A. Policy objective:

1. This policy addresses the assessment and management of risks associated with IT business process outsourcing. Outsourcing involves transferring responsibility for carrying out an activity (previously carried on internally) to an outsourcing provider (also known as an outsourcer) for an agreed charge. The outsourcer provides services to the customer based on a mutually agreed service level, normally defined in a formal contract. Many commercial benefits can be ascribed to outsourcing, including: reducing organizational costs; greater focus on core business by outsourcing non-core functions; access to world-class expertise and resources; and greater ability to address evolving business needs.

B. Intended audience:

2. Staff members throughout UNFPA responsible for the determination and selection of IT outsource vendors.

C. Policy statement:

a. Scope:

3. Outsourcers include: hardware and software support and maintenance staff; applications development staff; external IT consultants and vendors; and business process outsourcing firms.

b. Selection:

4. Criteria for selecting an outsourcer shall be defined and documented, taking into account the: company's reputation and history; quality of services provided to other customers; number and competence of staff and managers; financial stability of the company; quality assurance
and security management standards currently followed by the company (e.g. certified compliance with ISO 9000 and ISO/IEC 27001); and further security criteria defined as the result of the risk assessment (next paragraph).

c. Risk Assessment and Assurance:
5. Based on functional unit need, a suitable UNFPA owner for each business function/process outsourced should be identified (this is normally a senior unit manager). The owner shall assess the risks before the function/process is outsourced, using the selection process outlined above and must consider the: nature of logical and physical access to UNFPA information assets and facilities required by the outsourcer to fulfill the contract; sensitivity, volume and value of any information assets involved; commercial risks such as the possibility of the outsourcer's business failing completely, or of them failing to meet agreed service levels.

6. Considering their impact on existing systems and associated risks, proposals of outsourcing contracts greater than US$100,000 must be presented and approved by the ICT Board prior to entering into any commitments/contracts with the vendor. The Board will ensure that the contract is aligned to organizational strategic goals and shall decide if UNFPA will benefit from outsourcing the function, taking into account the information security aspects. If the risks involved are high and the organizational benefits are marginal (e.g. if the controls necessary to manage the risks are too costly), the function shall not be outsourced.

7. Related risk information should be recorded in the UNFPA Strategic Information System under the myRisks/Strategic Risk Assessment section.

8. Outsourcing contracts less than US$100,000 require the approval of the relevant MIS staff member, specifically, the Business Services Section Chief for applications and the Technology Services Section Chief for hardware/infrastructure.

9. Large outsourcing contracts (i.e., those with an estimated annual cost greater than US$200,000) must include a provision for UNFPA to obtain a service provider internal control attestation report prepared by an independent auditor based on recognized standards, such as the International Standard on Assurance Engagements (ISAE) 3402, Assurance Reports on Controls at a Service Organization, or the Statement on Standards for Attestation Engagements (SSAE) 16, Reporting on Controls at a Service Organization, to give UNFPA reasonable assurance on the adequacy of the design and operating effectiveness of the controls in place over the services provided to UNFPA. If the services provided to UNFPA are in turn subcontracted by the service provider, attestation reports should also be obtained for the concerned subcontractors.

d. Confidentiality:
10. A formal contract between UNFPA and the outsourcer shall exist to protect both parties. The contract shall clearly define the types of information exchanged and the purpose for so doing. If the information being exchanged is sensitive, a binding confidentiality agreement shall be
in place between UNFPA and the outsourcer, whether as part of the outsource contract itself or a separate non-disclosure agreement.

11. The contract shall clearly define the parties to the contract, effective date, functions or services being provided (e.g. service levels), liabilities, limitations on use of sub-contractors and other commercial/legal matters normal to any contract.

12. Depending on the results of the risk assessment, various additional controls must be embedded or referenced within the contract to monitor all access to and use of UNFPA facilities, networks, systems etc., and to audit the outsourcer’s compliance with the contract.

13. Following review by Procurement Services and ensuring that UN privileges and immunities are clearly stated, all contracts shall be submitted to UNFPA Legal for final approval.

D. Policy date:

14. This Outsourcing Management Policy (originally approved and issued on 18 July 2012 with subsequent revisions as shown in the beginning of this document) will remain in force without time limit, and will be reviewed annually to ensure relevance.

E. Policy owner:

15. The MIS Chief is responsible for the Outsourcing Management Policy.

F. Change authority:

16. The MIS Chief has the authority to change the policy. The MIS Chief, Technology Services Section Chief, and Business Support Services Section Chief can give exception waivers.