GUIDANCE NOTE ON INFORMATION SYSTEMS AND DATA SHARING

19 August 2020

Objective

The use of information systems, including email communications and electronic data sharing, is critical for the effective achievement of organization objectives and is key for efficient, reliable and timely availability of financial data for decision making at various levels of grant implementation.

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

Accordingly, Principal Recipients are expected to update as needed their internal manual of procedures and guidelines to ensure that effective management controls are in place to safeguard data related to activities implemented through Global Fund grants. In particular, critical data must be secured, especially data relating to bank accounts, suppliers, service providers, consultants and staff. This may require introducing or modifying procedures to implement these controls, as outlined in the recommendations below.

This guidance note does not amend, nor does it constitute a waiver of any rights or obligations under, Global Fund grant agreements. Principal Recipients must continue to ensure that they, and all their implementing partners (including Sub-recipients, suppliers and contractors), comply with applicable laws and regulations, such as those relating to the collection and processing of personal data and, the transfer of such data to the Global Fund upon request[1].

Key principles

The following key principles must be applied in all cases, irrespective of the nature of critical data:

- **Segregation of responsibilities**. Personnel responsible for processing payments should not have the right to access or make changes to the related master database maintained by the Principal Recipient or grant implementer. Changes to critical data must be approved by a senior staff member with appropriate authority who is functionally segregated from the persons undertaking the payment and amendment processes.

[1] For further information, refer to the Global Fund Privacy Statements https://www.theglobalfund.org/en/legal/privacy-statement/

- **Accountability**. The database should be managed by staff with appropriate authority over each respective module and there should be integration among modules. The principle applies to the management of Excel files if the system is manual-entry.
- **Confirmation**. For all payments above US$50,000[2], it is strongly recommended that the Principal Recipient obtain formal confirmation from the supplier's designated contact person before initiating the payment.

Specific controls

1. **Bank accounts**
   - Data related to bank accounts should be maintained in the Cash Management module of the database, or in files in the case of a manual system, by a person or department functionally segregated from the person or department responsible for processing payments.
   - Principal Recipients are strongly encouraged to implement multiple-signatory requirements for material and/or complex transactions. Principal Recipients are also encouraged to rotate authorized signatories for disbursements on a regular basis.
   - The requirements (as outlined in Annex 1) related to adding or deleting bank account information should be followed before updating the Cash Management module of the database, or manual systems as appropriate. Please refer to Section 5.6.1 – *Bank Account Management* of the Financial Management Handbook for Grant Implementers for further detail.

2. **Suppliers and service providers**
   - Principal Recipients should have a clear process for performing background and due diligence checks before signing or amending a contract with any supplier or service provider, including verification of key information such as business registration (through certificates) and bank account details.
   - All key information, including the name of the organization, authorized signatory, contact person, registered address and bank account details, should be included expressly in the contract.
   - Any request to change any of the supplier's or service provider's key information should be supported with appropriate documentation, verified and approved by authorized personnel before the information can be modified in the database and in the contract.
   - Sensitive correspondence, including relating to any request to change the key information of the supplier or service provider, should be conducted only through the contact person designated in the contract.
   - The supplier or service provider should be classified as inactive in the system only when all liabilities and obligations under any contract involving the supplier or service provider have been discharged in full.

3. **Staff and consultants**
   - Personal data, including names, dates of birth, and bank account details, should be maintained in the Human Resources (HR) module of the database, or personnel files, by authorized staff of the Principal Recipient.
   - Staff who are responsible for payroll preparation and/or payments, should not have the rights or access to modify or change personal data of staff in the organization.

[2] Or the threshold defined by the Principal Recipient, if it is lower.

- Personal data in the HR module should be integrated with the data in the cash management module to facilitate payment processes. In the case of a manual system, appropriate management controls, including verification, review and approval, should be in place.
- For further detail on staff data creation, modification or deletion, please refer to Section 4.5 - *Human Resources* of the "Financial Management Handbook for Grant Implementers".
- Safeguards should be put in place for data that identifies, or could be used to identify, individuals such as staff and consultants. Safeguards may include technical and organizational measures, such as access permissions, anonymization, confidential classification of sensitive personal data, retention periods to ensure personal data is not kept longer than necessary and secure systems for storing and transferring personal data.
- For further guidance on protection of personal data, please refer to the recommendations issued by the applicable data protection authority for your jurisdiction.

Strengthen your Information Security Management Systems

Implementers should take steps to continually strengthen the information security of their digital and information technology architecture, following best practice international standards, e.g., ISO 27001[3] and ISO 27002 (codes of practice)[4]. These framework standards provide implementers with guidance on how to manage information security risks, with the view to preserving the confidentiality, integrity, and availability of information by applying a risk management process and to giving assurance to interested parties that risks are adequately managed.

Additionally, the following references may aid implementers in developing their digital and information technology architectures, including defining policies and standards for security and privacy protection:

1. WHO ITU National eHealth Strategy Toolkit[5];
2. Digital Health Platform Handbook: Building a Digital Information Infrastructure (infrastructure) for Health. Geneva: International Telecommunication Union[6];and
3. Principles for Digital Development[7].

Training staff

As part of basic financial and cybersecurity risk management and good practices, Principal Recipients are expected to ensure staff are properly trained and aware of the characteristics and methods used in cybersecurity attacks, including phishing. There should be dedicated staff to receive and address queries related to financial and cybersecurity risks.

