Incident Response Policy

1.0 Introduction

1.1 Alfaplas Ltd holds, processes and shares a large amount of data, including personal data, on its employees.

1.2 Every care is taken to protect data from accidental and/or deliberate incidents that could result in a breach and compromise security of data.

1.3 Compromise of information, confidentiality, integrity or availability may result in harm to individuals, reputational damage, legislative non-compliance and/or financial costs.

2.0 Purpose

2.1 The General Data Protection Regulation (GDPR) requires us to implement appropriate technical and organisational measures to protect data, including personal and sensitive data against accidental or unlawful destruction, accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves transmission of data over a network, and against all unlawful forms of processing.

2.2 Such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

2.3 This policy sets out the procedures that should be followed to ensure a consistent and effective approach for managing data breaches.

2.4 The objective of this policy is to contain any breaches, minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent any further breaches.

3.0 Scope

3.1 This policy relates to all data, including personal data and sensitive personal data, held by Alfaplas Ltd, regardless of the format in which the data is stored.

3.2 The provisions contained in this policy will apply to all staff, including temporary and casual staff, contractors, consultants, suppliers and Data Processors working for or on behalf of the company.

4.0 Definitions

4.1 Personal data is defined as any information relating to an identified or identifiable Data Subject.

4.2 An identifiable Data Subject is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that Data Subject.

4.3 A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

4.4 An incident is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately and has caused or has the potential to cause, damage to the company's reputation.

4.5 An incident includes, but is not restricted to:

- Loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad/ tablet or paper record);
- Equipment theft or failure;
- Unauthorised use of, access to or modification of data or information systems;
- Attempts (failed or successful) to gain unauthorised access to information of IT systems;
- Unauthorised disclosure of sensitive/ confidential data;
- Website defacement;
- Hacking;
- Unforeseen circumstances such as fire or flood;
- Human error;
- "Blagging" offences where information is obtained by deceiving the organisation who holds it.

5.0 Reporting

5.1 Any individual who accesses, uses or manages information for or on behalf of Alfaplas Ltd, is responsible for reporting a data breach to the Data Controller.

5.2 Any breach (regardless of format) should be reported within 12 hours.

5.3 An Incident Report Form should be filled out as part of the reporting process. A copy of the form can be downloaded from the GDPR folder on the F drive. This is accessible to all employees.

5.4 If a report form cannot be filled out within the 12 hour timeframe then an email should be sent to the Controller detailing the following:

- Name & contact details of reporter;
- Full and accurate details of the incident;
- Date and time of when the breach occurred;
- The nature of the data affected;
- How many individuals are thought to be affected.

5.5 The Data Controller can be contacted at:

Alfaplas Ltd
Unit 1 Ramsden Road
Rotherwas Industrial Estate
Hereford
HR2 6LR

Phone: 01432 262626 Email: data.protection@alfaplas.co.uk Website: www.alfaplas.co.uk

6.0 Containment & recovery

6.1 The first course of action should be to determine whether a breach is still occurring. If so, appropriate steps will be taken immediately to minimise the effects of the breach.

6.2 An initial assessment will be made to establish the severity of the breach and to determine who should take the lead investigating the breach. This will be dependent on the nature of the breach.

6.3 The leading investigator will establish whether anything can be done to recover any losses and limit any damage that may be caused by the breach and to determine a suitable course of action.

6.4 The leading investigator will also establish who needs to be notified as part of the initial containment and, where appropriate, will inform the police of the breach.

7.0 Investigation & risk assessment

7.1 An investigation will be undertaken within 24 hours of the breach being reported.

7.2 The lead investigator will investigate the breach and assess the risks associated with it, taking into consideration the following:

- The potential adverse consequences for the individual;
- How serious or substantial those consequences are;
- How likely those consequences are to occur.

7.3 The investigation should take into account the following:

- The type of data involved;
- Its sensitivity;
- The protection in place (such as encryption of electronically stored data);
- What has happened to the data (i.e. whether it has been lost or stolen);
- Whether the data could be put to any illegal or inappropriate use;
- Who the affected individuals are, the number of individuals involved and the potential effects on those Data Subjects;
- Whether there are wider consequences to the breach.

8.0 Notification

8.1 The lead investigator will determine who needs to be notified of the breach.

8.2 Every incident will be assessed on a case-by-case basis. However, the following will need to be taken into consideration:

- Whether there are any legal/ contractual notification requirements;
- Whether notification would assist the individual affected – could they act on the information to mitigate the circumstance?
- Whether notification would help prevent the unauthorised or unlawful use of personal data

8.3 Where it is likely the breach concerns personal data and will result in a risk to the rights and freedoms of individuals, it must be reported to the ICO within 72 hours of the Controller becoming aware of the suspected breach.

8.4 If a personal data breach is likely to result in a high risk of adversely affecting individuals rights and freedoms, those individuals will be informed without undue delay and not more than 48 hours after the ICO has been informed of the breach.

8.5 Notification to the individuals whose personal data has been affected will include a description of how and when the breach occurred and the data involved or believed to be involved. Advice will be given on what they can do to protect themselves and include what action has already been taken to mitigate the risks.

8.6 The lead investigators will consider notifying third parties such as the police, insurers, bank and/or credit card companies. This would be an appropriate course of action in cases where illegal activity is known or is believed to have occurred, or where there is a risk it is likely to occur.

8.7 A record of any personal data breaches will be recorded regardless of whether the ICO or Data Subject has been notified.

9.0 Evaluation & Response

9.1 Once the initial incident is contained, a full review of the causes of the breach, the effectiveness of the response and whether there needs to be any changes to systems, policies and procedures, will be undertaken.

9.2 Existing controls will be reviewed to determine their adequacy and whether any corrective action should be taken to minimise the risk of a similar incident occurring again.

9.3 The review will consider:

- Where and how personal data is held and stored;
- Where the biggest risks lie and identifying any further potential weak points within its existing measures;
- Whether methods of transmission are secure;
- Staff awareness;
- Whether the current policy for reporting a breach and the individuals responsible for reacting to a reported breach, is adequate.

9.4 If it is deemed necessary, a report recommending any changes to systems, policies and procedures will be taken into consideration.

10.0 Related policies

10.1 This policy should not be read in isolation. The following documents also include specific and supporting information;

i. The Schedule – Information we collect and hold;
ii. Privacy Policy;
iii. Privacy Notice;
iv. Sphere Code of Conduct;
v. Employee Handbook, with particular reference to –

- *Section 1.7 – Data Protection*
- *Section 2.2 – Personnel Records*
- *Section 2.8 – Computer Use*
- *Section 2.12 - CCTV*

10.2 A copy of any of the above documents can be obtained from the HR Department.