Document 1.2
Best Practice Guidance on the use of
Electronic Banking Systems

Introductory Note

The purpose of this guideline is to provide those Boards who are beneficiaries of programmes that Pobal manage, on behalf of the Government, with general information on best practice in the area of Electronic Banking Systems (which may also be referred to as Internet Banking systems or Online Banking Systems).

Decision to implement an Electronic Banking System

The decision to implement an Electronic Banking System must be made by the Board of Directors. This decision must be approved and minuted in the Board papers. The decision should result from the research and investigation of more than one Electronic Banking product available from the banking institutions. Careful consideration should be given to issues such as security, access, functions, reports etc. The Board should assess the internal control risks associated with the introduction of an Electronic Banking System and where such a system is considered appropriate, the rationale for the final choice should also be noted.

Electronic Banking Internal Procedures Document

Once the decision to implement an Electronic Banking System has been taken, the Board must ensure that an internal procedure is written up and incorporated within the groups overall Internal Financial Procedures Document. Where appropriate, the Internal Financial Procedures Document should be cross-referenced to any relevant user manuals and/or system guidelines provided by the bank and the final document should also be approved and minuted by the Board.

This document must clearly outline the use of Electronic Banking within the organisation, with clear instructions in relation to the following:

- Bank accounts to be accessed
- Named authorised users - positions within organisation (staff / senior management), Board members, and Finance Sub-Committee members. All payments must ultimately be authorised by a Board member / registered director / others included within the existing current account mandate in line with the controls in place for making payments by cheque.
- Access to functions of system by individual users e.g. view only, print only, authorise payments, add new accounts, delete accounts, set up standing orders / direct debits etc.
- The additional controls regarding payments to suppliers i.e. cross reference bank account details to the payments listings on a regular basis.
- The inclusion of individuals with newly granted access to the system (i.e. Board members, directors, staff) and the deletion of individuals who no longer have access to the system, should be authorised at a senior level i.e. by the Manager or a Board member / registered director.
- The inclusion of new bank accounts onto the system and the deletion of old accounts from the system must also be approved in a similar manner.
- Thresholds regarding Euro value of transactions per day / week / month / per authorised user, which should be approved by the Board and set at a realistic level having regard to the average recurring payroll costs.
- Details regarding number of users required per type of function e.g. one user may view bank statements, minimum of two users to authorise a payment.
- Security controls regarding access to system & passwords.

Review of Electronic Banking Internal Procedures Document

The Internal Procedures Document should be reviewed and, where appropriate, updated at least once a year. The results of this review should be approved and minuted by the Board.

The Document must be reviewed and updated following changes to the Electronic Banking System. These changes must be approved and minuted by the Board prior to their implementation. Such a change may result from staff turnover and new appointments in relevant roles with responsibilities in the area of Electronic Banking.

Changes regarding users must also be communicated to the Bank so that old users may be deleted from accessing the system and new users added, per the Board's signed authorised mandate.

Security Issues

The security of the Electronic Banking System is vital. The Board must ensure that all necessary procedures are in place to protect the system from misuse.

All passwords / user names / codes must not be stored within the office environment. This will prevent unauthorised individuals from accessing them. Passwords may be memorised and destroyed rather than stored where they could be accessed.

Passwords / user names / codes should be confidential, therefore they must never be shared between individual users. They should be unique and individual to named authorised users of the Electronic Banking System.

Passwords / user names / codes should be changed regularly. They should automatically lapse after the expiration of a given time period e.g. 90 days. This will automatically require them to be changed.

Any separate handheld electronic devices that form part of the banking system (i.e. devices that provide unique transaction codes for subsequent input to the computer system) should be securely stored under lock and key.

The Board must also decide and minute the number of PC's to have the Electronic Banking System installed on them. The number of authorised users among the organisation's staff should inform this decision. The fewer PC's with the relevant software will add to the security of the System.

Segregation of Duties

It is vital to ensure the segregation of duties when using an Electronic Banking System. Such segregation protects the beneficiary from the possible misuse of the System by any one user and thus minimise the possibility of fraudulent transactions being undertaken.

The authorisation of transactions on an Electronic Banking System should not differ from those implemented on a manual paper-based system. The Internal Financial Procedures Document should detail the users responsible for different elements of the functions used on the system. For example, one user may prepare a payment on the System and a different user/s may authorise the payment. Before payments are processed, it is the responsibility of those authorised individuals to ensure adequate checks have been made and payments are transferred to the correct bank accounts, in line with your Internal Financial Procedures Document.

A user cannot exclusively authorise a payment to themselves. Such payments will need to be authorised by other user/s at a higher level within the organisation, e.g. a manager's salary should be co-approved by a Board member / registered director.

The Internal Procedures Document should outline the procedures to be implemented in the event of annual leave / sick leave by a user. These procedures should allow for the continued efficient running of the business while also adhering to the procedures agreed for the Electronic Banking System.

Where segregation of duties is not a viable option due to a limited number of staff, the beneficiary must implement additional controls to ensure there are satisfactory procedures in place i.e. increased review and monitoring of payments by Board members, members of the Management Committee etc. No one individual should have full autonomy.

Monitoring of use of Electronic Banking System

The Board must ensure that the use of the Electronic Banking System is monitored on an on-going basis. Such monitoring will ensure that all transactions are legitimate business transactions and have been conducted appropriately, in line with agreed approval procedures.

The Board, through the internal procedures document, must clearly identify the individuals responsible for this monitoring e.g. manager, Finance Sub-Committee, Board members. The Board should also detail the frequency of this monitoring. It is not appropriate for an individual preparing transactions to also monitor these transactions. Segregation of duties must be applied as much as possible.

Monitoring of transactions should include, but not be limited to, the following:

- Payments and transfers (including internal transfers)
- Setting up of new accounts
- Deletion of accounts
- Payroll transactions, with particular focus on start and finish dates for staff members

Banking Institution

As part of the Board decision to select a provider for the Electronic Banking System, the services provided should be reviewed. These should be considered in line with the Boards expectations and needs.

The agreement between the beneficiary and the banking institution should include the provision of the Electronic Banking System, a manual for its operation, training for users and a support / help desk function for the ongoing operation of the System.

The Board should also discuss the capabilities of the System with the Bank and agree the functions to be adopted and used and those to be blocked / removed. It may not be necessary or appropriate to have all the functions available to an individual beneficiary e.g. Share Trading functions.

Every group must have the original documentation used to set up the electronic banking system with the Bank on file. It should be a comprehensive document which provide details of the capabilities of the system i.e. functions, user controls, authorisation thresholds etc. It is essential that all groups retrieve this information from the bank in the immediate future, if it is not readily available. It should also be noted that it will be subject to audit from the 1st January 2009.

Summary

This guideline is to assist beneficiaries in the operation of a banking-on-line system. It is in addition to Programme Guidelines for financial management and accounting procedures and practices previously issued by Pobal.