

United Nations  Nations Unies

INTEROFFICE MEMORANDUM

MEMORANDUM INTERIEUR

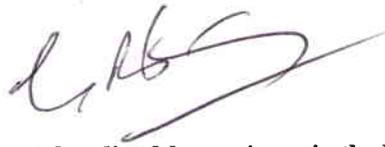
OFFICE OF INTERNAL OVERSIGHT SERVICES - BUREAU DES SERVICES DE CONTRÔLE INTERNE
INTERNAL AUDIT DIVISION - DIVISION DE L'AUDIT INTERNE

TO: Mr. Ashraf Jehangir Qazi,
A: Special Representative of the Secretary General
United Nations Mission in Sudan

DATE: 24 December 2009

REFERENCE: IAD: 09- **03263**

FROM: Fatoumata Ndiaye, Acting Director
TO: Internal Audit Division, OIOS



SUBJECT: **Assignment No. AT2008/510/01 – Horizontal audit of data privacy in the United Nations Secretariat**
OBJET:

The United Nations Mission in Sudan should implement adequate controls for the security of sensitive data, document Mission specific policies and procedures, and issue a protocol to regulate the exchange of data with other entities.

1. I am pleased to present the report on the above-mentioned audit which was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.
2. While cross-cutting issues related to data privacy in the UN Secretariat have been documented in a separate report, this memorandum addresses issues specific to the United Nations Mission in Sudan.
3. In order for us to close the recommendations, we request that you provide us with the additional information as discussed in the text of the report and also summarized in Annex 1.
4. Please note that OIOS will report on the progress made to implement its recommendations, particularly those designated as high risk (i.e., recommendations 1 and 4), in its annual report to the General Assembly and semi-annual report to the Secretary-General.

EXECUTIVE SUMMARY

Horizontal audit of data privacy in the United Nations Secretariat

OIOS conducted an audit of data privacy across the United Nations Secretariat. The overall objective of the audit was to determine whether the Secretariat has adequate controls in place to protect the confidentiality and integrity of sensitive information related to employees, representatives of Member States, and other individuals. The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

The cross-cutting issues identified during the course of the audit have been documented in a separate audit report (IAD:09-02378). This report addresses the risks and controls specific to the United Nations Mission in Sudan (UNMIS).

UNMIS performs several activities that require collecting, processing, and storing personal identifiable data. In consideration of the sensitivity of data collected, processed and stored by the various offices within UNMIS, OIOS recommended that the Mission:

- a) Implement Mission-specific policies to define access control rules and “need-to-know” requirements;
- b) Implement training/awareness initiatives for the classification and handling of sensitive data;
- c) Procure adequate storage containers to ensure the safe-keeping of sensitive documents; and
- d) Issue a protocol to regulate the exchange of data with other entities operating in the same programme areas.

I. INTRODUCTION

1. The Office of Internal Oversight Services (OIOS) conducted an audit of data privacy at the United Nations Secretariat. The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.
2. Data privacy refers to the right of individuals to control the collection and use of personal information about themselves. The Black's Law Dictionary defines it as "a private person's right to choose to determine whether, how, and to what extent information about oneself is communicated to others". It has not been formally defined by the United Nations Secretariat.
3. Comments made by the United Nations Mission in Sudan (UNMIS) are shown in *italics*.

II. AUDIT OBJECTIVES

4. The main objectives of the audit were to assess whether:
 - (a) A governance system is in place to manage privacy of data;
 - (b) The Secretariat has defined what data should be considered sensitive, with particular reference to privacy of data, per ST/SGB/2007/6 on Information sensitivity, classification, and handling; and
 - (c) Adequate controls are in place for the protection of data privacy.

