Policy Title	Policy for Third-party Information and Communication Technology (ICT) Risk Management
Document Identifier	PPM/THIRD-PARTY-ICT-RISK/2024
Previous title (if any)	N/A
Policy objective	This policy has been written to define principles for protecting the confidentiality, integrity and availability of information when stored, processed or accessed by third parties providing services to UNFPA.
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 THIRD-PARTY ICT RISK MANAGEMENT

TABLE OF CONTENTS

I. Purpose

1. The purpose of this document is to define the principles for third-party information and communications technology (ICT) risk management within UNFPA in line with the principles set out in the Information Security Policy of UNFPA.
2. All contracts must include appropriate clauses to ensure that third parties will abide by the principles set out in this policy are listed below:
    a. Service providers that collect, store, process, and/or transmit UNFPA digital data or manage systems or components such as routers, firewalls, databases, physical security and/or servers.
    b. Vendors that provide digital solutions and/or physical products that are used to collect, store, process and/or transmit UNFPA digital data (e.g. servers, computers, tablets, switches, routers, firewalls etc).
    c. Third parties (cloud, application developers or hosting facilities) that use and/or have access to UNFPA managed information assets.
3. Special relationships with other United Nations agencies are not included in the scope of this policy, as per strategic partnerships within the United Nations family with Memorandum of Understanding (MoU) and other specific agreements.
4. Entry into force: This policy first entered into force on 4 October 2024. All new third-party contracts established after the date of enforcement are required to comply with this policy. Existing contracts will remain in effect without complying with the policy until their next renewal.
5. This policy must be read in conjunction with the UNFPA policies and guidelines listed in the "Related documents" paragraph.

II. Policy

A. Third party classification

6. Following a risk-based approach to information security, users who need to to engage a third party providing digital services should classify the third party as per the following categories. In case there is ambiguity in performing this classification users can contact Infosec@unfpa.org to seek clarifications:
    a. **Critical:** third parties supporting UNFPA business critical processes or that stores, processes, and/or transmits UNFPA confidential or strictly c confidential information as defined in the UNFPA Oversight Policy.

b. **Standard:** third parties not supporting UNFPA business critical processes and not storing, processing, and/or transmitting UNFPA confidential or strictly confidential information as defined in the UNFPA Oversight Policy

B. Due diligence

7. Due diligence on cybersecurity practices should be requested by the users and performed by ITSO[1] on third parties prior to their engagement. This due diligence should include at minimum the following assessments:
   a. Third party organisation.
   b. Third party solutions that collect, store, process or transmit UNFPA data.
   c. Third party solutions that connect to or integrate with UNFPA infrastructure or systems.
8. A risk-based approach will be used by ITSO when assessing third parties as mentioned below:
   a. Critical – due diligence and security assurance via compliance review (i.e. ISO 27001 certification, SOC 2 type II audit, etc) must be performed.
   b. Standard – due diligence is required, and security compliance review is optional.
9. When additional security assurance is required, third-party security risk assessments are done following the procedures and flowchart defined within this document.

C. Contract obligations

10. Supply Chain Management Unit (SCMU) is responsible for ensuring information security requirements defined in the procedures section of this document are included in contracts and/or Service Level Agreements (SLAs) with third parties that access, store, transmit or process UNFPA digital data or provide information technology infrastructure components to UNFPA.

D. Service delivery management

11. An office that initiates a contract or Service Level Agreements (SLA) with a third party must regularly monitor and review service delivery to ensure compliance with the agreed security conditions.
12. Service delivery reviews should be conducted regularly and when significant business, legal, regulatory, architectural, policy and contractual changes occur.

[1] ITSO can perform due diligences based on the priorities and available resources.

E. Shared responsibility model

13. Roles and responsibilities for the shared security responsibility model should be clearly defined by SCMU, with ITSO support, between UNFPA and the third party.
14. UNFPA does not allow any third party to perform security monitoring in the UNFPA ICT environment unless this is explicitly agreed with ITSO.
15. Specific shared responsibility model for cloud services is documented in the Policy and Procedures for Network and Cloud Security.

