Queenstown Bank of Maryland
Business E-Sure Banking Agreement

These are the terms of your Agreement with Queenstown Bank for accessing your accounts and making use of other services via the Internet through Queenstown Bank. Whenever you use Internet Banking, or authorize others to use it, you agree to these terms. Queenstown Bank may amend these terms from time to time. You will be notified of any amendments that affect your rights or obligations within the appropriate time period. Each of your accounts at Queenstown Bank, which are accessed by Internet Banking continue to be governed by the applicable Account Disclosures and Regulations Relating to Deposit Accounts and Other Services and Electronic Fund Transfer Agreement and Disclosures, otherwise known as Disclosures and Regulations, and the applicable Schedule of Fees, as they may be amended from time to time.

GENERAL INFORMATION

1. **Definition of Terms**
   - "You", “User” and "Your" means any person who applies for Internet Banking with Queenstown Bank through completion of the Queenstown Bank Internet Banking Application and all persons authorized by the applicant to use their Internet Banking Identification and PIN (Personal ID Number) or other means of access we establish or approve.
   - "We," "Us," "Our," "Bank," and "QBM" refer to the Queenstown Bank or one of its affiliates.
   - "Business Day" shall mean Monday-Friday, except for federal banking holidays.
   - "Internet Banking Agreement" means the Queenstown Bank Business E-Sure Internet Banking Agreement.
   - "Internet Banking" or "The Service" "or "Business E-Sure Banking" means our service that allows you to make payments, transfer funds, access accounts, make purchases, obtain information, and perform other transactions via the Internet by use of a personal computer and modem and/or other means we authorize or allow.
   - “Security Codes,” refers to any combination of a “Users” Access ID and Password

2. General Description of Available Services

Account access via Queenstown Bank's Internet Banking Service allows you to:

- View account balances and transaction history for up to 90 days on accounts
- Transfer funds between QBM accounts
- Set up recurring transfers between QBM accounts
- Make loan payments on your QBM loan accounts
- Download account transactions to your third party accounting software
- Add or review stop payments orders on accounts
- View images of paid checks and processed deposit transactions on accounts
- Administrative features include adding, modifying, and deleting users for online banking access

3. Requirements for Your Use

To access your accounts through Business E-Sure Banking, you must have a Queenstown Bank account and complete the Business E-Sure Banking Enrollment process. In addition, you will need a personal computer and an Internet browser that supports 128-bit data encryption. You will need Internet access through the service provider of your choice (ISP). Business E-Sure Banking is viewed best with Microsoft Internet Explorer versions 7 or higher. Other browsers may work, but the display and printing

of pages may not be ideal. You need access to a printer and/or other storage medium, such as a hard drive for downloading information or printing disclosures. An external email address is required for the delivery of electronic notices and disclosures. Prior to enrolling in the service and accepting the electronic version of this agreement you should verify that you have the required hardware and software necessary to access Business E-Sure Banking and retain a copy of this agreement. If we revise hardware and software requirements that may impact your ability to access Business E-Sure Banking, we will give you advanced notice of these changes and give you an opportunity to cancel and/or change your method of receiving electronic disclosures (e.g. change to paper format vs. electronic format) without the imposition of any fees.

You are responsible for the installation, maintenance and operation of your computer and your browser software. The risk of error, failure, or non-performance is your risk and includes the risk that you do not operate your computer or your software properly. The Bank is not responsible for any errors or failures from any malfunction of your computer or your software. Queenstown Bank is not responsible for any electronic viruses that you may encounter. The Bank is not responsible for any computer virus-related problems that may be associated with the use of Business E-Sure Banking. The Bank has no liability to you for any damage or other loss, direct or consequential, which you may suffer or incur by reason of your use of your computer or your software.

