CYBERSECURITY INCIDENT MANAGEMENT STANDARD OPERATING PROCEDURE

I. PURPOSE

1. This document further describes the WHO standard operating procedure for dealing with Cybersecurity incidents as defined in WHO Cybersecurity Incident Management rules.

Security incidents include, but are not limited to: virus, worm, and Trojan horse detection, unauthorized use of computer accounts and computer systems, as well as complaints of improper use of WHO information assets as outlined in the WHO Global Cybersecurity Policy.

II. SCOPE

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

I. DEFINITIONS

Event – An "event" is an observed or observable occurrence in a system, a network, application or daily operations. Events are not necessarily adverse. When first observed, an event could appear to be an incident but after analysis, turn out to be an explainable anomaly in the environment.

Incident – An "incident" is an adverse event where a WHO asset (examples include, but are not limited to: personnel, information, hardware, software) is attacked or threatened with attack, accessed without authorization, used in a manner inconsistent with established WHO policies and which results in the real or possible loss of confidentiality, integrity, availability or potential damage to the WHO asset.

Examples of Cybersecurity incidents are given in the Appendix of this procedure.

II. PROCEDURE

General

3. Cybersecurity incidents in WHO must be reported through the correct channels. In the first instance, all suspected incidents must be reported through the WHO Global Service Desk (GSD).

4. Cybersecurity team is established to review and deal with Cybersecurity events. In case Cybersecurity Incident is identified, a Cybersecurity Incident Response Team (CSIRT) will be established by CISO. This task could be further delegated to WHO Incident manager.

5. CSIRT have optional members from other units (IMT, IOS, health technical units, regional or country offices) based on incident type and priority. CISO

6. The CSIRT has five primary responsibilities:

a. to respond to high impact incidents when they occur;

b. use technical measures required to contain incident and affected asset and to ensure that there are no threats to other WHO assets;
c. to perform Root Cause analysis (RCA) of the incident
(d) to take steps after an incident to improve the WHO's incident prevention, detection, and response capabilities;
(e) to ensure contingency plans are followed and updated where necessary;
(f) to analyse the Post Incident Review (PIR) report and lessons learned.

Reporting Cybersecurity Incidents

7. All suspected Cybersecurity events must be reported promptly.

8. The WHO IMT service is responsible for providing training on reporting information security incidents to users as part of the Cybersecurity awareness training.

Initial Assessment

9. Assessment must be done, following the WHO Cybersecurity Incident Handling Procedure, to determine whether a reported event is an incident, the extent to which information and/or information resources have been compromised and an approximate scope of the event at hand.

10. Operational procedures and guidelines for dealing with Cybersecurity incidents may be issued separately by WHO/HQ and each WHO Regional Office. All procedures and guidelines must comply with approved Cybersecurity Incident Management Procedure and should be used only to clarify locally specific processes.

11. Should the incident have a high impact on the WHO day-to-day business, if necessary, it will be dealt with according to the relevant area Business Continuity Plan. In case incident extends to multiple WHO offices or if there is a suspicion that incident may extend to multiple offices, Cybersecurity team should be always aware of the incident.

Containing and Resolving Incidents

12. Risk assessment and relevant actions must be carried out to contain the incident, return to normal operations and mitigate against new occurrences of that type of incident.

13. During incident containment and incident resolution all steps must be documented. Documentation should include following at minimal: status of incident, actions with timestamps, chain of custody, contact information of involved parties.

14. Where a follow-up action against a person or organization after a Cybersecurity incident involves legal action (either civil or criminal), evidence must be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

15. To support incident containment and resolution, Cybersecurity team has mandate to use technical and procedural measures required. This could be but are not limited to: take ownership of hardware, perform analysis of hardware or software, provided access to asset (server, application). Cybersecurity team member is required, when possible and feasible, to notify affected user about measures taken.

16. 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.

Lessons Learned

17. To learn from incidents and improve the response process, incidents must be recorded, and a Post Incident Review conducted. The following details must be collected and reviewed:

1.
1. (a) Type and impact of the incident
2. (b) Volumes of the incident and malfunctions
3. (c) Costs incurred during the incident
4. (d) Root cause analysis
5. (e) Details of incident resolution
6. (f) Proposed actions to prevent future incidents

18. The information must be collated and reviewed by the IT units and patterns and trends identified. Any changes required as a result of the Post Incident Review must be formally noted.

III. COMPLIANCE

19. All those persons referred to within the scope of this procedure are required to adhere to its terms and conditions.

20. 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.

21. 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.

IV. APPENDIX I – EXAMPLES OF INFORMATION SECURITY INCIDENTS (NON-EXHAUSTIVE LIST)

Confidentiality
Unauthorized access to systems or applications by WHO staff
Unauthorized access to systems or applications by external entities
Unauthorized access to systems or applications internal through circumvention of access privileges
Loss or theft of computer equipment
User ID and/or password compromise
Disclosure, loss or theft of WHO Confidential information
Leak of sensitive information
Sharing credentials (e.g. password)
Password compromise – password left visible to unauthorized parties
Impersonation – staff logging in as someone other than themselves
User accesses system or device using another's User Id and password
Unauthorised Software use

Masquerading identity
Confidential communication Interception
Integrity
System malfunctions leading to security risks
Virus infections
Hacking – unauthorized modification of systems or applications
Fraudulent activities – unauthorized manipulation of data
Absence of, or poor change control
Misuse or abuse of information systems
Scam mails
Massive virus spread on the WHO network (worm)
Hoax Warnings in circulation
Availability
Hardware/software/communications failure
Failure of environmental controls (air conditioning) potentially leading to services loss
Loss of backup media
Equipment theft
Disruption of services, equipment or facilities
Degradation of service – inadequate response time
Loss or theft of PC/laptop
Inability to execute backup processes
Loss or theft of information
Accidental Damage to computer equipment
Governance
User found sending inappropriate emails
User found sending chain emails
User found with inappropriate documents, pictures
User found with unauthorized and or malicious software loaded on their WHO provided PC
User taking advantage of security vulnerabilities
Inappropriate and repeated Internet usage by WHO /Third Party staff
Breach of WHO security policies and procedures
User found to make unauthorized access or manipulations to computer systems, networks and data
Security controls circumvented or switched off
Reputation
Incident causes adverse publicity for WHO