Data Breach Policy and Procedure

1. Purpose

The purpose of this Policy is to provide a description of how the RTO will respond to a data breach in accordance with the Privacy Act 1988 and Australian Privacy Principles.

2. Policy Statement

Belelmo Pty Ltd Essential Business Training - RTO: 91492 is committed to providing quality training and assessment products and services in compliance with the Standards for Registered Training Organisations (RTOs) 2015 and all other relevant legislation, including the Privacy Act and Australian Privacy Principles.

It is the RTO's belief that clear roles, responsibilities and procedures will serve as the foundation as a comprehensive privacy program.

This policy outlines:

- the steps that the RTO will take to contain, assess, notify, and review any data breaches that might occur; and
- Notifiable Data Breaches and how the RTO will address them if they occur.

All RTO employees, officers, representatives or advisers ('Employees') are required to understand and act in accordance with this policy.

This policy should be read in conjunction with the Privacy Policy and Records Management Policy and Procedure.

3. Data Breach Definition

A data breach occurs when personal information or intellectual property held by the RTO is subject to unauthorised access, disclosure, modification, or is lost. Data breaches can occur in a number of ways, including but not limited to:

- Unauthorised Third-party security breaches (for example, Hackers)
- Unauthorised access, disclosure or modification by Employees and users
- Data breaches of Third-party services used by the RTO that affect user data
- Specific to the RTO's business, the following have been identified as possible data breach sources:
- Accidental loss, unauthorised access, or theft of classified material data or equipment on which such the RTO data is stored, such as RTO Laptops and USBs.
- Unauthorised use, access to, or modification of data on the RTO's sharepoint, Xero, Student Management System, Client Relationship Manager or Learner Management System.

- Accidental disclosure of the RTO user data or intellectual property, such as via email to an incorrect address.
- Unauthorised data collection by third parties posing as the RTO, for example, Phishing Scam
- Failed or successful attempts to gain unauthorised access to the RTO information or information systems
- Unauthorised data collection by third parties through Malware infections on the RTO cloud databases, or hardware equipment.

4. What to do if you suspect a data breach has occurred?

All the RTO Employees who are aware of, informed of, or suspect a data breach must inform the RTO's Management and IT team immediately. The IT team must then assess the suspected breach to determine whether or not a breach has in fact occurred. If a data breach has, in fact, occurred, then the IT team will manage the breach according to the steps outlined in the Data Breach Management Plan.

It is important to note that disclosures of data breaches should only come from senior management, if an RTO Employee suspects that a data breach has occurred, this policy does not allow for this information to be shared with other Employees or Clients. This disclosure process must be handled by senior management.

5. Data Breach Response Plan

In accordance with OAIC recommendations, the following steps will be taken in response to a verified Data Breach.

- Contain the breach as soon as possible. Containment is ensuring that the breach itself is stopped. How a breach is stopped would depend on the particular instance but can include:
    - The suspension of compromised accounts;
    - Removal of malware, where identified;
    - Temporary platform downtime if necessary;
    - Recovering any lost data, if possible;
    - Repairing unauthorised modification of data, if possible;
    - Restoring access to the platform when able.
- Assess the risks involved and the repercussions on respective stakeholders. The following may be considered in assessing the stakeholder risks:
    - The type of information involved;
    - Establish the cause and the extent of the breach;
    - Assess the risk of harm to affected persons;

- Assess the risk of other harms: reputational damage;
- Notify Management and Affected Individuals and Organisations where appropriate;
- The CEO is to notify any relevant government entities such as State Training Authorities;
- Management must be notified of breaches as and when they occur, whether or not the breach is an eligible breach under the Notifiable Data Breach Scheme;
- the RTO is an APP 11 entity under the Privacy Act 1988 (Cth) and is and must, therefore, comply with its obligations under the Notifiable Data Breach Scheme;
- Data Breaches that are not eligible under the Notifiable Data Breach Scheme need not be reported and may be addressed internally.

- Prevent future similar breaches through strengthening security infrastructures and/or policies

6. Notifiable Data Breach Scheme

Under the Notifiable Data Breach Scheme, the RTO is obliged to report data breaches that satisfy the following criteria:

- there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that the RTO holds (such as USI, IDs, credit card details, and general personal information contained within enrolment forms required by AVETMISS;
- That the unauthorised access to or disclosure of, or loss of personal information is likely to result in serious harm to one or more individuals; and
- the RTO has not been able to prevent the likely risk of serious harm with remedial action.

For further information on how to assess a notifiable data breach, the RTO must refer to the OAIC's APP guidelines.

Where the RTO suspects that an eligible breach has occurred, it must carry out a reasonable and expeditious assessment of the breach: s 26WH(2)(a) of the Privacy Act. Where possible, the assessment must be completed within 30 days of the RTO becoming aware of information that causes it to suspect that an eligible breach has occurred. If the RTO is unable to complete the assessment within 30 days, a written document must be written which addresses:

- how all reasonable steps have been taken to complete the assessment within 30 days;
- the reasons for the delay; and
- that the assessment was reasonable and expeditious.

Where an Eligible Breach has occurred, the RTO must inform affected users AND the Privacy Commissioner. the RTO is allowed to disclose eligible breaches to users in either of the following ways:

- It may notify all the RTO users

- It may notify affected the RTO users
- It may publish a notification on its website

Disclosure of eligible breaches to the Privacy Commissioner may be done by online form.

For more information on disclosing Eligible Breaches under the Notifiable Data Breach Scheme, please refer to the OAIC's webpage on the topic.

7. Disciplinary Consequences

The RTO reserves the right to monitor Employees' use, access and modification of the RTO's data, and initiate an investigation in cases where an employee conducts an action that is in breach of this policy.

All Employees should handle the RTO's data with due diligence in accordance with this policy and any related policies. If an employee's action or omission that is prohibited under this policy causes a disruption of integrity to the data system or leads to a breach defined in the Privacy Act, the employee may face severe disciplinary action up to and including termination at the discretion of the RTO.

8. Monitoring of Data Security

Note that where an Employee is operating on RTO devices or systems, this information is stored and recorded within the RTOs IT systems and may be recovered or reviewed as required by the RTO. The following are examples of how the company records and keeps information;

- Company emails are recorded and backed up to cloud-based system, the RTO is able to access emails, including deleted emails during and after the Employees period of employment;
- Information about file transfers of documents which are the IP of the RTO are retained and tracked;
- Websites visited on RTO devices are recorded and some sites may be restricted.

9. Legislation

This policy reflects our commitment to the following legislation:

- National Vocational Education and Training Regulator Act 2011 (NVR Act) (Commonwealth)
- The Privacy Act 1988 (Privacy Act) (Commonwealth)
- Freedom of Information Act 1992 (WA)
- Information Privacy Bill 2007 (WA)

10. Monitoring and Improvement

Policy Review

This policy will be reviewed each year and as a standing item, include details of the date it was reviewed and any changes.

- November 2022 - initial creation

Policy Additions or Amendments

Separate to the mandated annual review, the policy may be varied at any time due to legislative changes or to fall in line with widely accepted best practices in the workplace. In the event of any changes, the policy will be updated, and relevant stakeholders advised.

<NAME> (POSITION)