4. Enrollment Process

Business customers interested in the commercial features of the Service should contact our Electronic Banking Department directly at (410) 827-8881 or visit one of our eight conveniently located branches and speak to a Branch Manager. Queenstown Bank will provide you with an application for Business E-Sure Banking. Upon receipt of the application our Electronic Banking Department will verify the information provided for accuracy and proper authorizations.

If eligible for Business E-Sure Banking, we will assign your Access ID and temporary password, which you will use for your first login. You will then be prompted to build a new password for your Access ID, which must be a minimum of 8 characters including at least 2 numbers and 1 special character. You will also be prompted to answer 3 security challenge questions/answers that will assist with authenticating your identity. You will also be assigned a PassMark™ image, to which you will assign a pass phrase. Your Access ID cannot be modified once established and you will be prompted every 60 days to change your password.

If you apply to originate ACH transactions, we will conduct a risk assessment to determine eligibility. If approved, a separate ACH origination agreement and additional security requirements for system access will be required.

5. Linked Accounts

When you first enroll for the Business E-Sure Banking, we will link the approved business accounts that were provided to us in writing during the application process. Additional accounts may be requested in writing after initial login.

6. Account Balances

Balances shown in your accounts may include deposits subject to verification by us. The balance reflected may differ from your records due to deposits in progress, checks outstanding, or other withdrawals, payments or charges. A transfer request may not result in immediate availability because of the time required to process the request. A transfer request must be made before the Business Day cut-off time to be effective the same Business Day.

The balances are updated in real-time and will display the available balance. There may be situations that cause a delay in an update of your balances. Business E-Sure Banking will use the memo available balance at the time of a transaction to base our approval for account transfers.

7. Hours of Accessibility

You can access your accounts through Business E-Sure Banking seven days a week, 24 hours a day. However, at certain times, Business E-Sure Banking may not be available due to routine system maintenance.

8. Fees, Changes to Fees, or Other Terms

There are no monthly or transaction fees for accessing your account(s) through Business E-Sure Banking for users.

Queenstown Bank reserves the right to change the charges, fees or other terms described in this Business E-Sure Banking Agreement. When changes are made to any fees, charges, or other material terms, we will update this Business E-Sure Banking Agreement and notify you accordingly. Notification will be given at least thirty (30) days in advance of the effective date of any additional fees for online transactions, or of any stricter limits on the type, amount or frequency of transactions or any increase in your responsibility for unauthorized transactions, unless an immediate change is necessary to maintain the security of the system. If such a change is made, and it can be disclosed without jeopardizing the security of the system, we will provide notice to you within thirty (30) days after the change. We reserve the option, in our business judgment, to waive, reduce or reverse charges or fees in individual situations. Changes to fees applicable to specific accounts are governed by the applicable Depositor Terms and Conditions and the deposit account information.

If approved to originate ACH’s, please see the ACH Agreement for any applicable fees.

9. Transfers

Through Business E-Sure Banking you are allowed to make transfers between your assigned Queenstown Bank accounts. You may also make payments to your Queenstown Bank loan accounts. We reserve the right to deny transfers between certain types or accounts under certain circumstances.

A transfer initiated through Business E-Sure Banking before 6:00 p.m. (Eastern Standard Time) on a business day is posted to your account the same day. All transfers completed after 6:00 p.m. (Eastern Standard Time) on a business day or on a Saturday, Sunday or banking holiday, will be posted on the next business day, however, may be available for your use sooner. Our business days are Monday through Friday, except for banking holidays. "Banking holidays" shall mean all federal banking holidays.

The number of transfers from accounts may be limited as described in the applicable portions of the deposit account information. Each payment or transfer through Business E-Sure Banking from a savings or money market account is counted as one of the six limited transfers permitted each statement period, as described in the Disclosure and Regulations.

If a hold has been placed on deposits made to an account from which you wish to transfer funds, you cannot transfer the portion of the funds held until the hold expires.

You cannot cancel a transfer after it has been entered into the system and the information has been processed and/or transmitted to us.