III. AUDIT SCOPE AND METHODOLOGY

5. The audit covered the current policies, procedures, working practices and systems in UNMIS.

IV. AUDIT FINDINGS AND RECOMMENDATIONS

Control mechanisms implemented for managing sensitive data and information

6. OIOS noted that UNMIS had taken positive steps in establishing mechanisms for managing and securing sensitive information, through the issuance of the following policies and procedures:
 - (a) DFS Policy Directive required the use of a file classification scheme;
 - (b) UNMIS/HR Office had a policy for the protection of personal data;
 - (c) UNMIS/HR Office defined a "Check In/Out" mail groups, in-boxes and databases; and
 - (d) UNMIS Records Management & Archives Unit issued Training & Guidelines for:

-
- i. 10 Steps to improving records management;
 - ii. Applying UNMIS File Classification Scheme;
 - iii. Transferring inactive records to archival storage;
 - iv. Email management;
 - v. Identification of Vital Records; and
 - vi. Self-assessment of Records Risks.

Absence of Mission specific policies and procedures to ensure protection of data and information

7. With regard to the mechanisms put in place by UNMIS for managing sensitive information, OIOS identified some control weaknesses that if not adequately addressed, would expose the Mission to risks of loss of confidentiality of data. These control weaknesses were as follows:

- (a) Lack of Mission-specific policies defining access control rules and “need-to-know” requirements for support and substantive offices and staff;
- (b) A limited number of substantive offices were aware and/or trained in data privacy requirements and practices; and
- (c) Lack of standard procedures to ensure confidentiality of communication and storage of sensitive information.

Recommendations 1 and 2

(1) The UNMIS Director of Mission Support, in collaboration with DFS at Headquarters, should issue Mission-specific policies to define access control rules and “need-to-know” requirements for both its support and substantive offices and staff.

(2) The UNMIS Director of Mission Support should implement training/awareness initiatives specifically focused on the classification and handling of sensitive data.

8. *UNMIS accepted recommendation 1 and stated that the Chief of Staff is taking the lead in developing “UNMIS Guidelines on Management of Information on Code Cables”, pursuant to ST/SGB/2007/6 on “Information sensitivity, classification and handling”, ST/SGB/2007/5 on “Records-keeping and the management of United Nations archives”, and UNMIS Administrative Instruction No. 22/2007 on “Records Management and Archives”. The Guidelines will be circulated to all heads of Units/Sections once finalized. Recommendation 1 remains open pending submission to OIOS of the finalized guidelines on access control rules and “need-to-know” requirements for both support and substantive offices.*

9. *UNMIS accepted recommendation 2 and stated that the Records Management Unit of the General Services Section has started developing a training module to be delivered in the form of workshops (both in HQ and Sector HQs) in early February 2010. One of the key modules is information sensitivity and handling, and classifying sensitive information*

(including code cables and note verbales). UNMIS would also consider including a session on handling sensitive information at its weekly integrated induction programme for the newly deployed personnel. UNMIS also suggested that Headquarters, NYHQ prepare a handbook or a CD-ROM for distribution to new personnel during the pre-deployment training course in Brindisi/Entebbe on “handling sensitive information in the field”. Recommendation 2 remains open pending submission to OIOS of evidence documenting the awareness training course conducted in UNMIS.

Risks to the security and confidentiality of data

10. OIOS noted that the Mission did not have adequate tools and procedures to securely store and transmit sensitive data. In particular, the following were observed:

- (a) Systematic use of data stored only on local desktop computers;
- (b) Systematic use of un-encrypted emails to communicate sensitive information (including personal identifiable information);
- (c) Limited physical and human resources to ensure proper storage and retention of sensitive data; and
- (d) Lack of criteria and procedures in the substantive offices handling personal identifiable data that were also shared with other UN entities operating in the same programme areas (i.e. UNICEF).

Recommendations 3 and 4

(3) The UNMIS Director of Mission Support should procure adequate storage containers to ensure the safe-keeping of sensitive documents handled by substantive offices.

(4) The UNMIS Director of Mission Support should develop a protocol to regulate the disclosure of personal data with other entities operating in the same programme areas.