An online Phishing Training course is available for external partners (link). All CCM, PR and SR staff involved in financial transactions are required to take this training. The training takes 15 minutes to complete.

[3] https://www.iso.org/isoiec-27001-information-security.html

[4] https://www.iso.org/standard/54533.html

[5] https://apps.who.int/iris/bitstream/handle/10665/75211/9789241548465_eng.pdf?sequence=1&isAllowed=y

[6] https://ehna.acfee.org/c67802a7d4b3dc8914700842bf6776402b8d343c.pdf

[7] https://digitalprinciples.org/

Staff involved in the following activities are required to take the training:

1. Modification of third party data (banks, suppliers, staff and consultants);
2. Payment of transactions; and
3. Ordering payments.

PRs are also responsible for ensuring that SRs complete the training. Local Fund Agents will verify the implementation of the training during the next PUDR review.

Participants who are not registered in the Global Fund iLearn platform are required to take a few minutes to register (here). Once registered, they will be able to access other free e-learning Global Fund courses such as Grant Making and PR Reporting.

Annex 2 of this guidance note highlights options and related resources for the above. Principal Recipients should explore these and other available resources and ensure staff are strongly encouraged to undertake adequate training.

Annex 1: Recommendations on internal procedures for the creation, change or deletion of key data related to suppliers and service providers.

Key Information	Creation	Change	Deletion
Bank Account	▪ Bank account details should be included in the database only when: ✓ A bank information form (preferably in a predefined format supplied by the PR) is provided; ✓ A list of authorized bank account signatories (at least two signatories), with certified signature specimens, is provided by the supplier or service provider; ✓ Procedures for multiple signature for complex or large transactions (over a defined threshold) are provided; ✓ A formal confirmation (letter) is obtained from the bank holding the account, on bank letterhead; ✓ The bank holding the account is included on the World Bank list of eligible commercial banks (or another internationally recognized list); ✓ The bank has been cleared following anti-terrorism screening, e.g. through ✓ https://bridgerinsight.lexisnexis.com/; ✓ The account's IBAN has been verified, e.g. through https://www.tbg5-finance.org/?ibancheck.shtml; and ✓ The bank's SWIFT code is verified through https://www2.swift.com/bsl/index.faces ➢ **Red Flags**: ○ The bank account is in another name than the supplier's or service provider's name ○ The account holder's address is different from the supplier's or service provider's registered address	▪ Bank account details should be changed only when: ✓ All steps outlined in the creation column are followed. ✓ The request is sent by the designated contact person through a formal communication on official letterhead; ✓ The request is duly signed by an authorized signatory; ✓ The request includes a valid justification for change; ✓ The change must be reviewed by senior staff before being validated; and ✓ The person processing the payment is not the one validating the change (segregation of duties)	▪ Bank account details should be classified as inactive in the database when all liabilities under any relevant contract have been discharged in full. ▪ Independent senior staff should review the entire supplier/service provider database on an annual basis to confirm active and inactive status. ➢ **Red Flags**: There are no outstanding liabilities under any relevant contract but the supplier or service provider is still listed as active in the database.
Contact for Notices	The contact information (including email address) of the person authorized to receive and send correspondence on behalf of the supplier or service provider should be included in each relevant contract.	All steps outlined in the creation column must be followed. Any request to change contact person information should be communicated only by an authorized representative of the entity through a formal letter. re-confirmed by implementers (by the senior staff of the implementers and/or the concerned entity for which the person is working for).	
Authorized Contract Signatory	Authorized signatory information should be created only when: ✓ Proof of authority to sign the relevant contract on behalf of the entity is provided (e.g. certificate from senior management; by-laws) and verified; and ✓ The signatory provides a certified signature specimen (preferably in a predefined format supplied by the PR or grant implementer).	All steps outlined in the creation column must be followed. Any request to change authorized signatories (e.g. for amendments to the contract) must be sent by the designated contact person through a formal communication on official letterhead duly verified by the implementer through confirmation from senior management before making any change.	
Counterpart Address and Contact Details	The entity's registered address, mailing address, email, fax and phone number, should be included in each relevant contract. The registered address should be verified through public records where available.	Any request to change the entity's registered or mailing address should be communicated by the entity's contact person duly verified by the implementer through confirmation from senior management before making any change. All the steps outlined in the "Creation" column should be followed.	

Annex 2: Additional Information Security resources to address cybersecurity risks

In addition to the online Phishing Training course provided by the Global Fund, Principal Recipients can request a range of information security services from information security service providers:

1. Information security awareness training
2. Strengthening Information Management Systems

The Global Fund is finalizing a list of pre-approved technical assistance suppliers to assist PRs and other grant implementers to improve information management systems and cyber security.

Additionally, Principal Recipients and other grant implementers may wish to consider Multi Factor Authentication. Please refer to the relevant email service provider's terms and conditions and guidance for activating multi-factor authentication. See below more details for Gmail and Yahoo.

- Gmail : https://www.google.com/landing/2step/
- Yahoo: https://help.yahoo.com/kb/add-two-step-verification-extra-security-sln5013.html

Principal Recipients and other grant implementers may also wish to consult the ISO 27002 Code of Practice for information Security Controls[8]. A strong information security management system (ISMS) can benefit Principal Recipients and other grant implementers by giving their beneficiaries and stakeholders confidence that they can protect their information, manage their finances and improve supply chain security.

[8] https://www.iso.org/standard/54533.html