Responding to Information Security Reports

Document History

1.

#	Version	Date	Created/ Modified by	Change Doc. No & Brief description of the change incorporated	Approved by / Approved Date
1	1.0	24th July 2024	Zamir Shaikh	Created the initial version.	Azim Shaikh

Responding to Information Security

1. Scope

All reports of information security weaknesses or events relating to any of the Organization's information are within the scope of this procedure. In addition, any events or weaknesses detected through logs on the servers, firewall, physical access control devices as well as audits conducted by the ISMS Head fall within the scope of this procedure.

2. Responsibilities

2.1. Users are required to report information security weaknesses and events to the IT Services team, as set out in DOC 13.1.
2.2. Owners are responsible for reporting (using REC 13.1A) those events (or sequence of events) that fall within the scope of DOC 13.1
2.3. The IT Services team is responsible for coordinating and managing the response to any reported weakness or event, including documentation of all emergency steps taken, evidence collection, and closing out the event.
2.4. All technical staff and other employees, contractors or third parties, are required to support the IT Services team in dealing with an event or weakness.
2.5. IT Services team authorizes access to live systems or data to authorized individuals who are concerned with the incident management.
2.6. ISMS Head is responsible for reviewing and analyzing the security event.
2.7. The ISMS Head is responsible for the contingency planning components of the Working Instructions identified in 3 below.

3. Procedure [ISO 17799 clauses 13.2.1 and 13.2.2]

3.1. The ISMS Head logs (on schedule DOC 13.5) all information security reports immediately upon receipt, allocating to each a unique number and uses this log to ensure that all reports are analyzed and closed out.
3.2. Upon receipt of any information security event, it is assessed immediately and categorized (with reasons, in Helpdesk tool) by the IT Services team. 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 or series of events that have a significant probability of compromising the Organization'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. or
3.3. The "unknowns" are subject to further analysis to allocate them to one of the other three categories as soon as possible.
3.4. The prioritization for responses, when there are multiple event reports to deal with, is: incidents, unknowns, vulnerabilities, events.
3.5. When there are multiple event reports in each category, the IT Services team in consultation with ISMS Head prioritizes responses in the light of the criticality of the business systems and information assets at risk, the danger of further compromise to the Organization's information security, and the resources at his disposal.

Responding to Information Security

3.6. Incidents involving high-value or business critical systems (as identified under section 7.1 of the Manual) are immediately reported by the ISMS Head to the Managing director.

3.7. The IT Services team seeks additional input from qualified technical staff, as necessary and where he considers the standing instructions to be inadequate, to analyze and understand the incident and to identify appropriate actions to contain it and to implement contingency plans.

3.8. The IT Services team invokes actions that he considers necessary to contain and recover from the incident, and to implement contingency plans.

3.9. The IT Services team confirms that the affected business systems have been restored and that the required controls are operational before authorizing a return to normal working.

3.10. Once the incident is contained, and the required corrective action is completed, the IT Services team reports a summary of the incident, identifying the cause of the incident and analyzing its progress, trying to identify how the Organization could have responded earlier or more effectively, or preventative 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.

3.11. The IT Services team is responsible for closing out the incident: this includes any reports to external authorities (see DOC 6.6); initiating disciplinary action by referring the incident to the HCM; planning and implementing preventative action to avoid any further recurrence; collecting and securing audit trails and forensic evidence (see DOC 13.4); initiating any action for compensation from software, service suppliers by referring the incident to the ISMS Head, and communicating with those affected by or involved in the incident about returning to normal working and any other issues.

3.12. The ISMS Head prepares a quarterly report to the Information Security Committee which identifies (from the event reporting log DOC 13.5) the number, type, category and severity of information security incidents during the preceding month, the cost of containment and recovery, and where possible, 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 the Organization’s ability to respond, and reduce the cost of response.

3.13. All the incident reports from the period since the last management review are taken into account at the next one, to ensure that the Organization learns from the incidents.

3.14. In the case of a personal data breach, the processor shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the data protection officer in accordance with Article 55.

4. The notification referred to Art. 33 GDPR;

a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

Responding to Information Security

c) describe the likely consequences of the personal data breach;

d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The ISMS Head 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 specified members of staff on the corporate intranet and is published.

This policy was approved and is issued on a version controlled basis under the signature of the director.