1.0 Purpose

1.1 Evanita Pty Ltd, PaysOnline and Paylink (the Company) recognise the importance of ensuring that appropriate measures are in place to:

1.1.1 effectively respond to an actual or suspected data breach involving data or information in any form or medium held by the Company (Data); and

1.1.2 ensure compliance with the relevant legislative framework under the Privacy Act 1988 (Cth) (the Act) concerning personal information data breaches.

1.2 This Data Breach Policy should be read in conjunction with the Company's Privacy Policy.

1.3 The Company is committed to protecting the privacy of personal information. The Company is required to comply with the Australian Privacy Principles contained in the Act (APPs). The APPs regulate the way personal information is handled by the Company.

1.4 As a provider of payroll and related services, and an employer, the Company is required to collect, use and disclose personal information. Personal information includes all information or opinion, whether true or not and whether recorded in a material form or not, about an individual. This includes (but is not limited to) the information that the Company holds in relation to prospects, clients, employees of clients, contractors to clients, staff, contractors, and even information regarding individuals who attend Company functions.

1.5 The APPs specifically require the Company to take reasonable steps to protect personal information from misuse, interference, loss, unauthorised access, modification or disclosure. This Policy is part of the Company's endeavours to comply with this obligation.

1.6 This Policy sets out the procedures and clear lines of authority for staff in the event that the Company experiences a data breach (or suspects that a data breach has occurred), where that data breach affects data or information stored electronically. The aim of this Policy is to ensure that the Company responds appropriately to a data breach and (to the extent possible) effectively mitigates any loss or damage arising from the data breach.

1.7 The flowchart at Figure 1 sets out a diagrammatic representation of the appropriate responses, options, and escalations for Company staff members in the event that a data breach has occurred, or is suspected to have occurred.

2.0 What is a data breach?

2.1 The Company hosts a large amount of Data in both physical and digital form as part of its provision of payroll services and administration of such. This can include client and client employee information, financial information, and supplier information. For the purposes of this Policy, a "data breach" occurs when electronic Data is lost or subjected to unauthorised access, modification, use or disclosure or other misuse by Company staff, contractors or any external parties and can occur inadvertently or maliciously. Data breaches are not limited to malicious actions, such as a theft of equipment or technology storing electronic Data or 'hacking' but may arise from internal errors or failure to follow information handling policies that cause accidental loss or disclosure. Data breaches can include:

2.1.1 instances where an unauthorised party maliciously accesses the Company's systems;

2.1.2 where portable devices, such as laptops, smartphones or storage devices are lost, stolen or not disposed of appropriately;

2.1.3 where emails are inadvertently sent to the incorrect recipient;

2.1.4 abuse of electronic access privileges by staff; and

2.1.5 the publishing of confidential material on social media or the internet generally.

2.2 Data breaches can be caused or exacerbated by a variety of factors, and can affect different types of information, including personal information, intellectual property and corporate or commercial information. Data breaches give rise to a range of actual or potential harms to individuals, agencies and organisations.

2.3 The Company strives to ensure the security of Data held by its systems but will react swiftly and proactively in instances where data breaches occur in accordance with this Policy. This enables the Company to contain, assess and respond to data breaches in a timely fashion and to help mitigate potential harm to affected individuals, the Company or third parties. This Policy 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 Company in responding to a data breach.

2.4 While this Policy deals with data breaches regarding all types of Data held by the Company, it also specifically seeks to assist the Company in meeting its obligations in relation to personal information data breaches.

3.0 Data breach notification requirements

OVERRIDING PRINCIPLE: All data breaches (actual or suspected), no matter how minor, must be reported to the Director of IT. Immediate notification is paramount. Nothing in this section should be taken to indicate that any report is necessary prior to notifying any other staff member.

3.1 What should a staff member who discovers the data breach do?

3.1.1 **Immediately Notify** each of:

- Director of IT; and
- Your supervisor.

3.1.2 **Record**:

- The time and date the suspected breach was discovered;
- The type of data involved, the cause and extent of the breach, and the context of the affected Data and the breach.