11. Signature Requirements

When any transfer or other payment instruction is initiated through the Service for your benefit, you agree that we may debit the designated accounts without requiring your signature on the item and without any notice to you. Accounts that have entered into a 'two signatures required' arrangement with Queenstown Bank of Maryland shall be prohibited from enrolling in Business E-Sure Banking.

12. Internet Security

Business E-Sure Banking may utilize a comprehensive security strategies known as multifactor authentication to protect your accounts and transactions conducted over the Internet.

Access IDs and Passwords - One of the main security features protecting Business E-Sure Banking is the unique combination of your Access Identification Code (Access ID), and confidential password.

Because your Password is used to access your accounts, you should treat it as you would any other sensitive personal data.

- You should carefully select a Password that is hard to guess.
- Keep your Password safe.
- Memorize your Password and do NOT write it down.
- You will be required to change your Password every 60 days.
- Your Password should be changed immediately if you suspect that it has been compromised. This can be done at any time from the "Account Services" menu after you log on to Business E-Sure Banking.

Neither this Institution nor its Service Providers will contact you via telephone or email requesting personal information, your Access ID, or your Password. If you are contacted by anyone requesting this information, please contact us immediately.

User Authentication – Your computer is registered with unique identifiers using secure cookies and Adobe® Flash® shared objects to identify your computer and your IP address, and other information to verify your identity. This prevents criminals from logging into your account even if they possess your unique Access ID and password.

Mutual Authentication – Not only must you prove your identity to our website, but our website must prove its identity to you. To do that, a secret image is assigned and a phrase is chosen during your first time login. When you see your secret information during login, you instantly know that you are at the Business E-Sure Banking website.

Encryption – Business E-Sure Banking uses the Secure Socket Layer (SSL) encryption technology for everything you do while using Internet banking. Your browser automatically activates this technology when it attempts to connect to our Service. The Service requires a browser that supports 128-bit encryption. The Service will warn you if your browser does not meet this requirement.

Whenever SSL is securing your communications, the browser will typically indicate this *secure session* by changing the appearance of a small icon of a padlock at the bottom of the screen from "open" to "locked". What this means to you is that your communications are scrambled from your browser to our servers at all times so no unauthorized party can read the information as it is carried over the Internet.

Cookies - During your use of Business E-Sure Banking, our Internet banking Service Provider will pass an encrypted *cookie* to your computer in order to identify your computer during the session. The encrypted cookie registers your computer with Business E-Sure Banking and your computer will be recognized during future logins. This cookie enables us to process multiple transactions during the

session without having to provide an Access ID and Password for each individual transaction. This cookie does not contain any personal information; it simply provides another level of security for our Internet banking product. The cookie is stored on your computer's hard-drive, identifying your computer while you are logged on. When you log off, close your browser, or turn off your machine, the cookie will be destroyed. A new cookie is used for each session; thus, no one can use the prior cookie to access your account.

Additional Security Guidelines:

- All Authorized Users should sign-off after every session; however, online sessions will automatically end after fifteen (15) minutes of inactivity. This is to protect you in case you accidentally leave your computer unattended after you log-in.
- The security of public computers (e.g. in a library, or Internet café) cannot be assured; therefore we recommend that you refrain from accessing the Service on a public computer.
- Routinely scan your computer, servers, and electronic media using reliable virus detection and anti-spyware products. Undetected or un-repaired viruses or spyware may affect the performance of your computer, corrupt and destroy your programs, files, and even your hardware. Additionally, you may unintentionally transmit sensitive data to another third party or transmit a virus to other computers.
- Use a firewall product (hardware and/or software), especially if you have a broadband Internet connection such as DSL or cable modem.
- Keep your computer's operating system and browser fully patched for critical security issues. We recommend use of the most current, fully patched, versions of Internet browsers for accessing Business E-Sure Banking.

