Legate Group Limited

Incident Management Policy

Revision History

Version	*Revision Date*	*Revised By*	*Section Revised*
V1	30/09/2014	T. Clarke	
V2	25/01/2018	T. Clarke	
V3	25/05/2018	T. Clarke	
V4	06/10/2018	T. Clarke	
V5	07/10/2019	T. Clarke	

Document Control

Document Owner:	***Next Review Date:***	***Version:***	***Unit:***
T. Clarke	***30/07/2023***	***V5***	***C&BR***
Latest Review Comments: ***Minor amendments to spelling, grammar and inclusion of the Risk Management Database.***			

Incident Management Policy
Tony Clarke
Last Reviewed: 30/07/2022
V5

1. TITLE

Incident Management Policy

2. POLICY STATEMENT

The Company is committed to ensuring normal business operations are maintained, but we recognise that on occasions the Company's service may be interrupted for a variety of reasons.

It is the Company's aim through this policy to restore normal service operations as quickly as possible, whilst minimising the impact to the business and its' clients, in the event that the Company suffers a severe incident.

3. PURPOSE

This document sets out the Company's policy relating to Incident management and the measures to be taken in order to protect it and its clients from losses arising from serious physical and/or technical incidents whether internal, external, deliberate or accidental.

4. SCOPE

All staff, contractors, agents and those appointed to act on behalf of the Company.

5. POLICY DETAILS

5.1 Detection and Recording

A major incident is one that incapacitates the business and/or is likely to have an adverse impact on the Company's or its' client's reputations.

All incidents must be notified to the Company's director and recorded in the Company's Risk Management Database.

5.2 Investigation, Diagnosis and Analysis

It will be the Company director's responsibility to investigate the incident and take steps to contain the incident and to restore operations in the short term and analyse the reasons leading to the incident.

5.3 Assessment of Ongoing Risk

Some incidents, for example, data security breaches will not lead to risks beyond

possible inconvenience to those who need the data to do their job. An example might be where a laptop is irreparably damaged but its files were backed up and can be recovered, albeit at some cost to the business. While these types of incidents can still have significant consequences, the risks are very different from those posed by, for example, the theft of a customer database, the data on which may be used to commit identity fraud.

The Company's director will assess the risks that may be associated with the incident breach and an assessment of potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen.

5.4 Ownership and Notification

The Company's director retains ownership of each incident and will notify its Client and regulators appropriately, but no later than within 48 hours of the breach identification and update the Company's Risk Management Database.

5.5 Evaluation and Response

It is important not only to investigate the causes of the incident, but also to evaluate the effectiveness of the Company's response to it. Clearly, if the breach was caused, even in part, by systemic and ongoing problems, then simply containing the breach and continuing 'business as usual' is not acceptable; similarly, if the response was hampered by inadequate policies or a lack of a clear allocation of responsibility then the Company will review and update its policies and lines of responsibility in the light of experience.