3.2 What should the supervisor notified of a data breach do?

3.2.1 Immediately escalate the matter to, or (if already notified) contact the Director of IT.

3.2.2 Pass on all relevant information to the Director of IT, verbally as well as by email. Information may include:

A description of the breach or suspected breach;

- Details of the action, if any, taken by the supervisor to address the breach or suspected breach;
- The outcome of that action, including a view as to whether any further action is required and the basis for that view; an
- Confirmation that the incident has been recorded in the Company's Data breach incident log and that a copy of that email in the folder specified in Section 10.0.

4.0 Data breach roles and teams

OVERRIDING PRINCIPLE: To protect data and contain any breaches (actual or suspected).

Non-escalated Breaches

4.1 The Director of IT may determine that the extent, severity or likely impact of the data breach is such that no further escalation is required, and it can be dealt with by the Director of IT, in accordance with the guidance set out in sections below (to the extent the Director of IT considers relevant) (Non-escalated breaches).

4.2 In the case of Non-escalated breaches, when the Director of IT considers that the breach has been responded to and resolved, the Director of IT must provide a report to the Company Principal and Company Director, setting out:

4.2.1 a description of the breach or suspected breach;

4.2.2 details of the action, if any, taken by the Director of IT to address the breach or suspected breach; and

4.2.3 the outcome of that action,

4.2.4 and, where the report is sent by email to the Company Principal the Director of IT must save of copy of that email in the folder specified in Section 10.0 below. The Company Principal must determine whether the Company Insurer should be notified.

Escalated Breaches

4.3 Where the Director of IT determines that the extent, severity or likely impact of the data breach is such that further escalation is required, the Director of IT must immediately notify the Company Principal and provide all relevant details of which the Director of IT is aware (Escalated Breach).

4.4 The Company Principal, upon being notified of an Escalated Breach, must:

4.4.1 work with the Director of IT to assess the severity of the breach;

4.4.2 notify the Company Director of the Escalated Breach; and

4.4.3 convene the Incident Management Team (as defined in Section 4.5 to 4.7 below).

4.4.4 Notify the Company's Insurer.

4.5 Upon being notified of an Escalated Breach, the Company Principal must appoint and mobilise a specialised team to respond to the data breach (Incident Management Team). The Incident Management Team will comprise subject matter experts (for example, Company staff with expertise in privacy and technology), departmental representatives and executives best placed and most suited to respond to, mitigate the impact of and take the appropriate actions in relation to, the data breach, as determined by the Company Principal. The Incident Management Team will likely comprise representatives from the Company's legal and IT department as well as the Director of IT, the Director of Finance, and Company Director, the "owner" of the data in respect of which the breach has occurred, and the Company's Marketing and Communications Officer.

4.6 Upon being mobilised, the Incident Management Team must respond to, resolve and review the data breach in accordance with Sections 5.0 to 9.0 below.

4.7 When the Incident Management Team considers that the breach has been responded to and resolved, the Incident Management Team must provide a report to the Company Director, setting out:

4.7.1 a description of the breach;

4.7.2 details of the action taken by the Incident Management Team to address the breach; and

4.7.3 the outcome of that action,

4.7.4 and, where the report is sent by email, a copy of that email must be saved in the folder specified in Section 10.0 below.

5.0 Data breach checklist: overview

Process

5.1 This Section provides guidance for the:

5.1.1 Director of IT, in the case of Non-escalated breaches; and

5.1.2 the Company Principal and Incident Management Team in the case of Escalated Breaches,

5.1.3 the Responding Person(s) on how to assess the severity of and respond to a data breach.

5.2 There is no single method or process for 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. Company staff should be aware that there are serious ramifications for breach of the legal obligations placed on the Company in relation to data breaches.

5.3 However, there are four key steps to consider when responding to every breach or suspected breach (Key Steps).

KEY STEP 1: Contain the breach and do a preliminary assessment

KEY STEP 2: Evaluate the risks associated with the breach

KEY STEP 3: Notification

KEY STEP 4: Prevent future breaches

5.4 The Responding Person(s) should ideally undertake Key Steps 1, 2 and 3 either simultaneously or in quick succession.

5.5 The Responding Person(s) should refer to the following guide published by the Office of the Australian Information Commissioner (OAIC):

Data breach notification - A guide to handling personal information security breaches. This guide provides further detail on each of the Key Steps and is available at: https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches.

