**Electronic Funds Transfer Standards**

1. The main purpose of this document is to:
2. Establish the policy that governs the management and operation of Electronic Fund Transfer (EFT) to protect UNDP financial assets and to inform UNDP users about the processes and controls pertaining to EFT transactions.
3. Establish a procedure for efficiently processing EFT payments to UNDP Suppliers, and Staff.
4. Ensuring a controlled protocol for releasing UNDP banking information to authorized third parties.
5. Ensure that UNDP receives accurate and sufficient information to correctly process outgoing and incoming EFT payments in a timely manner: as EFT data standards vary among financial jurisdictions.

**Note:** EFT is an Electronic Funds Transfer method implemented with banks using a) ISO Standard 20022, b) and any other electronic method using a ICT approved security standards.

1. This policy shall apply to:
2. UNDP Staff Members responsible for the management and or operation of the EFT process
3. All ICT resources used in the EFT process which are owned or managed by UNDP or provided by UNDP through contracts and other agreements with UNDP
4. EFTs must be traceable, uniquely identifiable, and reconciled on a periodic basis. Entry of financial transactions into Quantum is restricted by the prevailing Financial Rules and Regulations, Internal Control Framework (ICF) and Procurement Guidelines. Any request for the preparation of an electronic fund transfer must be supported by a purchase order, original invoice, or equivalent which indicate the propriety of the expenditure. Such documentation will be provided to, and reviewed by, staff responsible for the processing and authorization of those items prior to their approval.
5. EFT payments must be documented and approved subject to the ICF. The audit trail must evidence the generation and approval of the EFT, evidence of the transmission, and a confirmation that the EFT was processed by the financial institution. Documents or electronic data supporting EFT transactions must be safeguarded against loss or destruction and must be in a retrievable format. Documentation must be maintained in accordance with established retention guidelines. UNDP banking information must not be published (electronically or otherwise) in a format that could result in its wide and inappropriate distribution. It should only be shared with known approved third parties.
6. Only the UNDP Treasurer or designated officials shall grant the authority to the CO Representative to establish an EFT local interface at CO level.  Please refer to the Treasury policy [Establishment and Use of Electronic Banking Systems](https://popp.undp.org/node/10731) and [E- Banking with Quantum Design and Implementation Guidelines](https://popp.undp.org/node/3206) issued by UNDP ITM and Treasury for further information. Consistent with ICF, the file transfer should be handled by at least two individuals (one to approve and one to release) who do not have authority to create or approve suppliers. The Representative must document the name, title and contract status of the staff who approve and release payment instruction files.
7. Offices must use a valid and approved electronic sampling methodology to check the accuracy and certification of all payments and to ensure the integrity of the disbursement. In practical experience, the validation is done through review of bank acknowledgements, check of batch totals and lastly by bank reconciliation. When file uploads are executed on web e-banking, the validation is completed in at least two stages, first by the file uploader who will validate with more detail sampling and then by the approver who will validate the number of transactions, absolute total amount and sampling of the itemized transactions. Approved payments must be made within the agreed upon terms between UNDP and its goods or service providers. All payments must be properly and accurately recorded in the accounting records during the period in which the liability was incurred or the payment was made. This will ensure the appropriate allocation of expense and revenue recognition and is consistent with UNDP accounting practices.

Segregation of Duties

1. The UNDP Office of Financial Management promulgates guidelines in the ICF to ensure proper segregation of EFT creation and approval.
2. UNDP security policies and supporting access control software should enforce a clear separation of duties and effective checks and balances for the creation and transmission of EFT payments. Staff are authorized to have access to the systems to send EFT payment instructions in accordance with current security policies.
3. The UNDP Treasury Division is responsible for establishing and maintaining the operational controls specified in this policy. ICT Security is responsible for establishing and maintaining security controls specified in this policy (data shall be encrypted and transported through a secured protocol transmission, such as SFTP). When Web e-banking solution is used as a manual file upload method, the final payment files (UFF) when downloaded from the Quantum should be handled strictly by the authorized staff who will manually upload into the banks’ platform. Treasury Division and ITM will be responsible for EFT operations at HQ and will work with CO EFT Approvers, Requestors and System Administrators to ensure EFT operations are performed in accordance with the policies and guidelines established in this document.
4. No single staff member will be authorized to perform the entire funds transfer process. The UNDP Chief Information Security Officer (CISO) will not change or authorize access to information systems or software used to transfer funds without the written approval of the Director of Finance. A written, signed request will be required and maintained by the CISO to document any such changes. Authority for EFT interface in the Country Office(s) lie with the RR (Resident Representative) as per no. 5 above.
5. The Self- Assessment process provided in the [Annex 1](https://popp.undp.org/node/821)can be completed by the CO as a best practice to facilitate the creation of a user profile matrix and the verification of effective user segregation for an UNDP office.

