Policy Title	Policy and Procedures for Network and Cloud Security
Document Identifier	PPM/NET-CLOUD-SEC/2024
Previous title (if any)	N/A
Policy objective	This policy has been written to define principles for protecting UNFPA-managed networks and the confidentiality, integrity and availability of information when stored, processed or transmitted by a third-party cloud computing service provider.
Target audience	This policy applies to: • all UNFPA personnel, incorporating staff, and non-staff personnel, including but not limited to service contractors, individual consultants, interns, and outsourced providers responsible for managing UNFPA information systems, applications and data. • all UNFPA locations.
Risk control matrix	N/A
Checklist	N/A
Effective date	4 October 2024
Revision History	N/A
Mandatory review date	4 April 2026
Policy owner unit	Information Technology Solutions Office (ITSO)
Approval	Link to signed approval document

POLICY FOR NETWORK AND CLOUD SECURITY

TABLE OF CONTENTS

I. Purpose

This policy aims to ensure effective protection of UNFPA-managed information and communications technology (ICT) assets by defining principles for the design and management of networks and for cloud security.

With the embracing of cloud technologies and the adoption of teleworking, the traditional concept of an internal perimeter is fading. The networking stack is also being virtualized[1]; thus, the threat landscape has expanded beyond the traditional networks and now includes UNFPA ICT assets hosted in corporate cloud platforms. To reduce the overall risk to UNFPA on premises and in cloud environments, this policy includes both a) cloud security principles and requirements for cloud services providers (CSP) and b) network security principles for ICT assets hosted on premises within UNFPA.

II. Policy

Information and Technology Solutions Office (ITSO) is responsible for overall network design in the organisation. Therefore, all network designs must be cleared by ITSO before implementation.

The following principles should be taken into account:

1. UNFPA information technology officers must accomplish resilient network architecture that protects UNFPA against unauthorised access and malicious activities. This includes the adoption of best practices in network design, management and controls.
2. ITSO must establish and maintain a clear security responsibility model in order to achieve security control objectives set by UNFPA, according to what is stated in the Information Security Policy[2].

This policy must be read in conjunction with related policies stated in section III, D.

III. Procedures

A. Network security

1. The network security is further defined under the following headings:

2. The following paragraphs provide further detailed procedures under each of these headings.

[1] The traditional network functions and components are being managed through software instead of physical hardware.
[2] Paragraph b. Information Security Management Group.

Network design

3. Where possible UNFPA will use a standard centrally managed firewall solution as determined by ITSO.
4. Whenever deemed necessary by a risk assessment performed by ITSO, data transmitted will be encrypted using industry-standard encryption protocols.
5. Networks must be segregated (segmented) as appropriate, to protect critical business functions and to prevent issues in non-production environments affecting production services as outlined below:
   - The configuration will be performed by ITSO for systems managed by ITSO.
   - For UNFPA systems not managed by ITSO, the UNFPA field office ICT focal point or equivalent must ensure this requirement is met.
6. Access to the internal network segments managed by ITSO from remote connections must be made only via ITSO-approved connection points. Within networks, Virtual Private Cloud will be used to segregate organizational units.
7. The security policy[3] of each office firewall must be designed to:
   - not allow any traffic from the internet apart from trusted/needed sources/ports (e.g. centralized management, Voice over Internet Protocol (VoIP) services, locally hosted web-services etc.).
   - discard traffic from unknown sources.
8. For all the UNFPA systems that support such capabilities, Zero Trust security model[4] must be adopted by ITSO and all the UNFPA field office ICT focal points for managing access as follows:
   a. Micro segmentation or host-based segmentation should be adopted.
   b. Next-generation firewalls should be used to protect and filter traffic.
   c. Access should be secure regardless of their location, device or network (internal or external) as network is assumed to be always hostile.
9. When Zero Trust security model cannot be adopted, UNFPA managed networks must be designed, implemented and operated by ITSO or where applicable by the UNFPA field office ICT focal point with proper segregation at logical and physical level including zone-based approach, based on the sensitivity of the information being communicated and on risk, with all traffic flow between different zones evaluated through an appropriate enforcement point (e.g., Firewall, IDS/IPS, Proxy, WAF, etc).

