1. **Scope**

All information gathered during the course of responding to an information security incident is potentially evidence to be used in a disciplinary, criminal or civil action. All such evidence is within the scope of this procedure.

1. **Responsibilities**

The Information Security Manager is responsible for collection and retention of information in respect of information security incidents.

The Chief Information Security Officer (CISO (DIRECTOR)) is responsible for ensuring that the Information Security Manager is trained to an adequate level in the techniques of evidence collection required in Retirement Capital’s jurisdiction.

1. **Procedure** [ISO27002 Clause 16.1.7]
   1. Where the likelihood of legal, civil or criminal action is established early in the incident response process, the police or lawyers are involved as early as possible and their guidance is sought and followed in respect of evidence collection and retention. If the event, or the possible action, spans organisational or geographic boundaries, specialists must be consulted to ensure that evidence can be collected and how it should be collected. External advisers or third parties are subject to NDA agreements, as required by [ISMS-C DOC 13.2.4](../Control%20A13%20-%20communications%20security/ISMS-C_DOC_13.2.4.docx).
   2. In all other cases, all originals documents have, attached to them, a signed and dated statement describing precisely of paper where, and under what conditions, it was found, who found it, who witnessed the event, together with a machine date-stamped photocopy of the document that indicates its original state.
   3. Either the original computer media should be removed and retained securely or copies of information on hard drives, in memory or on removable computer media should be taken (with a log of all actions during the copying process) with a witness present.
   4. Paper documents or magnetic media must be kept securely by the IT Manager will access limited to the CISO (DIRECTOR) or authorised delegate. Any access must be recorded by the IT Manager.

***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 |
|  |  |  |  |
|  |  |  |  |