User ID / Password Security

1. The UNDP Password Policy governs the construct, management, and other issues associated with passwords for UNDP applications, such as Quantum. In addition to the provisions of this process, the process related to Quantum Finance application user accounts (User IDs/ Passwords) is:
   1. Only users who have been validated to require access to the Quantum Finance application (See section on Granting Quantum Finance User Access) will be given an Quantum Finance application user account.
   2. Each user will have a unique and distinct Account. Proprietary bank software programs used to transfer EFTs that include common passwords that may be used by more than one authorized users are excluded from this requirement.
   3. Users will be issued a temporary one time password and will be required to change this password upon initial log in to the Quantum Finance application.

Physical Security and Environmental Controls

1. Physical access to computer and network hardware, software, data, and documentation must be specifically authorized by management and restricted to only those personnel requiring such access for performance of assigned functional responsibilities. Each UNDP country office must explicitly demonstrate measures to safeguard e-banking access and other sensitive EFT system from unauthorized access by employing adequate physical security controls available to the local office. In order to maintain comprehensive records of user access details when accessing the e-banking platforms, the recommendation is to enforce the use of biometric devices or electronic card readers/ tokens.  The records should include: User ID, date and time.

Network Security

1. EFT files transferred to a bank at HQ under Direct Host-to-Host connection in Quantum must use secure protocols such as SFTP, SSL (more than 128 bit encryption). Acknowledgement files, reconciliation reports containing sensitive information need to follow the same guidelines.

EFT System Operations and Backup

EFT files and reports will be backed up following UNDP backup provisions for sensitive information as per [ICT Disaster Recovery Standards policy](https://popp.undp.org/node/10916) .

Violations of Policy

1. Use of ICT resources or data provided by UNDP constitutes agreement to the policies and standards contained in this document, and acceptance of accountability for compliance with them. Violations of these policies and principles, or activities inconsistent with relevant UN Staff Regulations and Rules may be subject to disciplinary actions.

Enforcement

1. To ensure compliance with the provisions outlined in this policy UNDP will establish processes and tools that will automate policy enforcement and will allow the monitoring and auditing of ICT resources and EFT transactions.

Investigations

1. Reviews of violations to this policy will be investigated according to guidelines and procedures of the organization. Violations of the policy may be investigated by the organization, to determine if misconduct or other violations of the code of conduct have occurred. Staff members who have been found to violate policy may be subject to accountability and disciplinary measures as defined by the UNDP Prescriptive Content on Accountability, Disciplinary Measures and Procedures.

Liability

1. Management and operations of EFT which is in contravention of the present policy and causes financial or other loss to UNDP, its clients, or its partners may result in the responsible staff member being held personally liable for such consequences, per UN Staff Rule 112.3.

Disciplinary Actions

1. UNDP policy prohibits the use of UNDP property for illegal purposes and for purposes not in support of UNDP mission. In addition to any possible legal sanctions, violators of this Policy may be subject to disciplinary action and/ or resulting in suspension of access. Suspension of access will be reported in the Performance Management and Development (PMD) of the staff member. OHR will be advised in such cases and further appropriate action may be taken, in the event of misconduct, per UN Staff Rule 110.1, UN Status, basic rights and duties of United Nations staff members (ST/ SGB/ 2002/ 13), and as defined by the UNDP Prescriptive Content on Accountability, Disciplinary Measures and Procedures.

Violations by Non-Authorized Users

1. Individuals or organizations not authorized to use UNDP ICT resources or data that have been found to violate this policy including the commitment of fraud using UNDP ICT resources or data will be prosecuted to the greatest extent of applicable law.

Effective Date

1. This process shall enter into force on when published to the POPP. Any questions regarding this policy may be directed to:
2. Treasurer, Office of Financial Management, OFM/ BMS
3. Chief Finance Officer, Office of Financial Management,

OFM BMS

1. Chief Information Officer, Office of Information Technology and Management, ITM/BMS

ITM BMS

1. Director, Office of Legal Services, OLS/ BMS
2. Director, Office of Audit and Performance Review, OAI
3. Director, Office of Human Resources, OHR/ BMS