1. **Scope**

All *users* (whether *15*, contractors or temporary *15* and third party users) and all *[owners]* of *undefined* information security assets or systems are required to be aware of and to follow this procedure.

1. **Responsibilities**
   1. *Users* and *[owners]* of *undefined* information security assets are required to follow this procedure for reporting information security weaknesses or events and this is documented in User Agreements.
   2. Information security events and weaknesses are reported to the *34* in line with this procedure.
   3. The *34* is responsible for managing information security responses.
   4. The *20* is responsible user training and awareness and for selecting those events which can be used to support training activities.
2. **Reporting information security events and weaknesses**
   1. Information security weaknesses and events are reported, immediately after they are seen or experienced, on Form [ISMS-C REC 16.1.2-3b](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_REC_16.1.2-3B.docm).
   2. *Users* are not allowed to continue working after identifying a possible weakness or information security event.
3. **Information security incident management procedures**
   1. The *34* logs (on Schedule [ISMS-C REC 16.1.2-3a](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_REC_16.1.2-3A.docm)) all information security reports immediately upon receipt, allocating 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 assessed and categorised by the *34*. 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 *undefined*’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.
   3. The ‘unknowns’ are subject to further analysis to allocate them to one of the other three categories as soon as possible.
   4. The prioritisation for responses, when there are multiple event reports to deal with, is: incidents, unknowns, vulnerabilities, events.
   5. When there are multiple event reports in each category, the *34* prioritises responses in the light of the criticality of the business systems and information assets at risk, the danger of further compromise to *undefined*’s information security, and the resources at his/her disposal.
   6. Specific Work Instructions set out the necessary containment and corrective action and standing contingency plans.
   7. The *34* 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.
   8. *[Where necessary, the 34 coordinates activity with other organisations.]*
   9. The *34* confirms that the affected business systems have been restored and that the required controls are operational before authorising a return to normal working.
   10. Once the incident is contained, and the required corrective action is completed, the *34* reports to the *5* with a summary of the incident.
   11. The *34* is responsible for closing out the incident: this includes any reports to external authorities (see [ISMS-C DOC 6](file:///Users/NEW%20ISMS/ISMS%20Development/ISO27001-FastTrackToolkit-v1.0/ISMS_DOC_6.docm)); initiating disciplinary action by referring the incident to the *20*; planning and implementing preventative action to avoid any further recurrence; collecting and securing audit trails and forensic evidence (see [ISMS-C DOC 16](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_DOC_16.docm)); initiating any action for compensation from software, service *[or outsource]* suppliers, and communicating with those affected by or involved in the incident about returning to normal working and any other issues.
   12. The *34* prepares a monthly report to the *33* 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 *undefined*’s ability to respond, and reduce the cost of response.
   13. All the incident reports from the period since the last management review are taken into account at the next one, to ensure that *undefined* learns from the incidents.
4. **Collection of evidence**
   1. In all information security incidents, irrespective of whether or not a follow-up action against a person or organisation involves legal action (either civil or criminal), evidence is collected, retained and presented as set out in ISMS-C REC 16.1.2-3a to conform to the rules for evidence laid down in [insert details of your legal jurisdiction(s)]

***Document Owner and Approval***

The *34* 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/specified*] members of staff on the *[corporate intranet]* and is published *[ ]*.

This procedure was approved by the *5* on *[date]* and is issued on a version controlled basis under his/her signature.

Signature: Date:

**Change History Record**

|  |  |  |  |
| --- | --- | --- | --- |
| Issue | Description of Change | Approval | Date of Issue |
| 1 | Initial issue | <Manager> | Xx/yy/zz |
|  |  |  |  |
|  |  |  |  |