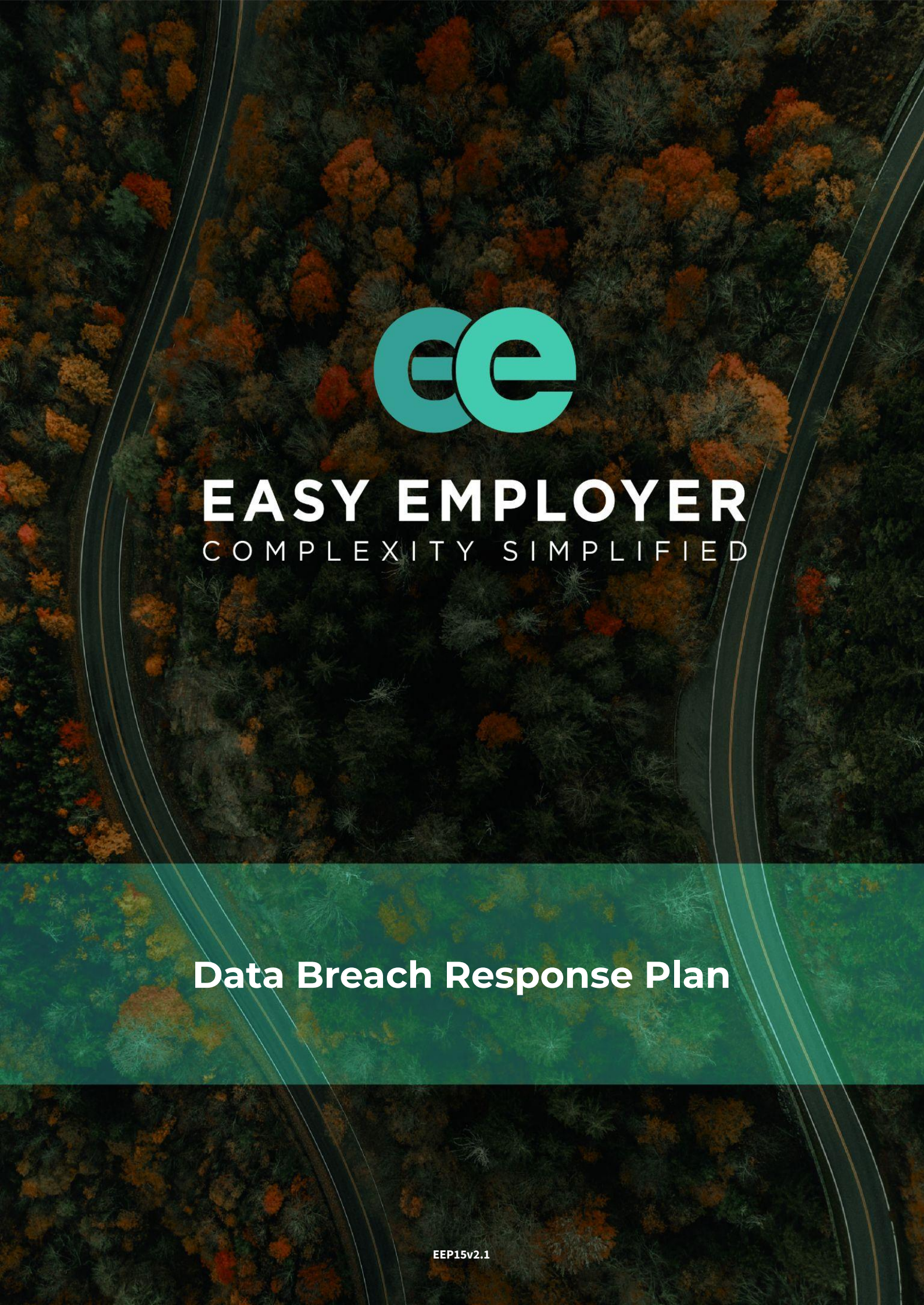

EASY EMPLOYER

COMPLEXITY SIMPLIFIED

Data Breach Response Plan

EEP15v2.1

EASY EMPLOYER

Table of Contents

EASY EMPLOYER

Document Management

Contributors

Name	Role
Aaron Upcroft	Chief Executive Officer
Jim Watts	Chief Technology Officer
Phil Combridge	Head of Development & SME
Irene Hazilias	Senior Manager
Ryon Gallagher	Senior Manager (Previous)
James Nikolaidis	Senior Manager & Director (Previous)

Version Control

Changes made to this document since initial distribution.

Date	Version	Author	Amendment
20/06/2018	**1.0**	Irene Hazilias	First Draft
20/06/2021	**1.1**	Irene Hazilias	Content update
08/07/2022	**1.2**	Ryon Gallagher	Review and content update
03/02/2023	**1.3**	Laird Anderson	Formatting and content update
10/02/2023	**2.0**	Aaron Upcroft	Major content review & full update
29/06/2023	**2.1**	Aaron Upcroft	Minor update regarding staff changes

EASY EMPLOYER

1. Introduction

1.1. Data Breach Response Plan

This data breach response plan sets out procedures and clear lines of authority for Easy Employer staff in the event of a data breach (or suspects that a data breach may have occurred).

1.1.1. What is a Data Breach?

A data breach is when personal information is lost or is 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.

1.1.2. The Plan

This response plan is intended to enable Easy Employer to act appropriately to suspected breaches and to contain, assess and follow through on suspected data breaches in a timely fashion. An aim is to first mitigate potential harm to affected individuals, analyse and check security, comply with reporting requirements agreed with customers and required by contracts or laws, and to act appropriately to correct any gaps in the defences against data breaches.

This document 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 Easy Employer to respond to a data breach.

2. Roles and Protocols

2.1. Company Experiences Data Breach/Data Breach Suspected

Discovered by a staff member, or Company otherwise alerted.

