Policy Title	Information Security Policy
Document identifier	PPM/INFO-SEC/2024/2
Previous title (if any)	N/A
Policy objective	Information is important and is of significant value to the mission of UNFPA. Information stored, processed, collected, and disseminated by UNFPA is referred to as data within this standard. Data needs to be protected from threats that could potentially disrupt the mission of the Organization or affect its reputation. This policy has been written to provide a mechanism to establish a framework to protect against security threats and minimize the impact of security incidents. The Information Security policy is supported by topic-specific policies/standards at a lower level, which address the need of certain target groups within UNFPA. Related information security documents such as standards and procedures govern in conjunction with this Policy.
Target audience	This policy applies to: ● all UNFPA personnel, incorporating staff, contractors, consultants as well as outsourced providers having access to UNFPA data. ● all data owned by and/or managed by UNFPA. ● all UNFPA locations.
Risk control matrix	The risk control matrix is referenced within section VI of this policy.
Checklist	N/A
Effective date	08 January 2024
Revision History	Revision 1: 08 January 2024 Originally issued: 05 January 2023
Mandatory review date	05 January 2026
Policy owner unit	Information Technology Solutions Office (ITSO)
Approval	Link to signed approval template

INFORMATION SECURITY POLICY

TABLE OF CONTENTS

I. Purpose

1. The purpose for this policy is to establish Information security guidelines to protect UNFPA's data from all threats, whether internal or external, deliberate or accidental.

2. This policy seeks to ensure the maintenance of:
    a. Confidentiality, information is accessible only to authorized users.
    b. Integrity, safeguarding of accuracy and completeness of information and processing methods, preventing unauthorized modification or loss of information.
    c. Availability, ensuring authorized users have access to information/assets.

II. Policy

3. All UNFPA personnel must respect the legitimate interests of the UNFPA. Ethical and acceptable use of information and associated systems and networks must be respected and strictly maintained by all users according to (where appropriate) the principles set out in the Standards of Conduct for The International Civil Service.

4. UNFPA encourages the use of its technical resources; however, they remain the organizational property; are provided to conduct official duties, and are offered on a privileged basis only.

5. All UNFPA personnel accessing UNFPA's information and communications systems shall:
    a. ensure that they use it in accordance with the Information Systems Acceptable Use Policy.
    b. protect the confidentiality, integrity and availability of those assets.
    c. ensure the correct and secure operation of systems supporting the daily operations of UNFPA.
    d. not use the systems in a manner that damages UNFPA's reputation or brand.

6. All UNFPA personnel shall complete annual information security awareness training to maintain awareness of the information security policy and their individual roles and responsibilities in the context of information security.

7. The Enterprise Risk Management Secretariat in consultation with the Legal Unit and Information Technology Solutions Office (ITSO) shall ensure applicable legislative and regulatory requirements related to information security are complied with.

8. All UNFPA personnel involved with system acquisition or system development must embed security as an integral component of the lifecycle (procurement, design, development, commissioning, implementation, maintenance and decommissioning) of information systems.

9. The supply chain management unit must ensure information security requirements are incorporated into all third-party contracts, to ensure UNFPA's information is protected against unauthorized access, data loss and outage.

10. The Information Technology Solutions Office (ITSO) must implement and maintain an information security incident management process to respond to cyber-attacks. Security incidents must be managed in a manner that allows timely and accurate identification of, containment of, and remediation of security incidents.

11. ITSO may monitor technology resources to detect, respond and remediate cyber threats.

12. Furthermore, and consistent with generally accepted business practices, ITSO may collect statistical data about its technology resources and monitor their use to ensure the ongoing availability and reliability of systems.

13. Before procurement, development of any new capabilities, or making any significant change to an ICT system, the ICT system owner must ensure that a risk assessment is conducted under the guidance of an ITSO Information Security representative. The

assessment must focus on identifying risks associated with the reputation of UNFPA and the confidentiality, integrity and availability of UNFPA's data.

14. All users shall ensure that UNFPA information is not stored or processed by third-party digital service providers (including cloud services) unless:
    a. there exists an official agreement or contract between UNFPA and the third-party service provider (e.g. Google Drive), and
    b. a security risk assessment on the third party digital service has been performed by ITSO.

15. The UNFPA Enterprise Risk Management Policy (and related procedures) must be followed for mitigating information security risks. The risks identified must be captured in a formal risk register.

16. Owners of business-critical services shall ensure that business continuity and disaster recovery plans are developed, maintained and tested to maintain service continuity during high-impact incidents.

17. It is the responsibility of all individuals to report information security incidents to infosec@unfpa.org.

18. If it is determined that a security incident arose, in whole or in part, due to user noncompliance with applicable regulations, rules, policies or procedures, this may result in forfeiture of the privilege to use technology resources as well as administrative, disciplinary or other legal action as applicable.

III. Procedures

a. Governance

19. ITSO shall develop information security standards, procedures, and business processes in line with the ISO: IEC 27000 series of standards to support compliance with this policy. These standards shall include:
    a. Information Systems Acceptable Use Policy
    b. Information Security Identity Access Management Policy
    c. Information Security Awareness Guideline
    d. Information Security Threat and Vulnerability Policy
    e. Network and Cloud Security Policy
    f. Information Security Incident Response Plan

b. Information Security Management Group

20. Information Security Management Group (ISMG) is responsible for information security governance and monitoring the effectiveness of the information security program and ensures the information security program supports the UNFPA's mission.

21. The ISMG comprises managers from UNFPA's ITSO divisions and other ICT specialists as appropriate. It is chaired by the Director of ITSO.

22. The roles and responsibilities of the ISMG include:
    a. Ensuring that security aligns with UNFPA's strategic plans.
    b. Review progress on UNFPA's cyber security roadmap.
    c. Identifying significant new threats or significant changes to the environment (technical, legal, contractual, social, etc.).
    d. Providing regular updates on identified information security risks and suggested risk treatment plans.
    e. Reviewing all relevant policies and procedures that comprise the Information Security Management System (ISMS), monitoring compliance with the ISMS, reviewing incidents, and recommending actions where necessary to strengthen information security controls.
    f. Monitoring and reviewing information security activities within UNFPA.
    g. Assessing the performance of implemented security measures and determining whether they meet expectations.
    h. Making recommendations or decisions on the selection of adequate and proportionate security controls that protect UNFPA data.
    i. Reviewing results of security audits and tests performed by or on behalf of UNFPA as input for making recommendations or decisions to continually improve UNFPA's security.

c. Roles and responsibilities

23. The Director, Information Technology and Solutions Office (ITSO) is charged with responsibility for information security leadership and coordination (including delivery of information security awareness training) throughout the UNFPA.

24. All UNFPA personnel are explicitly responsible for the security of the data they have been granted access to and are accountable for security to the extent of their individual work responsibilities in UNFPA.

25. UNFPA managers' responsibility is to ensure that staff, contractors, consultants, interns, visitors, and any other individuals that are accessing data, or planning / developing / deploying new or existing ICT systems for UNFPA are informed and agree to comply with relevant UNFPA information security policies.

26. Additional information security roles and responsibilities that are aligned with enterprise risk management are detailed within the Enterprise Risk Management policies and procedures manual (available here).

IV. Other (as needed)

No other content available.

V. Process Overview Flowchart(s)

No overview flowchart applicable.

VI. Risk Control Matrix

The risk control matrix can be found here.