1. **Scope**

All reports of information security weaknesses or events relating to any of Retirement Capital’s information assets and events that should have been reported but were not are within the scope of this procedure. In addition, any events or weaknesses detected through company IT system monitoring (ISMS-C-DOC-6.1.4) fall within the scope of this procedure.

1. **Responsibilities**

Users are required to report information security weaknesses and events to the Information Security Manager, as set out in [ISMS-C DOC 16.1.2-3](ISMS-C_DOC_16.1.2-3.docx).

Owners of monitoring and alert services are responsible for reporting (using [ISMS-C REC 16.1.2-3b](ISMS-C_REC_16.1.2-3b.docx)) those events (or sequences of events) that fall within the scope of ISMS-C DOC 16.1.2-3.

The Information Security Manager is responsible for coordinating and managing the response to the any reported weakness or event, including documentation of all emergency steps taken, evidence collection, and closing out the event.

All technical staff and other [employees/staff], contractors or third parties, are required to support the Information Security Manager in dealing with an event or weakness.

The IT Manager authorises access to live systems or data.

Asset owners carry out actual accesses to live systems or data in dealing with an incident.

The Operations Director is responsible for the contingency planning components of the Working Instructions identified in 3.5 below.

1. **Procedure** [ISO27002 Clauses 16.1.1, 16.1.4, 16.1.5 and 16.1.6]
   1. The Information Security Manager logs (on Schedule [ISMS-C REC 16.1.2-3a](ISMS-C_REC_16.1.2-3a.docx)) all information security reports immediately upon receipt, allocating to each a unique number and uses this log to ensure that all reports are analysed and closed out.
   2. All information security events and weaknesses are, immediately upon receipt (see ISMS-C DOC 16.1.2-3), assessed and categorised (with reasons, on the face of ISMS-C REC 16.1.2-3b) by the Information Security Manager.

Initially, there are four categories: events, weaknesses, incidents and unknowns.

* ‘Events’ are occurrences that, after analysis, have no or very minor importance for information security;
* ‘vulnerabilities’ are weaknesses that, after analysis, clearly exist as significant weaknesses compromising information security;
* ‘incidents’ are occurrences of events (series of events) that have a significant probability of compromising Retirement Capital’s information security;
* ‘unknowns’ are those reported events or weaknesses that, after initial analysis, are still not capable of allocation to one of the four categories.
  1. The ‘unknowns’ are subject to further analysis to allocate them to one of the other three categories as soon as possible.

The **prioritisation** for responses, when there are multiple event reports to deal with, is:

* incidents,
* unknowns,
* vulnerabilities,
* events.

When there are multiple event reports in each category, the Information Security Manager prioritises responses in the light of the criticality of the business systems and information assets at risk, the danger of further compromise to Retirement Capital’s information security, and the resources at his/her disposal.

* 1. Incidents involving high-value or business critical systems (as identified under control section 8.1 of the [Manual](../Manual/001%20Information%20Security%20Manual.docx)) are immediately reported by the Information Security Manager to the Chief Information Security Officer (CISO (DIRECTOR)).
  2. Specific Work Instructions set out the necessary containment and corrective action and standing contingency plans in respect of the following types of information security incident:

Systems failure and loss of service ISMS-C DOC 16.?

Malware, including viruses ISMS-C DOC 16.?

Denial of service ISMS-C DOC 16.?

Errors resulting from poor data ISMS-C DOC 16.?

Breaches of confidentiality ISMS-C DOC 16.?

Breaches of information integrity ISMS-C DOC 16.?

Misuse of information systems ISMS-C DOC 16.?

Non-standard incidents ISMS-C DOC 16.?

* 1. The Information Security Manager seeks additional input from qualified technical staff, as necessary and where he considers the standing instructions to be inadequate, to analyse and understand the incident and to identify appropriate actions to contain it and to implement contingency plans.
  2. The Information Security Manager invokes actions as set out in the standing work instructions plus additional activity that he considers necessary to contain and recover from the incident, and to implement contingency plans.

The Information Security Manager confirms that the affected business systems have been restored and that the required controls are operational before authorising a return to normal working.

* 1. Once the incident is contained, and the required corrective action is completed, the Information Security Manager reports to the Chief Information Security Officer (CISO (DIRECTOR)) with a summary of the incident, identifying the cause of the incident and analysing its progress, trying to identify how Retirement Capital could have responded earlier or more effectively, or preventive action that might have been taken in advance of the information, the effectiveness of the containment and corrective actions and the contingency plans, and how the incident was closed out (see 3.9 below).
  2. The Information Security Manager is responsible for closing out the incident: this includes
* any reports to external authorities (see [ISMS-C DOC 6.1.3](../Control%20A6%20-%20organisation%20of%20information%20security/ISMS-C_DOC_6.1.3.docx));
* initiating disciplinary action by referring the incident to the Managing Director;
* planning and implementing preventative action to avoid any further recurrence;
* collecting and securing audit trails and forensic evidence (see [ISMS-C DOC 16.1.7](ISMS-C_DOC_16.1.7.docx));
* initiating any action for compensation from software, service or outsource suppliers by referring the incident to the Procurement Manager, and
* communicating with those affected by or involved in the incident about returning to normal working and any other issues.
  1. The Information Security Manager prepares a monthly report to the Information Security Committee which identifies (from the Event Reporting Log ISMS-C REC 16.1.2-3a) the number, type, category and severity of information security incidents during the preceding month, the cost of containment and recovery, and the total cost of the losses arising from each incident, and recommends (where appropriate) additional controls that might limit the frequency of information security incidents, improve Retirement Capital’s ability to respond, and reduce the cost of response.
  2. All the incident reports from the period since the last management review are taken into account at the next one, to ensure that Retirement Capital learns from the incidents.

***Document Owner and Approval***

The Information Security Manager is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the ISMS.

A current version of this document is available to all members of staff on the corporate intranet.

This procedure was approved by the Chief Information Security Officer (CISO (DIRECTOR)) on 14th November 2020 and is issued on a version-controlled basis under his/her signature.

Signature:

Date: 14/11/2020

**Change History Record**

|  |  |  |  |
| --- | --- | --- | --- |
| Issue | Description of Change | Approval | Date of Issue |
| 1 | Initial issue | Gavin McCloskey | 14/11/2020 |
|  |  |  |  |
|  |  |  |  |