as outlined at 4.2 below.

3.5 Step 5: Response Team

(a) The Privacy Officer is defined within the CRC SAAFE Privacy Policy and is the Business Operations Manager (or equivalent), acting as Response Team Coordinator to convene the Response Team, comprising:

(i) the Chief Executive Officer;

(ii) the Chief Operating Officer;

(iii) corporate and communications team: Communications Manager;

(iv) information technology team: Authorised Comunet Account Manager;

The contact details for the response team are included at the end of this document.

4. Escalating a data beach to the Response Team

4.1 Managers to use discretion in deciding whether to escalate to the Response Team

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

(b) For example, Staff may, as a result of human error, send an email containing personal information to the wrong recipient. Depending on the sensitivity of the contents of the email, if the email can be recalled, or if the officer can contact the recipient and the recipient agrees to delete the email, it may be that there is no benefit in escalating the issue to the Response Team.

(c) Managers should use their discretion in determining whether a data breach or suspected data breach requires escalation to the Response Team. In making that determination, Managers should consider the following questions:

(i) Are **multiple individuals** affected by the breach or suspected breach?

(ii) Is there (or may there be) a risk of **serious harm** to the affected individual(s)?

(iii) Does the breach or suspected breach indicate a **systemic problem** in the SAAFE's processes or procedures?

(iv) 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 is likely to be appropriate for the Manager to notify the Response Team.

(d) If a Manager is unsure as to what steps might be appropriate, they should contact the Response Team Coordinator in the first instance.

4.2 Managers to inform the Response Team Coordinator of minor breaches

(a) If a Manager decides not to escalate a minor data breach or suspected data breach to the Response Team for further action, the Manager or should send a brief email to the Privacy Officer that contains the following information:

(i) description of the breach or suspected breach;

(ii) action taken by the Manager, Staff or Partner Staff to address the breach or suspected breach;

(iii) the outcome of that action; and

(iv) the Manager's view that no further action is required.

(b) All privacy breaches should also be considered to be incidents and an incident form should be completed and notified.

5. Response Team checklist

5.1 Process

(a) 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.

(b) There are four key steps to consider when responding to a breach or suspected breach:

(i) **Step 1:** Contain the breach and do a preliminary assessment

(ii) **Step 2:** Assess the risks associated with the breach

(iii) **Step 3:** Notification

(iv) **Step 4:** Review

These steps are explained in more detail in the checklist below.

(c) The Response Team should ideally undertake steps 1, 2 and 3 either simultaneously or in quick succession.

(d) The Response Team should refer to Part 3 of the OAIC document *Data breach preparation and response — A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)*,[1] which provides further detail on each step.

(e) 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 particular incident.

(f) In reviewing SAAFE processes and procedures to reduce the risk of future breaches (Step 4), the Response Team should also refer to the OAIC's *Guide to securing personal information*.[2] This guide presents a set of non-exhaustive steps and strategies that may be reasonable for SAAFE to take in order to secure personal information and considers actions that may be appropriate to help prevent further breaches following an investigation.

(g) The following checklist 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.

[1] https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response
[2] https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information

RESPONSE TEAM CHECKLIST

Step 1: Contain the breach and make a preliminary assessment

- Convene a meeting of the Response Team.
- If unsure whether a breach has occurred, the Privacy Act requires that the Company 'carry out a reasonable and expeditious assessment' and take 'all reasonable steps to ensure that the assessment is completed **within 30 days**' of any suspicion arising.
- The Response Team should work to ensure that the this is completed as soon as possible, with 30 days representing the absolute maximum amount of time before further steps are taken.
- Immediately contain any breach:
  - IT to take any necessary immediate action, if applicable.
  - Building security to be alerted if necessary.
- Inform the SAAFE Board and the Chief Executive Officer and provide ongoing updates on key developments.
- Ensure evidence is preserved that may be valuable in determining the cause of the breach, or in allowing SAAFE to take appropriate corrective action.
- Consider developing a communications or media strategy to manage public expectations and media interest.

Step 2: Assess the risk for individuals affected by the breach

- 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, and its sensitivity;
  - 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;
  - any security measures that may protect or obscure the information involved, and the likelihood that these could be overcome; and
  - the kinds of persons who have obtained or who could obtain the information.
- Determine whether the context of the information is important.
- Establish the cause and extent of the breach.
- Assess priorities and risks 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.

Step 3: Consider breach notification

- Determine who needs to be made aware of the breach (internally, and potentially externally) at this preliminary stage.
- Review whether SAAFE will be required to provide notification of the breach as an Eligible Data Breach under Part IIIC of the Privacy Act. This will likely be the case where:
  - the breach is **likely to result in serious harm** to one or more individuals; and
  - SAAFE has not been able to prevent the likely risk of serious harm with remedial action.
- If there is any doubt as to whether the breach is an Eligible Data Breach, SAAFE should promptly seek legal advice on this point, as the Privacy Act requires that the Company 'carry out a reasonable and expeditious assessment' and take 'all reasonable steps to ensure that the assessment is completed **within 30 days**' of such query arising.
- The Response Team should work to ensure that this is completed as soon as possible, with 30 days representing the absolute maximum amount of time before further steps are taken.
- Where an Eligible Data Breach has occurred, SAAFE must prepare a statement that meets the requirements of Part IIIC of the Privacy Act, which will include:
  - SAAFE's name and contact details;
  - a description of the breach;
  - the kinds of information concerned; and
  - recommendations about the steps that individuals should take in response to the breach.

  SAAFE must then take steps as soon as practicable to provide this statement to individuals affected or likely to be affected by the breach, along with the OAIC.
- Determine whether it may be appropriate to notify affected individuals in any event, even if not strictly required to do so by the Privacy Act.
- Determine whether SAAFE may be required to notify the Commonwealth of the breach under the terms of its Grant Agreement.
- Consider whether others should be notified, including police/law enforcement, or other agencies or organisations affected by the breach, or where SAAFE is contractually required to notify other specific parties.

Step 4: Review the incident and take action to prevent future breaches

- Fully investigate the cause of the breach.
- Report to the SAAFE board on outcomes and recommendations.
- Where required because of the circumstances of the breach:
  - update security procedures and this Response Plan;
  - make appropriate changes to other policies and procedures; and
  - revise staff training practices.
- Consider the option of an audit to ensure necessary outcomes are implemented.
- Fully document the incident.

6. Response Team Details

Name	Role	Responsibility	email	phone
Rohan Wighton Backup: Alex Lloyd	Operations Manager / Privacy Officer / Response Team Coordinator	Ensure policy and systems are maintained, deployed and improved. Ensure breaches are managed on the day and reviewed.	Rohan.wighton@crcsaafe.com.au	0427713014
Alex Lloyd Backup: Charlotte Ferrier	Chief Executive Officer	Ensure Information Security systems are appropriately resourced	Alex.lloyd@crcsaafe.com.au Charlotte.ferrier@crcsaafe.com.au	0451596564 04880778112
Rachael Nightingale Backup: Charlotte Ferrier	Communications Manager	Ensure communications across Information Security System are timely, targeted, appropriate and professional	Rachael.nightingale@crcsaafe.com.au	
Tristan Sullivan Backup: N/A	Comunet Information Security Officer	Ensure protections are fit for purpose and adequately implemented. Ensure any data breach is supported by appropriate mitigation and recovery and review efforts	tsullivan@comunet.com.au	0402567937
Carmen Lam Backup: Sai Gabbita	Business Operations Officer	Assist with the maintenance and improvement of policy and systems. Assist with the on the day management of data breaches and their incident review	Carmen.Lam@crcsaafe.com.au	