5.6 Depending on the breach, not all Key Steps may be necessary, or some Key Steps may be combined. In some cases, it may be appropriate to take additional steps that are specific to the nature of the breach.

5.7 In reconsidering processes and procedures to reduce the risk of future breaches (Key Step 4), the Responding Person(s) should also refer to the following guide published by the OAIC:

Guide to securing personal information - 'Reasonable steps' to protect personal information. This guide presents a set of non-exhaustive steps and strategies that may be reasonable to take to secure personal information and considers actions that may be appropriate to help prevent further breaches following an investigation. Available by visiting: https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information.

5.8 Sections 6.0 to 9.0 below, in relation to the Key Steps, are intended to guide the Responding Person(s) in the event of a data breach and alert the Responding Person(s) to a range of considerations when responding to a data breach. In the event of any ambiguity, legal advice should be sought.

6.0 STEP 1: Contain the breach and make a preliminary assessment.

6.1 If considered necessary, in the case of Escalated Breaches, an externally sourced breach response team will be provisioned to provide specialist support.

6.2 Immediately contain breach if this has not already been done. Building security or IT security should be alerted if necessary. As noted above, often with IT system attacks a breach can be of a current or continuing nature. Therefore, in those circumstances, it is very important for appropriate IT security personnel to be alerted so that appropriate action can be undertaken.

6.3 In the case of Escalated Breaches, keep the Company Director informed and provide ongoing updates on key developments.

6.4 Ensure evidence is preserved that may be valuable in determining the cause of the breach or allow appropriate corrective action to be taken.

6.5 Consider developing a communications or media strategy to manage public expectations and media interest, working with the Company's Marketing and Communications Officer.

7.0 STEP 2: Evaluate the risks for individuals associated with the breach

7.1 Conduct an initial investigation, and collect information about the breach promptly, including:

7.1.1 the date, time, duration, and location of the breach.

7.1.2 the type of Data involved in the breach;

7.1.3 how the breach was discovered and by whom;

7.1.4 the cause and extent of the breach;

7.1.5 a list of the affected individuals, or possible affected individuals;

7.1.6 the risk of serious harm to the affected individuals; and

7.1.7 the risk of other harms.

7.2 Establish the cause and extent of the breach.

7.3 Assess priorities and risks based on what is known.

7.4 Keep appropriate records of the suspected breach and actions of the Responding Person(s), including the steps taken to rectify the situation and the decisions made.

8.0 STEP 3: Consider the breach notification

8.1 Determine who needs to be made aware of the breach (internally, and potentially externally) at this preliminary stage. Consideration should be given to the substance and form of notification, with deliberation occurring as to the audience, purpose and possible action that could result from the notification.

8.2 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. The Company must notify the individual(s) concerned and the OAIC in the event of a personal information data breach where there is a real risk of serious harm arising from the breach. It is important to note that this includes non-monetary loss, such as reputational damage.

8.3 Consider whether other individuals or third parties should be notified, including the OAIC, police/law enforcement, or other agencies or organisations affected by the breach, or any other specific party which the Company is contractually required to notify of a data breach. As noted above, the Company must notify affected individual(s) and the OAIC in the event of a personal information data breach where there is a real risk of serious harm arising from the breach.

8.4 The context surrounding an incident, or the nature of the Data may be extremely relevant in guiding relevant personnel as to what subsequent action is necessary. This could include instances relating to Data that contains financial information which may be misappropriated with the intention of exploitation. In such circumstances, it may be necessary to alert the relevant individual or financial institution immediately to mitigate loss or damage incurred.

9.0 STEP 4: Review the incident and act to prevent future breaches

9.1 Fully investigate the cause of the breach.

9.2 In the case of Escalated breaches, report to the Company Director on outcomes and recommendations:

9.2.1 Update security and response plan if necessary.

9.2.2 Make appropriate changes to policies and procedures if necessary.

9.2.3 Revise staff training practices if necessary.

9.2.4 Consider the option of an audit to ensure necessary outcomes are affected.

10.0 Records management

Documents created by the notified supervisor, Director of IT, Company Principal, the Incident Management Team or any member of staff in relation to an actual or suspected data breach should be saved in the following folder: O:\Security\Data Breaches.

Figure 1 Escalation Process Flow