F. Related documents

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

#	Document	Location
1.	UNFPA Policy and Procedures on Personal Data Protection	UNFPA website
2.	Information Disclosure Policy	UNFPA website
3.	UNFPA Oversight Policy	UNFPA website
4.	UNFPA Policy against Fraudulent and other Proscribed Practices	UNFPA website
5.	Disciplinary Framework	UNFPA website
6.	UNFPA Information Security Policy	UNFPA website
7.	UNFPA Policy for Network and Cloud Security	UNFPA website
8	UNFPA Enterprise Risk Management Policy	UNFPA website
9	UNFPA Guidance on the Safe and Ethical Use of Technology to Address Gender-based Violence and Harmful Practices	UNFPA website

G. Monitoring and inspections

17. ITSO shall monitor compliance to the SLAs by performing regular reviews as prescribed below:
    - Annual reviews for critical third parties.
    - At the contract renewal for standard third parties upon request by the business unit.
18. UNFPA has a zero-tolerance principle for wrongdoing (including prescribed practices). Any violation of the provisions of this policy, shall be reported to OAIS in accordance with UNFPA Policy against Fraudulent and other Proscribed Practices, or other relevant policy that is specific to the wrongdoing.
19. Routine technical monitoring of the use of third-party services may be conducted by ITSO or a field office focal point designated by ITSO as per the provisions of this policy.

20. Non-routine monitoring ("inspections") may be initiated by ITSO if, at any time, there is reason to believe that there is a risk that will significantly interfere with or impact the operations of UNFPA.

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

III. Procedures

A. General terms and conditions for third-party services

22. SCMU shall include the following terms and conditions in contracts with third parties providing services to UNFPA.

Table 1: Third-party general terms and conditions

Domain	Requirement
Information Security program	a. Supplier shall maintain an information security management program that includes information security policies, procedures and controls governing confidentiality, integrity and availability of data.
Data ownership	b. The supplier acknowledges UNFPA data remains the property of UNFPA. c. The supplier shall ensure UNFPA has access at all times to UNFPA data whilst in the possession or under the control of the supplier.
Data backup	d. The supplier shall maintain backup copies and disaster recovery capabilities for UNFPA data stored or processed in supplier systems. e. Backups shall be stored securely in compliance with UNFPA information security policies.
Data confidentiality	f. The supplier shall complete non-disclosure agreements prior to accessing UNFPA data. g. The supplier shall not disclose UNFPA data to any third parties without prior consent from UNFPA.
Data access	h. The supplier shall ensure all access (by their personnel) to UNFPA data is subject to formal authorised access provisioning and governance procedures.

Domain	Requirement
	i. The supplier shall revoke access immediately when a member of their team ceases work with the team or is transferred to a different role not related to the engagement.
Data records	j. The supplier must maintain complete and accurate records of all UNFPA data accessed, collected, or changed by it, including details of individual members' who have accessed UNFPA data within the scope of the engagement.
Data retention	k. The supplier shall not retain UNFPA data longer than needed for the purposes of the engagement. l. Upon the conclusion of the supplier's engagement with UNFPA, or upon earlier direction from UNFPA, the supplier must (at its own cost): i. stop using UNFPA data ii. return UNFPA data or iii. at UNFPA's direction, erase or destroy UNFPA data (in accordance with approved destruction methods)
Data encryption	m. The supplier shall encrypt all UNFPA data that is stored or transmitted by systems managed by the supplier or the supplier's third-party partner. n. Any workstation, laptop, mobile device used to access or process UNFPA data must have endpoint encryption installed and enabled.
Security audits	o. UNFPA may conduct or require the supplier (or third party) to conduct a security review or audit on the supplier's facilities, people, processes and technology, associated with the performance of the contract / engagement. p. Where a review or audit is required, the supplier shall provide the auditor or its nominees with access to the supplier's facilities, people, processes and technology.
Incident response	q. The supplier shall ensure security monitoring is performed on all supplier systems used to process, store or transmit UNFPA data. r. The supplier must maintain a security incident response plan.

Domain	Requirement
	s. The supplier shall immediately notify UNFPA by phone and in writing where it becomes aware of (or suspects) a breach of UNFPA data associated with the engagement.
Personnel security	t. The supplier shall conduct reasonable and appropriate background vetting of all personnel in accordance with industry best practices. u. All supplier personnel are to complete mandatory security awareness training prior to accessing UNFPA data or systems.
Operational security requirements	v. The supplier must ensure their handling, processing and storage of UNFPA data is performed from within secure facilities and secure systems. w. The supplier must maintain technical vulnerability management and patching capabilities for all their software, firmware and hardware used to facilitate processing, storage or transmission of UNFPA data. This includes any device, server or system element connecting to UNFPA networks. x. The supplier must establish and maintain ICT change management procedures, incorporating information security risk assessments of any major change to their systems used to facilitate processing, storage or transmission of UNFPA data. y. The supplier shall protect UNFPA data (and systems) against the introduction of any malware or other malicious threat vector. This includes use of industry-recognized malware prevention solutions on all supplier networks and systems used to store, process or transmit UNFPA data.

