06 ESTABLISH A STANDARD OPERATING PROCEDURE FOR DATA INCIDENT MANAGEMENT WITHIN THE OFFICE

Purpose:

Data incident management enables actors to address data incidents and supports the development of a knowledge base to help prevent and better address future incidents. Communicating about data incidents fosters more coordinated approaches to incident management over time and creates awareness across the sector.

Policy Requirement:

☐ Where the data incident involves personal data or non-personal data in a sensitive context, OCHA must adhere to the obligations established in section 15 of the UN Secretariat Data Protection and Privacy Policy.

Recommended Approach:

☐ The SOP for Data Incident Management should be prepared jointly by an HAO and IMO and be approved by OCHA's data protection focal point and the Head of Office. It should be aligned with other incident management procedures (e.g., applicable UNDSS guidance).

☐ The SOP should include a process for notification, classification, treatment and closure of the incident. It should also specify appropriate channels for rectification and redress for individuals impacted by data incidents.

☐ Establish a data incident registry to capture key details about the nature, severity and resolution of each incident, as well as any mitigation measures taken to prevent future incidents.

☐ Share the data incident registry with the data protection focal point.

☐ OCHA offices should share their experience in managing and mitigating data incidents with other actors, i.e., at the cluster/sector and system-wide levels to foster more coordinated approaches to incident management.

Relevant Tool or Template:

OCHA SOP for Data Incident Management Template

OCHA Data Incident Registry Template

[21] Including forthcoming administrative issuances on data protection and privacy from the United Nations Secretariat.