The Global Fund to Fight
AIDS, Tuberculosis and Malaria

Global Health Campus
Chemin du Pommier 40
1218 Grand-Saconnex
Geneva, Switzerland

theglobalfund.org

Geneva, 22 April 2020

Dear Global Fund Principal Recipients,

The use of information systems exposes organizations to cybersecurity risks including phishing, a fraudulent practice used to collect important information from users or provide them with incorrect information to obtain unlawful advantages.

A recent investigation by the Global Fund's Office of the Inspector General found deficiencies in the security, access and controls of IT systems of an implementing partner of programs the Global Fund supports. The main findings pointed to unsafe processes and procedures, particularly concerning the management of critical data, including key information relating to bank accounts, suppliers, service providers, consultants and staff, leaving the implementer and the Global Fund potentially vulnerable to attack.

To support implementing partners in ensuring robust processes and procedures are in place for the management of critical data, the Global Fund has developed a guidance note on information systems and data management, attached to this letter.

All Principal Recipients should review carefully their internal procedures and guidelines to ensure that appropriate risk mitigation measures and staff trainings are in place to address cybersecurity risks. Principal Recipients are expected to update their internal manual of procedures and guidelines as needed to incorporate the controls described in the guidance note. Each Principal Recipient is requested to confirm in writing to its Global Fund Country Team that this update has been completed by **30 June 2021**.

If you have any questions, please do not hesitate to reach out to your Country Team.

Best regards,

The Global Fund

Resource:

- Guidance Note on Information Systems and Data Sharing