Email Security

1. All use of email must be consistent with WHO policies and procedures of ethical conduct, safety, compliance with applicable WHO rules and regulations.

2. WHO email account should be used primarily for WHO work related purposes; personal communication is permitted on a limited basis, but non-WHO related commercial uses are prohibited.

3. Deleted Email shall be retrievable for up to two years.

4. The WHO email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about health, race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any WHO employee should report the matter to their supervisor immediately.

5. Users are prohibited from automatically forwarding WHO email to a third-party email system (noted in item 6 below). Individual messages which are forwarded by the user must not contain WHO confidential or above information (noted in item 4 above).

    a. Forwarding of email to systems which require it (for example ticketing systems) is permitted pursuant to CISO approval

6. Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and Microsoft Hotmail etc. to conduct WHO business, to create or memorialize any binding transactions, or to store or retain email on behalf of WHO. Such communications and transactions should be conducted through proper channels using WHO-approved documentation.

7. Using a reasonable amount of WHO resources for personal emails is acceptable, but non-work-related email shall be saved in a separate folder from work related email.

8. WHO users shall have the expectation of privacy in anything they store on the WHO email system. Internal Oversight Services (IOS) is the only WHO entity capable and allowed to access a WHO user email mailbox during an official investigation.

9. WHO IT shall monitor the Email system to prevent, prepare, and react to cyber-attacks.

10. WHO user messages shall not be accessed by the WHO IT department.