AFPA DATA BREACH RESPONSE PROCEDURE

Version: 0001

Effective: DAY MONTH YEAR

Document Summary

Document Prepared By:
Angela Lowe, Senior Corporate Services Officer

Document Authorised By:
Angela Smith, National President

Review Date:

Version	Date
0001	

Change Summary:

Version	Date	Change Description	Updated By	Approved
0001	23 January 2018		Angela Lowe	

Table of Contents

AFPA DATA BREACH RESPONSE PROCEEDURE

INTRODUCTION

This data breach response plan (the response plan) sets out procedures and clear lines of authority for Australian Federal Police Association (AFPA) employees if the AFPA experiences a data breach, or suspects that a data breach has occurred.

A data breach occurs when personal information is lost or subjected to unauthorised access, modification, use or disclosure or other misuse. Data breaches can be caused 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 and organisations.

This response plan is intended to enable the AFPA 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 the AFPA to respond to a data breach.

PROCEDURES

1. **AFPA experiences data breach/data breach suspected**
   (Discovered by AFPA employee, or AFPA otherwise alerted)

2. **What should the employee do?**
   - Immediately notify your supervisor of the suspected data breach.
   - Record and advise your supervisor of the time and date the suspected 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.
3. **What should the supervisor do?**
   - Determine whether a data breach has or may have occurred.
   - Escalate to the Data Breach Response Coordinator (Manager Legal and Industrial).

Supervisors to use discretion in deciding whether to escalate to the response coordinator

Some data breaches may be comparatively minor, and able to be dealt with easily without action from the Data Breach Response Coordinator (response coordinator).

For example, an AFPA employee 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 need to escalate the issue to the response coordinator.

In exercising their discretion whether a data breach or suspected data breach requires escalation to the response coordinator, supervisors should consider the following:

- 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 AFPA 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 the supervisor to notify the response coordinator.

If a supervisor decides not to escalate a minor data breach or suspected data breach to the response coordinator for further action, they should **send a brief email to the response coordinator** that contains:

- a description of the breach or suspected breach
- action taken by the supervisor or AFPA employee to address the breach or suspected breach
- the outcome of that action, and
- the supervisor's view that no further action is required
- AFPA Data Breach Response Checklist

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 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 coordinator should ideally undertake steps 1, 2 and 3 either simultaneously or in quick succession.

The response team should refer to the OAIC's *Data breach notification: a guide to handling personal information security breaches* which provides further detail on each step.

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.

In reconsidering AFPA processes and procedures to reduce the risk of future breaches (Step 4), the response coordinator should also refer to the AFPA's Privacy Policy. This policy sets outs the AFPA's requirements for dealing with personal information, particularly of members.

The following checklist is intended to guide the response coordinator in the event of a data breach:

RECORDS MANAGEMENT

Documents created by the response team should be saved in the following AFPA j:drive folder:

- Data Breach Response – reports and investigation of data breaches within the OAIC (internal link)

Step 1

Contain the breach and make a preliminary assessment

- 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 the OAIC Executive, including the Australian Privacy Commissioner; provide ongoing updates on key developments.
- Ensure evidence is preserved that may be valuable in determining the cause of the breach, or allowing the OAIC to take appropriate corrective action.
- Consider developing a communications or media strategy to manage public expectations and media interest.

STEP 2

Evaluate the risks for individuals associated with 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
- 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 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

- 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?* In some cases, it may be appropriate to notify the affected individuals immediately; e.g., where there is a high level of risk of serious harm to affected individuals.
- Consider whether others should be notified, including police/law enforcement, or other agencies or organisations affected by the breach, or where the OAIC is contractually required or required under the terms of an MOU or similar obligation to notify specific parties.

Step 4

Review the incident and take action to prevent future breaches

- Fully investigate the cause of the breach.
- Report to OAIC 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 effected.