13. Your Password Responsibilities

When you accept the terms and conditions of this Agreement, you agree not to give or make available your password or other means to access your account to any unauthorized individuals. You are responsible for all transfers you authorize using Business E-Sure Banking. If you permit other persons to use Business E-Sure Banking, your password, or other means to access your account, you are responsible for any transactions they authorize.

If you believe that your password or other means to access your account has been lost or stolen or that someone may attempt to use the Service without your consent or has transferred money without your permission, you must notify us at once by calling (410) 827-8881 during customer service hours.

If you or your Authorized users disclose your Password to anyone, and/or if you allow someone to use your Password to access your accounts, you are authorizing them to act on your behalf and you will be responsible for any use of the Service by them (e.g., such as when you provide this information to a joint account holder, an employee, and/or an aggregation service provider).

In addition to the security features described above, there may be other security related notices posted on our website or Business E-Sure Banking from time-to-time. It is your responsibility to read all security notices.

ROLES AND RESPONSIBILITES

<u>Senior Administrators</u>

The Senior Administrator must be authorized to conduct business with us, included as part of your account opening documents or otherwise authorized (or deemed authorized) to act on your behalf, whether under this Agreement or any other agreement with us. You will be required to designate at least

one Senior Administrator. You (through the Senior Administrator) then control the Funds Management Services, through the systems available at our website. Your Senior Administrator may establish other users (including Supervisor, Administrator and Corporate employees, collectively with any Senior Administrator, the "Users"). You are responsible for any and all Users to maintain the confidentiality of his or her password or login identification and other Security Codes.

The Senior Administrator(s) will be responsible for maintaining your Service settings and User security. Access to your account(s) through the Service will be based upon the identification of Users and authority levels specified by you in your Enrollment Form. You must notify us if you terminate or wish to change the Senior Administrator. You must also notify us if you add or delete accounts or functionalities.

Senior Administrator responsibilities may include:

- Add, modify, and delete users associated with the client.
- Assign the security level to the user.
- Establish roles for the user (Administrator, supervisor, corporate employee)
- Establish ability to inquire or add stop payments for the client.
- Choose the electronic documents the user will have access to view. (DDA Credits/DDA Debits)
- Establish which transfer templates the user will be assigned.
- Give access to the user for ACH manager, if applicable
- Add, modify and delete transfer templates
- Add or modify the display groups and nicknames assigned to each account

The Senior Administrator is responsible for setting up your Users. The Senior Administrator is also responsible for assigning all Supervisors, employees, or other persons with the Security Codes that are necessary to access Services and for establishing what, if any, limitations will apply (including what level of activity is appropriate for each Account). The Senior Administrator changes and maintains your Security Codes.

We will not control or oversee the Senior Administrator function or the activity of Users. You agree to the creation of a Senior Administrator and to all action taken by the Senior Administrator, by any User, and by any person given access to one or more Services by the Senior Administrator or by a User, and all such persons that are your agents for purposes of use of the Services. You further agree to assume all risks associated with providing Security Codes to your Senior Administrator, understanding that this can result in Users and possibly other persons obtaining access to your Account without control or monitoring by us. You must establish authorization parameters and/or limits for each person you authorize to use the Service. You agree to use and implement each control (including template management, verification, access, use of maximum process settings, security, audit and review procedures) to prevent unauthorized persons gaining access to Security Codes or your Accounts.

Supervisors, Administrators and Corporate Employees:

Supervisors, Administrators, and Corporate Employees are granted access to E-Sure Banking functions at the discretion of you and your assigned Security Administrator.

If the approval process is required for various functions it would require authorization from a senior security level.

ACH ORIGINATION

If you are approved to originate ACH entries, you will be required to sign Queenstown Bank's ACH Origination Agreement which outlines ACH rules and responsibilities as mandated by the National Automated Clearing House Association (NACHA).

Each user authorized to submit ACH entries will be issued a Go3 Token for added security. This token generates a one-time password that is used each time an ACH file is submitted. This password is unique to your account and changes frequently for your protection.

One token will be issues per user at no charge. In the event a token becomes damaged or lost, a replacement token will be issued for a $25.00 fee.

ADDITIONAL PROVISIONS

1. Bank Liability

We will use commercially reasonable efforts to make all your transfers properly. However, we shall incur no liability if we are unable to complete any transactions initiated by you because of the existence of any one or more of the following circumstances:

- If, through no fault of ours, your Eligible Account(s) and/or Payment Account does not contain sufficient funds to complete the transaction or the transaction would exceed the credit limit of your overdraft account (if applicable);
- Business E-Sure Banking is not working properly and you know or have been advised by this Institution and/or its Service Providers about the malfunction before you execute the transaction;
- If your computer, software, telecommunication lines were not working properly and this problem should have been apparent to you when you attempted the transfer
- The transaction request involves funds subject to hold, dispute, restriction, or legal process we believe prevents their withdrawal;
- We have reason to believe that a transaction request may not be authorized by you or any third party whose authorization we believe is necessary; and/or
- Circumstances beyond control of the Service, our Service Providers, and this Institution (such as, but not limited to, fire, flood, or interference from an outside force) prevent the proper execution of the transaction and we have taken reasonable precautions to avoid those circumstances.

2. Electronic Disclosures

We may deliver amendments to this Agreement and other disclosures to you in an electronic format. Other disclosures may include: monthly account statements, deposit account disclosures, notices regarding changes in account terms and fees, and privacy notices. The equipment necessary for accessing these types of disclosures electronically is described within this Agreement in Section 3.

With your acceptance below, you agree to accept this agreement and other Internet Banking related disclosures in an electronic format. You also agree and represent that you have the necessary equipment for accessing the Service and for viewing electronic disclosures.

You may change the method of delivery at any time (e.g., from electronic format to paper format) of any of the aforementioned disclosures, statements or notices, by contacting us at the below listed address or by stopping into any Queenstown Bank of Maryland branch location.

Queenstown Bank of Maryland
Electronic Banking Department
PO Box 120
Queenstown, MD 21658-0120
(410)827-8881

You should print or save a copy of all disclosures delivered electronically.

3. Address, E-mail, or Payment Account Changes

When you enroll in Business E-Sure Banking, we may send you a "Welcome" e-mail. We will also send you e-mails and/or secure messages through Business E-Sure Banking regarding important Internet Banking matters and/or changes to this Agreement. You must provide us your current e-mail address in order for us to deliver this information to you.

It is your sole responsibility to ensure that your contact information is current and accurate. This includes, but is not limited to, name, address, phone numbers, and e-mail addresses. Changes to your email address can be made within Business E-Sure Banking in the "Options" menu or by contacting our Electronic Banking Department at (410) 827-8881. Other changes to your account must be made in person at any Queenstown Bank of Maryland location.

4. Service Termination, Cancellation, or Suspension

In the event you wish to cancel the Service, please contact our Electronic Banking Department at (410) 827-8881.

We may terminate or suspend the Service to you at any time. Neither termination nor suspension shall affect your liability or obligations under this Agreement.

Access to Business E-Sure Banking may be canceled in whole or part without prior notice due to insufficient funds in one of your accounts or other circumstances that may create an unanticipated liability to us. If your account(s) is closed or restricted for any reason, or if there has not been any Internet Banking activity for a period of 6 consecutive months, accessibility may automatically terminate.

After termination or suspension of Business E-Sure Banking, we may consider reinstatement once sufficient funds are available in your accounts to cover any fees and other pending transfers or debits. In order to request reinstatement of the Service, you must call our Electronic Banking Department at (410) 827-8881.

5. Governing Law and Relation to Other Agreements

Accounts and services provided by this Financial Institution may also be governed by separate agreements with you. This Agreement supplements any other agreement(s) and/or disclosures related to your Account(s) and provided to you separately.

This Agreement shall be governed by and construed in accordance with federal laws and the laws of the State of Maryland.