B. Third-party risk management for software development services

23. In addition to the requirements set out in Table 1 above, contracts entered with suppliers providing software development services to UNFPA shall meet the requirements identified in Table 2 below.

Table 2: Third-party terms and conditions for software development services

Domain	Requirement
Secure coding	a. Supplier shall ensure code is securely developed as per industry (Oper Web Application Security Project[2]) best practices, and includes controls for: i. Authentication ii. Authorisation iii. Session management iv. Data validation v. Data encryption (protection of data at rest, in transit and in use) vi. Application-level logging and auditing vii. Error handling
Security testing	b. Supplier will maintain a formal software development lifecycle that includes static, dynamic and interactive security testing. i. Manual and automated code reviews shall be conducted during the application development lifecycle. ii. Web application vulnerability scanning (and penetration testing) shall be conducted prior to operational acceptance of the developed application. c. Any identified critical or high severity vulnerabilities shall be remediated prior to release of the application into the production environment.

IV. Other

A. Definitions

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

Term	Definition
Third Party/ Vendor/ Supplier	• Service providers that store, process, and/or transmit UNFPA data[3] or manage systems or components such as routers, firewalls, databases, physical security and/or servers.

[2] OWASP Foundation, the Open Source Foundation for Application Security.
[3] UNFPA data: any information that is generated, collected, stored, or used by UNFPA in the course of its operations.

	• Vendors that provide digital solutions and/or physical products that are used to store, process and/or transmit UNFPA data. • Third parties (cloud, application developers or hosting facilities) that use and/or have access to UNFPA managed information assets.
Data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, UNFPA data.
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.

V. Process Overview Flowchart(s)

A user can submit a request to ITSO for a third-party risk assessment via the Global Service Desk.

ITSO will perform the risk assessment following the procedure mentioned below:

A. Collect information

25. The Information Security Team in ITSO will initiate the risk assessment after receiving a go-ahead from the ITSO Director and according to the rules established by the Enterprise Risk Management (ERM) framework.
26. ITSO will request the user through procurement to either:
    a. Share all vendor security related documentations (if any)

    OR

    b. Share the vendor contact details with the Supply Chain Management Unit (SCMU) so that SCMU, in close collaboration with ITSO, can request the security documentation from the vendor.
27. ITSO reviews the vendor supplied documentations with consideration of the following steps:
    c. If the vendor has a SOC 2 Type 2 report, then go to paragraph 28.
    d. If the vendor does not have SOC 2 Type 2 report, then go to paragraph 27.
28. ITSO shares the questionnaire derived from third-party security requirements (see Table 1: Third-party general terms and conditions and Table 2: Third-party terms and conditions for software development services) with the vendor and set a deadline for returning the

completed questionnaire. If the vendor does not respond, ITSO must inform the requestor and SCMU that ITSO is unable to perform the risk assessment.

B. Assess risk

29. ITSO reviews all provided documentations including the followings:
    a. Any publicly reported data breach
    b. Vendor risk rating[4] reports, if available
    c. Cloud Security Alliance (CSA) Star Registry[5] record (for cloud hosted services)

C. Report

30. ITSO drafts a third-party risk assurance report.
31. ITSO shares the report with the business unit or requester of the third-party risk assessment.
32. Head of business unit accepts the residual risk if all risks are not mitigated.

    If available risk response actions will not allow to manage the risks within the established operational risk appetite levels, the head of the business unit will escalate to the appropriate management levels.

D. Monitor compliance

33. Business unit that initiated the contract must monitor[6] service delivery as per "Service Delivery Management" section above and in line with the classification of the third party.
34. The Information and Communication Technology (ICT) Board will evaluate the overall ICT risk related to third-party providers of digital services through the annual report provided by ITSO, which details the activities performed for all business units that requested risk assessments.

VI. Risk Control Matrix

[4] Vendor risk ratings can be acquired through third parties such as *Security scorecard, Bitsight* or similar.
[5] STAR Registry | CSA (cloudsecurityalliance.org).
[6] The staff will be specifically trained.

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 confidential or strictly confidential information exposed /compromised because of insecure practices at third parties.	Policy details the security procedures and requirements for acquiring third-party services that mitigate the risk	Section II B, C and D Section III A, B and C	All UNFPA personnel	Monitoring compliance to SLAs Monitoring compliance to this policy	Section II, G 17 Section II, G, 18, 19, 20 Section III D, 34 and 35	Office that initiated the contract, Information Security Team, Information and Communication Technology (ICT) Board