SHADOW IT POLICY

A. Policy objective:

1. Shadow IT is a growing concern that needs addressing to ensure the integrity and efficiency of enterprise technology, and to prevent fragmentation of information and processes. Shadow IT is defined as IT systems and solutions outside the ownership or control of MIS (e.g. Country Office development of a financial monitoring system). The issue is shadow IT remains largely unmanaged and unacknowledged. Shadow IT isn't necessarily detrimental to the organization. However, it can create risks of data loss, corruption or misuse, inefficient and disconnected processes, and fragmented information which must be addressed appropriately.

B. Intended audience:

2. UNFPA users responsible for the creation and propagation of hardware and software which are not addressed or covered by current MIS policies.

C. Policy statement:

a. Ownership:

3. UNFPA owns its shadow IT systems and the information and resources remain the property of the organization.

b. Monitoring:

4. MIS is responsible for assessing and monitoring shadow IT systems to determine associated risks, support services, stability, effectiveness, and impact on internal system performance.

c. Accountability:

5. Irrespective of where they are charged, considering their impact on existing systems and associated risks, proposals of large shadow IT systems (greater than US$10,000 or 80 person-hours of development) must be presented and approved by the ICT Board. The Board will ensure that the shadow IT system is aligned to organizational strategic goals and must also be informed of any major changes to such systems as these may affect other IT areas as well.

6. Smaller shadow IT systems (less than US$10,000 or 80 person-hours of development) require the approval of the relevant MIS Branch staff member, specifically, the Business Services Section Chief for applications and the Technology Services Section Chief for hardware/infrastructure.

d. Security:

7. One of the most significant areas of concern with Shadow IT relates to security. The potential of external, reputational damage to the organization from failure or malfunction is greater with shadow IT systems. Providing MIS with details regarding the security and appropriateness of information in such systems is essential.

D. Policy date:

8. This Shadow IT Policy dated 18 July 2012, will remain in force without time limit, and will be reviewed annually to ensure relevance.

E. Policy owner:

9. The MIS Chief is responsible for the organizational Shadow IT policy.

F. Change authority:

1. The MIS Chief has the authority to change the shadow IT policy. The MIS Chief, Technology Services Section Chief, and Business Services Section Chief can give exception waivers. Exception waivers should be logged and reported to the ICT Board on a quarterly basis.