11. *UNMIS accepted recommendation 3 and stated that the Records Management Unit has received additional storage space in El Obeid. However, some logistical challenges have been encountered for the transportation of the records by road. Discussions are on-going to seek more space to be allocated in HQ to store sensitive documents.* Recommendation 3 remains open pending submission to OIOS of evidence confirming that the storage of sensitive documents has been completed.

12. *UNMIS accepted recommendation 4 and stated that in cases where business units advise UNMIS Communications and Information Technology Section (CITS) of special security requirements, CITS undertakes specific solutions commensurate with the level of security deemed necessary by the business units. CITS is in the process of recruiting two IT security officers. Upon their arrival in the Mission, they will take a lead in ensuring that risks to the security and confidentiality of data through appropriate confidentiality classifications are being considered and addressed by relevant responsible business units.* Recommendation 4 remains open pending submission to OIOS of the protocol and

procedures for the disclosure of personal data, developed by the IT security officers in coordination with the business units.

V. ACKNOWLEDGEMENT

13. We wish to express our appreciation to the Management and staff of United Nations Mission in Sudan for the assistance and cooperation extended to the auditors during this assignment.

cc: Ms. Susana Malcorra, Under-Secretary-General, Department of Field Support
Mr. Nicholas Von Ruben, Acting Director of Mission Support, UNMIS
Mr. Choi Soon-hong, Assistant Secretary General, Chief Information Technology Officer
Mr. Swatantra Goolsarran, Executive Secretary, UN Board of Auditors
Ms. Susanne Frueh, Executive Secretary, Joint Inspection Unit
Mr. Moses Bamuwanye, Chief, Oversight Support Unit, Department of Management
Mr. Byung-Kun Min, Special Assistant to the USG, OIOS
Ms. Eleanor Burns, Chief, Peacekeeping Audit Service, OIOS

CONTACT INFORMATION:

ACTING DIRECTOR:

Fatoumata Ndiaye: Tel: +1.212.963.5648, Fax: +1.212.963.3388,
e-mail: ndiaye@un.org

ACTING DEPUTY DIRECTOR:

Gurpur Kumar: Tel: +212.963.5920, Fax: +1.212.963.3388,
e-mail: kumarg@un.org

CHIEF, PEACEKEEPING AUDIT SERVICE:

Eleanor Burns: Tel: +1.917.367.2792, Fax: +1.212.963.3388,
e-mail: burnse@un.org

STATUS OF AUDIT RECOMMENDATIONS

Recom. no.	Recommendation	Risk category	Risk rating	C/O ¹	Actions needed to close recommendation	Implementation date ²
1	The Director of Mission Support, in collaboration with DFS Headquarters, should issue Mission-specific policies to define access control rules and “need-to-know” requirements for both its support and substantive offices and staff.	Governance	High	O	Submit to OIOS documented evidence of the finalized guidelines on access control rules and “need-to-know” for both support and substantive offices.	Not provided
2	The Director of Mission Support should implement training/awareness initiatives specifically focused on the classifications and handling of sensitive data.	Governance	Medium	O	Submit to OIOS documented evidence of the training/awareness training course conducted in UNMIS.	February 2010
3	The Director of Mission Support should procure adequate storage containers to ensure the safe-keeping of sensitive documents handled by substantive offices.	Information Resources	Medium	O	Submit to OIOS evidence confirming that the storage of sensitive documents has been completed	Not provided
4	The Director of Mission Support should develop a protocol to regulate the disclosure of personal data with other entities operating in the same programme areas.	Governance	High	O	Submit to OIOS the protocol and procedures for the disclosure of personal data, developed by the IT security officer in coordination with the business units.	Not provided

1. C = closed, O = open

2. Date provided by the United Nations Mission in Sudan.

ANNEX 2

*Use this page if the orientation of Annex 2 is portrait. If the orientation is landscape, insert a section break at the end of Annex 1 and continue on the new page. (On the **Insert** menu, point to **Break**, select **Next page** under **Section break types**.) Leave the page blank if not required; do not delete it.*