Collection of Evidence

Reference: NIS DOC D1-05
DocumentKits Issue No: 1.0
DocumentKits Issue Date: 25/08/2021

1. Scope

All information gathered in the course of responding to an information
"or privacy"

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.

2. Responsibilities

The Information Security Manager is responsible for collection and retention of information in respect of information security
"and privacy"

incidents.

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

"The Data Protection Officer is responsible for ensuring that all information relating to privacy breaches necessary for reporting to personally identifiable information (PII) controllers, PII principals and regulators/authorities is collected as necessary."

3. Procedure

3.1 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,
"details of specialist lawyers"

must be consulted to ensure that evidence can be collected and advise how it should be collected. External advisers or third parties are subject to non-disclosure agreements.

3.2 In all other cases, all originals of paper documents have, attached to them, a

SAMPLE

"signed and dated"

statement describing precisely where, and under what conditions they were found, who found them, who witnessed the event, together with a machine date-stamped photocopy of the document that indicates its original state.

3.3 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.

3.4 Paper documents or magnetic media must be kept securely
"identify where, who is responsible for their safekeeping, who is authorised to access them, and what records must be kept of any accesses."

"3.5 Incidents are recorded, especially where PII is or could be affected. Records include sufficient information to provide a report for regulatory and/or forensic purposes, including:
3.5.1 A description of the incident;
3.5.2 The time period of the incident;
3.5.3 The consequences of the incident;
3.5.4 The name or source of the incident report;
3.5.5 To whom the incident was reported;
3.5.6 Steps taken to resolve the incident, including the person in charge and the data recovered;
3.5.7 Whether the incident affected unavailability, loss, disclosure or alteration of PII;
3.5.8 A description of the information and/or PII affected;
3.5.9 Whether or not regulators, customers, suppliers, partners and/or data subjects have been notified, and the steps taken to do so; and
3.5.10 [Other information.]

3.6 Records are retained [for how long?].

Document owner and approval

The Information Security Manager is the owner of this document and is responsible for ensuring that it is reviewed in line with the requirements of the management system.

The current version of this document is available to
"Specify which members of staff this document is intended for"

and is published
"Describe the location(s) - electronic and physical - where this document is available"

Its approval status can be viewed in the Master List of Document Approval.

SAMPLE