[3] A firewall security policy is the set of instructions prepared by ITSO or where applicable by the UNFPA field office ICT focal point that tells the firewall how to manage the flow of data across a network.
[4] Zero trust is a security model designed to enforce accurate, least privilege per-request access decisions in information systems and services - in a network seen as compromised.

Approved connection

10. Access to information hosted on the UNFPA network must be established using only ITSO-approved connection points and methods. The number of connection points and methods to and from UNFPA networks must be kept to a minimum. ITSO must immediately disable and remove, in a timely manner, all connection points and methods no longer required. This covers all points of connection to the UNFPA network. This includes (but is not restricted to): LAN, WAN, remote, internet.
11. Personnel may not connect personal devices[5] to the UNFPA corporate network. All personal devices must be connected via the guest network.

Non-essential services and ports

12. All non-essential services and ports on the UNFPA network must be disabled by ITSO or by UNFPA field office ICT focal point when networks are not centrally managed.

Wireless networks

13. A guest wireless network may be provided for visitors. This must be virtually or physically separated (via physical access points) from all internal networks (including internal wireless networks) and secured using firewalls.
14. Wireless access point admin logon password must always be changed from the default by ITSO or by UNFPA field office ICT focal point when UNFPA networks are not centrally managed.

Logging and monitoring

15. Security incidents and/ or events on the UNFPA network must be logged, securely maintained, and monitored on a regular basis by ITSO for systems managed by ITSO. Cloud services critical logs must be replicated by ITSO to the enterprise central logging solution in a tamper-proof mode for analysis and monitoring when supported.

Security incidents and reporting

16. It is the responsibility of all individuals to report information security incidents to infosec@unfpa.org.
17. Network incidents and/ or events that are deemed to be security incidents must be recorded and managed according to the Information Security Incident Response Plan.

[5] The corporate network cannot be accessed through a personal device.

Network management

18. Management of all aspects of the network must be carried out only by authorized specialists or individuals who fully understand security threats and the application of mitigating protective controls.

B. Data encryption

19. Data encryption statements are further defined under the following headings:

Network design

20. When networks are designed, data encryption has to be configured for all data in transit, both within Virtual Private Cloud (VPC) network and peered VPC network, between cloud network and local network and within local network. Encryption level and techniques have to be adjusted accordingly as deemed appropriate by ITSO.

Remote access

21. Where there is a requirement of remote access to the UNFPA network a Virtual Private Network (VPN) will be made available by ITSO providing session encryption using Transport Layer Security (TLS) version not deprecated.

Wireless networks

22. UNFPA's wireless networks must be secured by ITSO and, when applicable, by field office ICT officers at minimum using Wireless Protected Access 2 (WPA2) encryption. Periodically the minimum standard for wireless networks must be reviewed by ITSO or, when applicable, by UNFPA field office ICT focal point to ensure data is protected against up-to-date threats.

C. Cloud security responsibility model

23. Roles and responsibilities for the shared security responsibility model should be clearly defined when consuming or providing cloud services.

24. When undertaking procurement for cloud services, respective UNFPA personnel[6] are responsible for ensuring that contracts and service level agreements must regulate the following aspects for both regular operations and during service disruptions:

- Relevant and proportional information security objectives and measures, encompassing minimum cybersecurity requirements as described in the pertinent information security policies and guidelines:

[6] If needed, personnel can ask ITSO for support in meeting these requirements.

- Specifications for the data life cycle.
- All requirements related to data encryption.
- Network security and processes for security monitoring.
- Data center locations.
- Procedures for operational and security incident handling, including escalation and reporting.

D. Related documents

25. The following related documents should be referenced for additional context.

#	Document	Location
1	UNFPA Information Security Policy	UNFPA website
2	UNFPA Policy and Procedures on Personal Data Protection	UNFPA website
3	Information Disclosure Policy	UNFPA website
4	UNFPA Oversight Policy	UNFPA website
5	UNFPA Policy against Fraudulent and other Proscribed Practices	UNFPA website
6	Disciplinary Framework	UNFPA website
7	UNFPA Internal Control Framework (ICF)	UNFPA website
8	Enterprise Risk Management	UNFPA website

E. Monitoring and inspections

26. UNFPA has a strong commitment to information security. In line with the overall Information Security Policy, any violation of the provisions of this policy, shall be reported to the information security team.

