CYBERSECURITY O365 AUDITING AND EDISCOVERY STANDARD OPERATING PROCEDURE

I. PURPOSE

1. This document further describes the WHO standard operating procedure for dealing with auditing and related security activities in O365 platform (mainly eDiscovery process).

II. SCOPE

2. This procedure applies to all WHO employees, contactors and visitors ("users") using the WHO information assets.

I. DEFINITIONS

O365 – is line of subscription offered by Microsoft that allows to use selected Microsoft cloud-based software as a service (SaaS) business products as well as Microsoft Office suite.

eDiscovery (electronic discovery) - process of identifying and delivering electronic information that can be used as evidence in legal cases. eDiscovery in Office 365 could be used to search for content in Exchange online mailboxes, Office 365 groups, Microsoft Teams, Sharepoint online and OneDrive for business sites, MS Teams sites and conversations and Skype for business conversations.

II. PROCEDURE

General

3. All security capabilities available in O365 are accessed via single Security & Compliance portal https://protection.office.com/
4. Access to Security & compliance portal should be limited to need to know basis only. By default, all O365 Global administrators have access to most of offered Security & compliance functions. Security & Compliance portal allows to define specific access rights for accessing the portal.
5. WHO Global Cybersecurity policy and rules available on eManual needs to be followed when granting access to Security & compliance portal.
6. Description of roles available together with permission is included in Annexes to this Standard operating procedure.

O365 Auditing process

7. All O365 business product provide audit capabilities from single Unified Audit log. Unified audit log is part of Security & Compliance portal.
8. Access to Unified audit log Is available by default to Global administrators of O365 through inherited functions, Security Administrators and Compliance administrators' roles within Security & Compliance portal. Both mentioned roles are normally dedicated to selected members of Cybersecurity unit.

9. If access to Unified Audit log is required by user that is not member of O365 Global Administrators or Cybersecurity unit, business justification and CISO approval is required. CISO may delegate this responsibility to member of Cybersecurity unit.
10. Every user accessing Unified Audit log must adhere to rules on access as defined in WHO Acceptable use policy in case of search performed in Unified audit log includes personal information.
11. Unified audit logs are available online and log retention is 90 days.
12. Extract of logs may be provided to users or other internal WHO party (if they do not have access to Unified Audit log) based on provided business justification and detailed specification on scope. Logs could be provided only on need to know basis (Data contained in logs needs to be limited to as little as possible to accommodate business request).

O365 eDiscovery process

13. eDiscovery capabilities of Security & Compliance portal should be restricted to members of Cybersecurity unit nominated by CISO.
14. eDiscovery process could be started only for 3 defined purposes:
    a) Request from Department of Internal Oversight Services (IOS)
    b) Cybersecurity incident investigation
    c) In special circumstances mailbox/Sharepoint Site/OneDrive site recovery requested by respective owner
15. Requests for eDiscovery other than described above will be evaluated by Cybersecurity team on case by case basis and may be processed if business justification and appropriate approval exists:
    a) Mailbox/Sharepoint Site/OneDrive folder owner approval
    b) If not possible, at minimum approvals from ADG Business operations and HRD are in place
16. Once eDiscovery process is started, Security & Compliance alert is generated, stored within Security & Compliance portal (without the possibility to be deleted) and O365 global administrators are informed. This ensure that eDiscovery is not misused and provides control over actions performed by Cybersecurity unit. All eDiscovery searches must be logged into O365 Unified audit log.
17. During all eDiscovery investigations, the principal of minimal required data needs to be followed. Scope should always be limited only to what is really required.

eDiscovery for IOS requests

18. eDiscovery extract could only be provided to IOS department as a part of official investigation process. To ensure that this is in place, following must apply:
    a) Request needs to include all specifications (timeframe, target person, email address of target person)
    b) Request needs to be approved by Director IOS
    c) Request needs to be approved by CIO
19. Fully approved request is assigned to member of Cybersecurity unit for processing.

20. Cybersecurity unit provides exported pst files or zip archive to IOS investigator. Separate guidelines should be issues to describe the process required to export pst file by Cybersecurity unit.

eDiscovery during Cybersecurity incident investigation

21. Usage of eDiscovery process during Cybersecurity investigations needs to be limited and must be only performed if all other options are exhausted and if it is identified that running eDiscovery would help in incident response.
22. WHO Cybersecurity Incident Management SOP must be adhered to during incident investigation.
23. If it is identified that eDiscovery process is required, Incident number referring to the ongoing Cybersecurity incident must be provided as part of the eDiscovery search.

eDiscovery for mailbox recovery

24. In exceptional circumstances eDiscovery process may be used to recover lost/deleted/corrupted mailbox/SharePoint site/OneDrive site. The initial request needs to be made by the respective owner and the owner needs to formally accept all steps that will be required in the process, mainly the fact that data to be recovered could be accessed by member of Cybersecurity or IMT team during the process.
25. Recovery requests must be evaluated on case by case basis and the decision would be made within IMT department. IMT department (mainly Cybersecurity and ESS units) will evaluate the request together with associated risks and benefits.
26. Cybersecurity unit will provide the exported pst file or zip archive directly to the owner.
27. Where, in the course of incident handling and investigation, access to personal information is necessary, rules on access defined in the WHO Acceptable Use Policy must be adhered.

III. COMPLIANCE

28. All those persons referred to within the scope of this procedure are required to adhere to its terms and conditions.
29. All alleged violations of this procedure should be reported to the Global or Regional Service Desk and the appropriate authority responsible for administering this procedure in the WHO location involved (primarily members of the Cybersecurity team, Regional ICT Managers, WHO Representatives in the COs), who will investigate the allegations and if appropriate refer the matter to the relevant WHO authorities.
30. Individual WHO supervisors are responsible for ensuring that this procedure is applied within their own teams. This also extends to any contractors, consultants or visitors who are working within them. Any queries on the application or interpretation of this procedure must be discussed with the IT Department prior to any action being taken.