Cybersecurity Incident Management

Data Breaches

1 Any data breach must be immediately reported according to the Cybersecurity Incident Management Rule and related procedure.

Incident Response

Reporting information security events

2 All users are responsible for reporting Cybersecurity breaches to cybersecurity@who.int.

Incident response phases

3 Cybersecurity events must be assessed to identify impact and severity.
4 The containment phase and return to normal operations must be subject to a risk assessment.
5 Actions performed during each incident response phase must be documented, and evidence of actions collected.
6 WHO Acceptable use of computing resources must be adhered to when accessing personal information.
7 Post incident review must be carried out and lessons learned documented.

Security Operations

8 All end-user computers, and all servers, regardless of operating system, must be equipped with the Endpoint Detection and Response agent specified by the Cybersecurity Team.
9 Logs from all servers, regardless of operating system or hosting environment, must be able to ship logs to the SIEM solution specified by the Cybersecurity Team.
10 Documentation must be available in the Cybersecurity Risk Assessment library for all IT products being operated by or on behalf of WHO, so that the Security Operations Centre agents can quickly understand the architecture and attack surface of the product.