Demo Company Limited		
Information Security Incident Management Policy		
ISO/IEC 27001:2013		
Issue 3	**Schedule A.16 (16.1.1, 16.1.2, 16.1.3, 16.1.4, 16.1.5, 16.1.6 & 16.1.7) Information Security Incident Management.**	**Authorised by:- Directors of Demo Company Limited**
Page 1 of 2	**Effective Date: 1st Nov 2021**	**Classification :- Internal**
Issue Date: 1st Nov 2021	**Last Reviewed Date: 1st Nov 2021**	

Scope

Limited are committed to ensuring a consistent and effective approach to the management of information security incidents.

Responsibility and Authority

It is the responsibility of senior management to review this policy, and amend it where necessary.

Operators are responsible for following the policy, as set out below.

Control and Distribution

This procedure is issued as a controlled document and can only be updated by the authorised information management representative and must include a revision status and traceability of the change process.

A master is retained as part of the information security management system with uncontrolled copies issued at point of use.

The Policy

Demo Company Limited defines an information security incident as an attempted or successful unauthorised access, use, disclosure, modification or destruction of information; interference with information technology operation; or violation of acceptable use policies. A security incident may include any of the following:

- A breach, attempted breach or other unauthorised access of a Limited information resource originating from with the Limited network or an outside entity
- An exposure of sensitive or confidential non-public information
- An intentional disruption or attack impacting Limited information resources
- A loss or theft of an information system asset

Information security incidents should be reported through appropriate channels as quickly as possible.

All staff & authorised users granted use of Limited's information resources must notify senior management immediately of any suspected or real information security incident. If it is unclear as to

whether a situation should be considered an information security incident, senior management should be contacted to evaluate the situation.

In response to an information security incident, senior management will plan and coordinate the response and advise where appropriate. In carrying out this responsibility, senior management will ensure that important operational decisions are relayed to applicable regulatory authorities to protect the fundamental interests of the Company and others impacted by the incident.

Limited are required to report any breach to the Isle of Man Information Commissioner who are the 'Relevant Supervisory Authority', unless the breach is unlikely to result in a risk for the rights and freedoms of individuals, Limited ensures that notification of the breach to the Relevant Supervisory Authority is done so without undue delay and where feasible within 72 hours of becoming aware. If for any reason Limited are unable to notify the Relevant Supervisory Authority within 72 hours then a reasoned justification must be provided.

A Relevant Supervisory Authority may, in any case, request that the following details are provided:

- Description of the nature of the breach including (where possible)
    - The categories and approximate numbers of Data Subjects concerned
    - The categories and approximate number of data records concerned
- Description of the likely consequences
- Describe the measures taken or proposed to address the breach and mitigate possible adverse effects
- The name and contact details of the DPO

All of the above information can be provided together, or where that is not possible in phases without undue delay to the Relevant Supervisory Authority.

Senior management will be responsible for writing any final reports which summarises the findings regarding the information security incident and, if necessary, making recommendations for improvement of related information security practices and controls.