INTERNATIONAL MONETARY FUND
WASHINGTON, D.C. 20431

CABLE ADDRESS
INTERFUND

DEPUTY MANAGING DIRECTOR

January 30, 2004

To: Members of the Staff

E-mail and the Internet—Transmission of Sensitive Information

1. I wish to remind staff not to use personal and Internet-based e-mail accounts (e.g., those established through AOL, MSN, Yahoo, etc.) for business purposes involving sensitive information. Such accounts do not provide safeguards sufficient to protect the confidentiality of sensitive Fund information. Staff should use, without exception, the Fund's email and remote access facilities for secure communication.[1]

2. The ease with which electronic information can now be shared calls for added vigilance in handling sensitive information. Accordingly, the Fund's information security policy is designed to protect such information against unauthorized access by third parties. The policy classifies the security level of information and thus provides an indication of the degree of care that needs to be taken to prevent its falling into unauthorized hands. In addition, the Fund has incorporated security measures into its e-mail system which, by default, encrypt message content and attachments, and has provided for secure communication through its three remote access facilities.

3. For these reasons, staff should use the messaging systems that the Fund has put at their disposal and that provide secure communication. When in the office at headquarters, staff should use the Fund's e-mail system for sending any sensitive information, and refrain from using personal and Internet-based e-mail accounts. When at home, on mission, or in a resident representative office, staff should use the remote access facilities or the e-mail system provided by the Fund.

4. On occasion, staff may have resorted to personal and Internet-based e-mail accounts in case of urgency when the Fund's e-mail system was unavailable because of scheduled maintenance work. I am therefore pleased to report that, before the end of February, TGS will have in place a back-up system that will reduce the unavailability of the Fund's e-mail system during maintenance or other interruptions to less than thirty minutes.

[1] These are the Web-based terminal server (for e-mail and other applications), the Cyber Café (for Web-based e-mail only) and the Fund's VPN (Virtual Private Network, a secure connection to the Fund's local network including Outlook e-mail across the Internet).

5. The basis of this policy can be found in the guidance management issued to staff in October 2002, on *Information Security—Policies Regarding Classified Documents* (General Administrative Order No. 35, Rev. 1). Staff also received through their departments more detailed *Information Security Guidelines* and a *Practical Guide to Information Security.* All three documents can be found on the Fund Intranet under the heading of Information Security at: http://www-int.imf.org/categories.asp?Item=6.

6. If you have any questions on security of information or communications, please contact TGS, Security Services Division (Mr. Avignone, ext. 38895).

Shigemitsu Sugisaki