Data Breach Policy

1. Introduction

1.1 PSI2000 Ltd ("PSI", "we", "us") is committed to ensure the security and confidentiality of all personal data it processes. Every care is taken to protect the data from unlawful incidents to avoid data breach and unauthorised data disclosure.

2. Purpose

2.1 Under Data Protection law we have an obligation to have a framework for security and protection of all personal data during its lifecycle including clear lines of responsibility.
2.2 This policy applies to all employees, contractors, data processors and suppliers who work for us or on our behalf.
2.3 This policy sets out a clear plan and procedure for handling data breach incidents.
2.4 This policy relates to all types of personal data that PSI2000 processes.

3. Definition of Data Breach incident

3.1 In the context of this policy, an incident is an event that can compromise the confidentiality, integrity or availability of data.
3.2 An incident can be suspected or confirmed and includes:
3.2.1 Loss or theft of personal data or equipment on which such data is stored for example loss of computer, tablet or paper document
3.2.2 System failure which leads to loss of data
3.2.3 Unauthorised access, use or disclosure of personal data including data released by an act deceit
3.2.4 Unforeseen circumstances such as fire or flood
3.2.5 Website vandalism
3.2.6 Hacking attack
3.2.7 Human error

4. Reporting

4.1 Any individual who comes to know a data breach should report to IT personnel at "support@psi2000.com" immediately.
4.2 The Report should include incident's date and time, nature and scale and details of the person reporting. Refer to Appendix 1: Data Breach Report Form
4.3 The Data Protection Officer (DPO) must seek legal advice to determine if the incident needs to be reported to Information Commissioner's Office (ICO)

5. Assessing

5.1 The Data Protection Officer (DPO) will investigate the data breach and prepare a risk assessment report within 24hours of the incident being discovered, Refer to Appendix 2: Data Breach Assessment Form. The report will consider the following
5.1.1 The cause of data breach
5.1.2 The type of data involved and if there are protections in place for example encryption
5.1.3 The affected data subjects and possible risks to them
5.1.4 The wider consequences of the data breach

6. Containment and recovery

6.1 The immediate priority is to contain the breach and limit its impact.
6.2 The recovery team will use the risk assessment report to recover the losses and stop any further damage the breach could cause.
6.3 Expert advice may be sought to resolve the incident promptly.

7. Evaluation and response

7.1 Once the incident is contained, the Data Protection Officer (DPO) will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and
procedures should be undertaken.
7.2 Existing measures will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring. The review will consider:
7.2.1 Where and how personal data stored
7.2.2 Where the biggest risks lie including identifying potential weak points
7.2.3 Whether methods of transmission are secure; sharing minimum amount of data necessary
7.2.4 Staff awareness through additional training

8. Notification

8.1 The Data Protection Officer (DPO) will establish who may need to be notified. This can include:
8.1.1 Third parties such as the Police, The Information Commissioner's Office (ICO), banks and insurers. This would be appropriate where an illegal activity is likely to have happened.
8.1.2 Individuals whose personal data has been affected by the incident, and where it has been considered likely to result in a high risk of adversely affecting that individual's rights and freedoms. Notification will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks.
8.1.3 Unauthorised recipient of personal data and warn them of the consequences if they disclose the data to others.

9. Policy Review

This policy will be reviewed and updated when necessary to comply with latest regulation.
Last reviewed: May 2018.

Appendix 1
Data Breach Report Form

If you discover a data breach, please complete section 1 of this form and send it to support@psi2000.com as soon as possible.

Section 1 – Report of Data Breach	
Date incident discovered	
Date incident reported	
Location incident happened	
Contact details of the person reporting (Name, Email address, Telephone number)	
Brief Description of incident	
Number of Data Subjects affected by incident (if known)	
List possible risks involved	
Brief description of actions taken	

Section 2 – To be completed by DPO	
Received by	
Date	
Actions Take	

Appendix 2
Data Breach Assessment Form

Section 1 – Assessment **Assessment Number**	eg year/001
Cause/s of Data Breach	
Details of devices involved	
Details of information lost, include nature of information and scale of loss	
What are the consequences of the loss?	
How many data subjects affected?	
Are there any security arrangements in place?	
Can the information be used to commit identity fraud? If yes give details	
Details of significance damage or distress to data subjects	
Should this breach be reported to ICO	

Section 2 – Actions	
Details of actions taken by responsible persons	
Was the incident been reported to:	
Police – if yes give details	Date: Ref No:
ICO – If yes give details	Date Ref No:

Other Third Parties – If yes give details	
Notification to Data Subjects – If yes give details	
Completed by:	Name: Date: