**Electronic Banking Policy and Best Practice Procedural Guidelines**

General Comments -

* This is a template/precedent document only. It should be tailored as appropriate to suit the needs of each individual firm.
* All sections should be considered and implemented as deemed appropriate for the firm. This cover page should not be included.
* The LQSI cannot accept any responsibility for any errors or omissions contained in this template document.
* The document should be reviewed on an annual basis, or as required.

Specific Comments –

* These procedures should be followed when working remotely (with enhanced procedures if required) and to reflect additional cybersecurity/resilience questions in the 2020/21 Common Proposal Form.
* The new Solicitors Accounts Regulations 2023 came into force on the 1 July 2023 and apply from the beginning of a firm’s next accounting year e.g. if a firm’s year end was the 31 October 2023, the new regulations will apply from the 1 November 2023. This policy was updated in February 2024, to reflect who is an ‘authorised signatory’ under the new regulations and also the new requirements in relation to retaining EFT records.
* This policy also references the July 2023 Practice Note from the Conveyancing Committee regarding protecting solicitors’ client accounts in conveyancing transactions.

The Legal Quality Standard of Ireland

Updated February 2024

**[Firm Name]**

**Electronic Banking Policy and Best Practice Procedural Guidelines**

Electronic Banking is now increasingly used as a payment tool in law firms. In this regard, the setting of internal controls will be imperative for all businesses small, medium or large. The same internal controls implemented in the firm that are applicable to manual banking transactions should apply for e-banking transactions, at a minimum. In addition, if staff (fee earners, accounts staff or the Principal/Partners with authority to authorise EFTs) are working remotely, all of the controls listed in this policy must continue to be followed with appropriate additional measures implemented, as required, in relation to IT security and verifying transactions.

Law firms face considerable risks with regard to paying money out to third parties and beneficiaries and it is very important that they take as many precautions as they can in order to mitigate these risks. Where possible dual authorisation should be in place so that two people are involved in both setting up and making payments in e-banking.

Best Practice Internal Controls

Electronic Payments

We at [*Name of Firm*] are aware of and have introduced procedures to comply with the requirements under Regulation 25(1)(h) of the Solicitors Accounts Regulations 2023 (hereinafter referred to as SAR 2023) which came into force on the 1 July 2023, namely:-

For all client account transactions, a copy of each document of record issued by the bank in respect of electronic transfers of funds must be kept on a file dedicated for that purpose.

Where moneys are withdrawn from a client account by means of an electronic funds transfer from the client account, the solicitor shall retain on the client’s file, and a copy on a separate file dedicated to recording such transactions, the document of record issued by the solicitor and such other documentation issued by the bank to confirm that the transaction has been completed in accordance with the instructions of the solicitor.

Where moneys are received by electronic funds transfer into the client account, the solicitor shall also retain on the client file a copy of the document of record issued by the bank to confirm that such transaction has taken place.

*[Firm can add to the above to specify the procedures they have in place.]*

Assigning of rights and Authorised Signatories

The assigning of rights to electronic banking administrators and users is the first critical step. This is where the controls and payment limits are set. Ideally a minimum of two administrators / users should be set-up one of which must ~~should~~ be an “authorised signatory” ~~e.g. a principal or partner~~. - Regulation 9(5) of the SAR 2023 sets out who can be an “authorised signatory”.

Regulation 9(5)(a) of the SAR 2023 states ‘an “authorised signatory” under these regulations shall be, subject to Regulation 9(5)(b) and 9(5)(c), a solicitor who is a partner or sole practitioner in the firm with a practising certificate in force who is authorised to sign cheques or to conduct electronic transfers of funds on the client account.’

Regulation 9(5)(b) of the SAR 2023 states ‘where there is more than one authorised signatory, a person who is not referred to in Regulation 9(5)(a) above may act as an authorised co-signatory where at least one of the authorised signatories is a solicitor within the meaning of Regulation 9(5)(a)’.

Regulation 9(5)(c) of the SAR 2023 states ‘a person who is not a solicitor within the meaning of Regulation 9(5)(a) above may act as the sole authorised signatory for a firm if the Society is satisfied that there are exceptional circumstances permitting such a person to act and has granted prior approval in writing for same.’

Setting up a Beneficiary:

When creating a beneficiary in e-banking it is crucial to ensure that the correct bank account is assigned to the correct beneficiary. Verification of the correct beneficiary is not always carried out by banks and should not be relied upon. The account number and sort code of the beneficiary has now been replaced with a BIC and IBAN code.

* The bank account details should be communicated by the payee on formal headed note paper where possible or if emailed they should not be contained in the body of the email.
* Administrator / User 1 sets up the account in e-banking.
* Administrator and Authorised Signatory / User 2 approves the beneficiary, ensuring the correct bank account details are assigned to the correct beneficiary.
* Once the first payment is made, a follow up phone call should be made to the beneficiary to confirm the safe receipt of the funds.

Making a payment:

* Ensure that there are cleared funds in the client account prior to making the payment.
* Ensure that typed written instructions are received to include the name of the third party to whom payment is being made and all relevant bank account details of the payee.
* User 1, with the approved invoice / cheque requisition to hand, inputs the value to be paid. A payment date can often be specified.
* User 2 should authorise the payment, checking the value back to the invoice / documentation.