2.1.1. What should the staff member do?

- Immediately notify your Manager of the suspected data breach.
- Record and advise your Manager 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.

2.1.2. What should the Manager do?

- Determine whether a data breach has or may have occurred.
- Determine whether the data breach is serious enough to escalate to the Project Coordinator (some breaches may be able to be dealt with by Management).
- If so, immediately escalate to the Project Coordinator.

2.1.3. Manager convenes response

Executive	Product & Delivery	Client Engagement
Chief Technology Officer	Head of Product & Delivery	Head of Client Engagement

3. Escalation

3.1. Escalating a data breach to a Manager (Staff)

Staff must escalate any data breach related issue. The Manager responsible for software development is the first point of contact.

Some data breaches may be comparatively minor, and able to be dealt with without direct Management involvement, but all issues still need to be reported. For example, a staff member may, because of human error, send an email containing personal information to the wrong customer. After informing their direct manager and depending on the sensitivity of the contents of the email, staff can attempt to recall it (if the option is available), or contact the recipient to request the email is deleted. If the recipient agrees to delete it, then the situation can be considered to be adequately addressed without requiring direct management intervention.

The appropriate response needs to be acceptable to the parties involved —whose data security has been breached, Easy Employer and the recipient. If any party remains aggrieved the issue must be then addressed by management.

The manager should use their discretion in determining whether a data breach or suspected data breach requires escalation to the Management Team. In making that determination, the manager should consider the following questions:

- Are multiple individuals affected by the breach or suspected breach?
- Is there a real risk of serious harm to the affected individual/s?
- Could there be a real risk of serious harm to the affected individual/s?
- Does suspected breach indicate a systemic problem in Easy Employer processes or procedures?
- Could there be media, mayor, councillor, management or other customer stakeholder group whose attention this would come to - because of the suspected breach?

If the answer to any of these questions is ‘yes’, then it may be appropriate for the manager to escalate the issue to the Management Team.

3.2. Escalating minor breaches to the Management Team (Manager)

If the manager decides not to escalate a minor data breach or suspected data breach to the Management Team for further action, the manager should:

- Send a brief email to the Management Team that contains the following information:
    - Description of the suspected breach situation
    - Action taken by the manager, staff and other involved parties, to address the situation
    - the outcome of that action, and
    - the manager’s view that no further action is required

4. Process Flow

Maintain Information Security

Protect information from misuse, interference and loss, and from unauthorised access, modification or disclosure. Consider the sensitivity and confidentiality of the information.

If a data breach is suspected or reported

(Personal information is lost, subject to unauthorised access, modification, use or disclosure; or other misuse or interference)

Contain breach and gather facts

- Act to stop the breach
- Act to prevent the risk of further breaches
- Do preliminary assessments

Evaluate risks

- What personal information (or combination of information) is involved
- Assess if context of the information is important
- Establish cause and extent of the suspected breach
- Identify the risk of harm

Notifications

- **When?**
  As soon as is reasonably possible
- **How?**
  Direct contact by phone, with follow up in writing.
- **Who to?**
- The nominated point of contact, a Manager in the affected organisation. The organisation then notifies the affected individuals.
- **What?**
  Description of the breach, type of information involved, steps to help mitigate the situation, contact details for information and assistance.
- **Who to notify specifically?**
  Consider the following:
  - Office of the Australian Information Commissioner
  - Police/Law enforcement
  - Professional or regulatory bodies
  - Other agencies
  - Organisation(s) affected
  - Organisations with contractual obligation to be notified

Prevent future breaches

- Investigate the cause of the breach
- Create/improve a prevention plan
- Update security. response plan
- Make appropriate updates to policies and procedures
- Revise staff training practices

5. Data Breach Checklist

5.1. Process

Data breaches are to be approached on a case-by-case basis, assessing the risks involved, and deciding on an appropriate course of action.

There are four key steps to consider:

Step 1: Contain and gather facts

- Stop the breach
- Act to prevent the risk of further breaches
- Do preliminary assessment

Step 2: Evaluate the risks

Step 3: Notifications

Step 4: Prevent future breaches

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

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 Easy Employer processes and procedures to reduce the risk of future breaches (Step 4).

The following checklist is intended to guide the response team in the event of a data breach, and alert the manager to a range of considerations when responding to a data breach.

5.2. Records Management

Documents created by the response team should be attached to the non-conformance report, a non-conformance report that is created to be a record of the suspected breach and the determinations made.

Step 1: Contain the breach and make a preliminary

- Convene a meeting or notify the manager.
- Immediately contain breach:
    - IT to implement relevant response plans, if necessary.
    - Building manager to be alerted, if necessary.
- Inform a manager, provide ongoing updates on key developments.
- Ensure evidence is preserved that may be valuable in determining the cause of the breach, or allowing Easy Employer to take appropriate corrective action.
- Consider developing a communication strategy to manage customer expectations and community 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 manager, including the steps taken to rectify the situation and the decisions made.

Step 3: Evaluate the risks for individuals associated with the breach

- Determine who needs to be made aware of the breach (internally, and potentially externally) at this preliminary stage.
- Determine whether to notify affected customer(s) —is there a real risk of serious harm to the affected individuals? In some cases, it may be appropriate to notify the affected customer(s) immediately; e.g., where there is a high level of risk of serious harm or to affected individuals.
- Consider whether others should be notified, including police/law enforcement, or other agencies or organisations affected by the breach, or where Easy Employer is contractually required or under similar obligation to notify specific parties.
    - OAIC – notifiable data breaches.
- Examples of a data breach include when:
    - a database containing personal information is hacked
    - personal information is mistakenly provided to the wrong person

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

- Fully investigate the cause of the breach.
- Report to Easy Employer management 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