Reporting Information Security Weaknesses and Events

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

Reporting Information Security

1. Scope

All users (whether employees, contractors and third party users) and all Owners of Organizational information security assets or systems are required to be aware of and to follow this procedure.

2. Responsibilities

2.1. Users and Owners of Organizational information security assets are required to follow this procedure for reporting information security weaknesses or events and this is documented in user agreements.
2.2. Information security events and weaknesses are reported to the IT Services team in line with this procedure.
2.3. The IT team in coordination with ISMS Head is responsible for the overall managing information security responses (see DOC 13.2)
2.4. The HCM is responsible for user training and awareness and for selecting those events which can be used to support training activities.

3. Procedure [ISO 17799 clauses 13.1.1, 13.1.2 and 15.2.2]

3.1. Information security weaknesses and events are reported and logged into the Helpdesk tool, immediately when they are seen or experienced. The reports are available in the form of soft copy with the IT Services team in the Helpdesk tool.
3.2. Momentarily users are not allowed to continue working after identifying a possible weakness or information security event.
3.3. The IT Service team reports back to describe how the event was dealt with and closed out.
3.4. All the findings are logged in to the Helpdesk tool, and any documentation arising from the event and the response that has been generated as per the DOC 13.2.

4. Reporting Privacy Concerns – External Parties

4.1. Prospects can contact DPO using following methods;
4.1.1 Email to the following email address i.e. dpo@mondialbusinesses.com
4.1.2 Form submission from the portal i.e. https://mondialbusinesses.com/Preferences/
4.1.3 Postal Mailing Address - Attn: Data Protection Officer (DPO)
Office No 1 & 2, Arihant Avenue, Divya Nagar, Wanwadi,
Pune, Maharashtra 411040

5. Tracking of logged Incident

5.1. A unique case – ID is generated to track the incident.

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.

Reporting Information Security

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