27. Routine technical monitoring[7] of the use of UNFPA ICT resources may be conducted by ITSO or a UNFPA field office ICT focal point designated by ITSO.

28. Non-routine monitoring ("inspections") may be initiated by ITSO if, at any time, there is reason to believe there has been or risk there will be use of ICT resources which significantly interferes with or impacts the operations of UNFPA. Any allegations of wrongdoing are immediately reported to the Office of Audit and Investigation Services (OAIS).

29. An annual report on the monitoring activities performed and any findings is sent to the Information and Communication Technology (ICT) Board.

[7] Regular technical monitoring of the utilisation of ICT resources involves periodical observation and assessment to ensure efficient and secure operation.

IV. Other

A. Definitions

30. The following definitions shall apply for the purposes of the present policy:

Term	Definition
Authorized user	Any UNFPA personnel who is authorized to use information and communication technology (ICT) resources
ICT resource	Any tangible or intangible asset capable of generating, transmitting, receiving, processing, or representing data in electronic form, where the asset is owned, licensed, operated, managed, or made available by, or otherwise used by, the United Nations, Examples include but are not limited to user workstations, servers, software, cloud systems, databases, networks, communication systems, telephones and conferencing systems.
ICT data	Any data or information, regardless of its form or medium, which is or has been electronically generated by, transmitted via, received by, processed by, or represented in an ICT resource. Examples include but are not limited to text, numbers, files, documents, emails, photos, and web content.
Official use	Use of ICT resources by an authorized user in the discharge of his or her official functions and within the scope of his or her authorization.
Personal use	Use of ICT resources by an authorized user for other than official purposes and within the scope of his or her authorization.
Sensitive data	Data where the unauthorized disclosure would adversely impact UNFPA operations or its reputation. It includes data whose use or distribution is otherwise restricted pursuant to UNFPA Oversight Policy.
VPC	A virtual private cloud (VPC) is a secure, isolated private cloud hosted within a public cloud.
Non-essential services and ports	Services or ports not required by any business application to operate.
Information security objectives	Specific goals set by the UNFPA to comply with requirements and policies related to information security and reduce information risks.

Term	Definition
Inspection	The examination/ analysis of anomalies (or security incidents) to determine both root causes and specific impact, aiming to implement actions that maintain information security.
UNFPA field office ICT focal point	Any office that owns or operates an ICT environment must appoint a "UNFPA field office ICT focal point". This is the UNFPA personnel responsible for managing and maintaining the ICT environment in the field office. ICT environment includes endpoints, servers, office networks and other locally procured ICT and cloud computing services.

V. Process Overview Flowchart(s)

No overview flow chart applicable.

VI. Risk Control Matrix

Risk Description	First Line of Defense Controls			Second Line of Defense Controls		
	Control Activity Description	Reference (Policy section, paragraph or Control #)	Who performs	Control Activity Description	Reference (Policy section, paragraph or Control #)	Who performs
UNFPA staff members build computer networks that are inherently insecure	Policy details the security procedures and requirements for building secure networks	Section III, A	ITSO and selected staff	Monitoring compliance to this policy through reporting on Threats targeting insecure networks	Section III, E	ITSO, Information Security Team, Information and Communication Technology (ICT) Board

Risk Description	First Line of Defense Controls			Second Line of Defense Controls		
	Control Activity Description	Reference (Policy section, paragraph or Control #)	Who performs	Control Activity Description	Reference (Policy section, paragraph or Control #)	Who performs
UNFPA staff member subscribe to cloud services that are insecure and expose UNFPA sensitive information to cyber threats	Policy details security requirements and procedures to procure and manage third party cloud services	Section III, D	All UNFPA personnel	Monitoring compliance to this policy through reporting on the use of ICT resources	Section III, E	ITSO, Information Security Team, Information and Communication Technology (ICT) Board