# Information Security Breach Management

## 1. Introduction

1.1 This management process outlines elements to consider and address in the event of data loss or an information security breach. It will assist Sustainable Tech 4 Good Group Ltd & Veritas Digital Services Ltd in determining appropriate courses of action if a security breach confidential data occurs and dealing with any security breach effectively.

1.2 Data loss and security breaches can happen for a number of reasons and occur in different contexts. They may encompass more than personally identifiable information (e.g. trade secrets, intellectual property, or client data of whatever nature).

1.3 The Company takes appropriate measures against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or client data. This breach management process constitutes one of these measures and supports the Company's obligations under GDPR.

## 2. Breach management

**2.1** Breaches of information security must be reported as soon as discovered and notified in accordance with the protocols outlined in 3.3 below**.**

2.2 Breach management has four important strategic elements. When a security breach is discovered the priorities are:

a. **containment and recovery**, to limit as far as possible any damage.

b. **assess the risks associated with the breach**. A risk assessment will help inform decisions about remedial actions and notification.

c. **notifying the appropriate people/organisations** that a breach has occurred.

d. **understanding the causes and evaluating the effectiveness of our response** to the incident, revising as necessary our information security measures in the light of any findings.

2.3 Where we hold data supplied by a third-party organisation, where there is a contractual duty to report an incident to that organisation within a particular timeframe, we will respect the reporting timescales and guidelines agreed in any such agreement or contract.

2.3 The Company will monitor and review any information security incidents to identify recurring incidents and areas of risk.

## 3. Process

3.1 **Containment and Recovery**

(i) Ascertain the extent and nature of the breach – see 3.2 – Risk Assessment

(ii) Establish who needs to be made aware of the incident and inform them of what they must do to assist in the containment/recovery exercise. E.g. Finding lost piece of equipment, changing passwords or access codes, isolating/closing part of network, informing police, checking any contractual obligations to act/report where data has been supplied under contract.
(iii) Ensure that any possibility of further data loss is removed or mitigated as far as possible
(iv) Determine whether anything can be done to recover any losses and limit any damage that may be caused.

3.2 **Risk Assessment** - To identify and assess the ongoing risks that may be associated with the breach. In particular: an assessment of (a) potential adverse consequences for individuals or clients, (b) their likelihood, extent and seriousness. Determining the level of risk will help define actions in attempting to mitigate those risks.

(i) What type and volume of data is involved?
(ii) How sensitive is the data and could it be misused?
(iii) What has happened to the data? E.g. if the data has been stolen, it may be used for harmful purposes, whereas damaged sustained to data would present a different level of risk.
(iv) If data is lost or stolen, were any protections in place to prevent access or misuse? E.g. Encryption
(v) If data is damaged/corrupted/lost can it be recovered from back-ups or copies?
(vi) Who is affected by the breach? E.g. staff or clients
(vii) Are there wider consequences to consider? E.g. reputational loss etc.

3.3 **Notification** – consider any necessary notification of people, clients or organisations

(i) Determine whether there are any contractual obligations to notify – eg for clients where notification is part of the contract we hold with them
(ii) Determine whether the breach is reportable to the ICO, and make notification as soon as possible – and within 72 hours of identification
(iii) Determine whether data subjects need to be notified of the breach, e.g. employee data
(iv) Consider any third parties that may need to be notified to help with response or mitigation – e.g. insurers, banks, credit card companies
(v) Consider how to notify: Include a description of how and when the breach occurred and what data was involved. Include details of what has already been done to respond to the risks posed by the breach. Provide a way in which they can contact us for further information or to ask questions about what has occurred

3.4 **Evaluation**- To evaluate the effectiveness of the Company's response to the breach, and learn any lessons in the light of findings or experience.

(i) Establish where any present or future risks lie.
(ii) Consider and identify any weak points in existing security measures and procedures.
(iii) Consider and identify any weak points in levels of security awareness/training and address these through training or advice.

Approved By: Sue Gowling
Date: 29th November 2019 Reviewed: 27th January 2026