

# Legate Group Limited

## Incident Management Policy

### 1. Introduction

Legate Group (the "Company") is a commercial investigation company and operates as a small business. As such the Company's policy is designed to be proportionate to the risks and business size.

This document sets out the Company's policy relating to Incident management and the measures to be taken by all staff, contractors, agents and those appointed to act on behalf of the Company and by the Company as a whole in order to protect it and its clients from losses arising from serious physical and/or technical incidents whether internal, external, deliberate or accidental.

### 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 to through this policy to restore normal service operation 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. 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 Business Continuity Plan with major incidents being recorded in the Company's Risk Register.

### 4. 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. 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.

**6. 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 Register where appropriate.

**7. 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.

This Policy has been approved and authorised by:

**Name:** Anthony Paul Clarke  
**Position:** Director  
**Date:** 25/01/2018

Version Control:

Version	Date	Date Approved	Review
V1	30/09/2014	01/10/2014	30/09/2017
V2	25/01/2018	25/01/2018	30/09/2019
V3	25/05/2018	25/05/2018	30/09/2019
V4	06/10/2018	06/10/2018	30/09/2019