Physical Security:

* Do not share Digi passes / Fobs or Pin codes. These physical means of security should be locked away in the firm’s safe at the end of each day as was done with cheque books and cheque stationery in the past.
* 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.

Passwords:

* All passwords / user names / codes must not be stored within the office environment to prevent unauthorised individuals from accessing them. Passwords should 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.

Other safeguards:

* The firm should incorporate into the terms and conditions of the engagement letter and/ or S.150 Notice the responsibility of the recipient of funds to provide the correct client and other third-party bank account details.
* Ensure that anti-virus software is in place and up-to-date and that a firewall and/or other appropriate network safety security safeguards are in place.
* Online payments should be made from within the office to avail of the network safety security safeguards in place.
* Ensure a receipt or acknowledgment of receipt of payment is obtained from clients/third parties and retained on file.
* Ensure that online payments are authorised by an ‘authorised signatory’ ~~the principal or one or more of the partners~~ with appropriate supporting documentation.
* Are all instructions subject to authentication by the employee receiving the request by one of the following:-
  + Making a call back to the requestor using a predesignated telephone number that is held on file for the purpose of call back. It is recommended that either a fee earner/secretary or other member of staff familiar with the file/recipient completes this verification call
  + Verifying that the requestor has the authority to make such instruction.
  + Prior to payment of request being actioned, ensuring supporting documentation of the payment transfer request is provided.
  + Verifying that any signature provided on any written instruction or telefacsimile matches that held on file.
  + For email instructions verifying the requestors work email address has been used.
* For telex or telefacsimile, ensuring the test key/algorithm matches that held on file.
* With respect to vendors/suppliers all requests for payment should be subject to verification that such vendor/supplier is owed such funds.
* Prior to payment, payment details should be verified with the supplier with those held on file.
* Before any change is made to a third party’s account details, we obtain authorisation from the third party via an authentication method which is different to the original method used to request the change.
* Before we transfer funds to an account that we have not paid into before, we obtain authorisation from the recipient of the funds via an authentication method which is different to the original method used to request the transfer.
* Notify the bank, without delay, in the event of any suspicious online activity.
* The firm should consider putting in place an insurance policy to cover theft and possible online fraud.
* Take a printout (from the banking online system) of the transaction at the time of making the payment.
* Retain all subsequent correspondence relating to the payment on file, e.g. outward payment advice note.
* Ensure that the correct bank account is chosen to make the payment from.
* Ensure regular staff training is provided to all staff and that up-to-date best practice guidelines are followed.
* In conveyancing transactions and in accordance with the Law Society Practice Note in July 2023 ‘Protection of solicitors’ client accounts in conveyancing transactions’, where the vendor’s solicitor wishes to include account details in the Contract (or other document likely to be issued to the purchaser or other third party), it is prudent that the bank account number should not be included in totality. Consideration should be given to redacting, for example, the last four digits necessitating further verification action.

Staff Training and Updating Procedures

The period of crisis has unfortunately opened the door to many new types of hackers, scammers and phishers. These tricksters may try to target staff via email, social media ads or over the phone. The scammers may try to mimic other staff, (including the Principal/Partners), client of the firm or professional organisations including your bank in order to trick a staff member into giving away sensitive information or transfer funds. All staff should be extra vigilant at this time and should always ask for additional proof if they are suspicious of have any doubts about the enquirer.

All employees in accounting and payment functions and anyone who has authority to transfer money, must be made aware of ‘*fake president*’, ‘*social engineering’* frauds and general cybersecurity frauds and regular and relevant training to avoid falling victim to these frauds must take place. Records of such training must be maintained. In addition to cybersecurity training all employees in accounting and payment functions and anyone who has authority to transfer money on behalf of the firm will receive suitable training on this policy every 6 months and a record of the date and each employee in attendance will be kept. Where the firm enters into a new cyber insurance policy training will take place within 60 days of the continuity date.

Telephone call reception desks must be warned about the dangers of providing names and contact details of finance department staff and partners to callers ‘phishing’ for information. Relevant training in this area should be provided.

All internal controls and procedures surrounding bank account controls, funds transfer and any other function where money transfer can take place must be reviewed regularly to ensure that they are still appropriate and effective vis a vis ‘*fake president’* and ‘*social engineering’* fraud.

The LQSI monthly updates (in the member’s area) provides details of current cyber threats against law firms. These should be circulated to all relevant personnel.

Note: As part of the National Payments Plan, Government Departments/Offices, Local Authorities and State Agencies will no longer use cheques in their dealings with businesses. This is to encourage Small and Medium Sized Enterprises to migrate from cheque usage to electronic payment methods. A shift to electronic as a preferred method of payment will result in reduced costs and improved cash-flow for the overall business sector.

As part of best practice standards firms are encouraged to use electronic banking in the legal transaction as much as possible i.e. in conveyancing, litigation etc. It should reduce the time it takes to complete transactions which would increase client satisfaction and profitability for the firm. Appropriate safeguards must always be followed.

Signed:

Date:

Date of next review: