Schoellerbank
Private Banking

Terms and Conditions for the Use of Electronic Banking

1. Object of the Agreement

This Agreement governs the use of the Schoellerbank Electronic Banking system, a service of Schoellerbank Aktiengesellschaft (referred to as “Schoellerbank” in the following) which enables the customer to communicate with our data processing centre through a data transmission line using the Internet and to conduct banking transactions or retrieve information via this connection after electronic authorisation. Schoellerbank Electronic Banking comprises Schoellerbank Online Banking (online account, online securites account), Schoellerbank Business Banking, and Multi Bank Standard Service (MBS Service). A version of Online Banking optimised for mobile devices (e.g. smartphones and tablets) can also be used to access Online Banking.

The extent to which the customer may use Electronic Banking services is based on the Electronic Banking Agreement concluded and does not automatically cover the entire range of present or future services offered by Schoellerbank. Electronic Banking is a product offered in addition to the account/ securities account maintenance agreement and is therefore subject to the terms of the account/ securities account maintenance agreement. Electronic Banking enables the customer to execute specific transactions and use specific services through electronic communication, as an alternative to traditional methods.

Depending on the requested product, the “Application for the Use of Online Banking and the Online Execution of Securities Orders”, the “Application for the Use of Online Banking including Portfolio Analysis and the Online Execution of Securities Orders”, the “Application for the Use of Schoellerbank Business Banking”, or the “Application for the Use of the Electronic Banking Service of Schoellerbank Aktiengesellschaft – Multi Bank Standard Service” shall be concluded between the customer and Schoellerbank for an indefinite term, on the basis of which the customer shall be entitled to use Online Banking, Schoellerbank Business Banking, or MBS Service.

The rules governing single and joint signing authority for the account as specified in the signature specimen sheet are also binding for transactions conducted via Electronic Banking. In the case of joint (collective) signing authority, certain functions of Electronic Banking (e.g. eps online transfers) cannot be used. The account holder is required to issue his/her written consent before an authorised signatory is granted an Electronic Banking authorisation. Each account/securities account holder can revoke this consent at any time. The user may also revoke his/her own authorisation at any time by giving written notice to us. For joint accounts, all account holders are required to issue their written consent before an Electronic Banking authorisation is granted to another account holder or authorised signatory.

2. Instructions for use and security notices

Although the Schoellerbank Electronic Banking system is simple, user friendly, and secure against manipulation in accordance with the current technological standards, the customer agrees to familiarise him/herself with the instructions for use and security notices prior to his/her first transaction. The instructions for use and security notices can be accessed and printed by the customer at any time either through the “Help” section in the Schoellerbank Electronic Banking system or on Schoellerbank's web site. They describe the currently available functions, and the currently amended version constitutes an integral part of this Agreement.

3. Access to Schoellerbank Electronic Banking

Authorisation to use the system is granted through the assignment of the following personal identifiers:

- User number
- User name
- Password (PIN = personal identification number)
- Transaction number (TAN)

The customer may decide wheter he/she wants to use mobileTAN, tresorTAN, or cardTAN for Electronic Banking.

Any provisions that make reference to TAN in these Terms and Conditions for the Use of Electronic Banking shall apply to mobileTAN, tresorTAN, and cardTAN, unless otherwise indicated.

If the customer uses a digital signature, transactions are signed using an authorisation card and the associated authorisation details as opposed to entering a TAN.

User number (user identification)
Every customer receives a user number from Schoellerbank by post, which enables Schoellerbank to assign a customer to the accounts which he is authorised to access via Electronic Banking. It consists of a multi-digit code that is generated by the system when it is issued. The user number may not be changed by the customer.

User name
The user name is an additional security feature during login. The system automatically prompts the user to define a freely selectable user name the first time he/she logs in. Each time the customer logs in after that, he/she must identify him/herself by means of this freely definable user name. The user name can be changed at any time and with immediate effect in Online Banking using a TAN.

Password (PIN/personal identification number)
The password serves to verify the customer's identity in the Electronic Banking system and must be entered before the customer can submit orders and access information through the Electronic Banking system. The PIN is a 16-digit alphanumeric code which is either handed to the customer personally in a sealed envelope or sent by post. This initial PIN must be changed by the customer the first time he/she logs into the selected Electronic Banking product. Each time the customer logs in after that, he/she must identify him/herself by means of this newly defined PIN. The PIN can be changed at any time and with immediate effect in the selected Electronic Banking product using a TAN. The customer can request a new initial PIN by contacting his/her relationship manager by phone.

Fingerprint/Touch ID
The fingerprint/Touch ID is a personal identifier for the customer that allows the customer's identity to be verified in the Online Banking app using a fingerprint and must be activated by the customer in the Online Banking app. The fingerprint/Touch ID method is an alternative to verifying the customer's identity using the user number, user name, and PIN.
In order to use the fingerprint/Touch ID method, the customer must have a mobile device (e.g. smartphone, tablet) that supports fingerprint/Touch ID.

short PIN
The service can also be accessed on mobile devices using simplified authentication (device integration combined with a user-specific four-digit PIN code). Under this access method, the functions available are limited to a read-only authorisation (transactions cannot be executed).

Transaction number (= TAN)
Along with the personal identifiers, the customer also needs transaction numbers to execute transactions and to submit other legally binding declarations of intent to Schoellerbank via the Electronic Banking system. A TAN serves to replace the signature, and when a customer uses Electronic Banking services he/she must enter the transaction number in the designated field in order to sign the relevant transaction or legally binding declaration of intent with binding effect.

- mobileTAN
  If the customer decides to use the mobileTAN method, the mobileTAN required to sign a transaction

in the Electronic Banking system will be sent to his/her mobile phone via SMS (Short Message Service) following his/her request.

The customer must provide the telephone number to which the mobileTANs are to be sent when signing up for this method. The customer can change the provided mobile phone number by making a request to the relationship manager in person or directly in the Electronic Banking system provided that an SMS containing the mobileTAN required to sign this change can be sent to the number previously on file with Schoellerbank.

The SMS with the mobileTAN also includes information on the transaction to be completed (the payee's IBAN and amount or a reference code [electronic note] and control value [total amount of all orders]) for verification purposes. A mobileTAN may only be used to sign the transaction for which it was requested and is valid for a maximum of 30 days after it is issued. If a transfer order is changed after a mobileTAN is issued for it, the previously issued mobileTAN is no longer valid. A new mobileTAN must be requested. A mobileTAN is rendered invalid once it is used.

The customer must note that an SMS with a mobileTAN can only be received on his/her mobile phone when the basic requirements for the receipt of SMS messages are met, for example the phone must be capable of receiving SMS messages, the service contract with the mobile communications provider must include the receipt of SMS messages, and the customer must be in an area in which his/her mobile communications provider delivers SMS messages.

- tresorTAN
  The transaction numbers required for the authorisation of orders are sent to the Tresor app provided by Schoellerbank. The app must be installed on the customer's mobile device and the device integration process completed beforehand. Authentication occurs via device integration and the customer's access data (user number, user name, and personal identification number). Access is also possible using simplified authentication (device integration combined with a four-digit PIN code [shortPIN] and fingerprint/Touch ID). The customer can change the device integration and his/her shortPIN in Online Banking at any time. Note: The tresorTAN method can only be used with an Internet connection.

  For verification purposes, the message containing the TAN also includes information about the orders to be completed. In the case of transfer orders, the payee's IBAN and the transfer amount or a reference code (electronic note) and control value (total amount of all orders) are included. The customer is required to check that this information matches the submitted order. The tresorTAN may only be entered if the information is correct.

  A tresorTAN is only valid for the execution of the transaction for which it was requested and becomes invalid as soon as it has been used.

- cardTAN
  When using the cardTAN method, the TAN required for the authorisation of transactions in the Electronic Banking system is generated by a special program saved on the chip of a bank card (TANcard). In order to use the cardTAN method, the customer must have an active bank card that supports the cardTAN function (a Maestro debit card issued by Schoellerbank with the cardTAN logo on the back) and a special card reader (cardTAN generator). In addition, Schoellerbank must activate the cardTAN method for the customer.

  After entering the order data, the customer chooses the cardTAN authorisation method. Then the bank card (TANcard) is inserted in the cardTAN generator and activated using the EB-PIN generated specifically for this purpose. The customer receives the EB-PIN from Schoellerbank during the activation of the cardTAN method. The customer can change the EB-PIN directly in Electronic Banking. Next, certain data about the submitted transaction are transmitted either via an optical interface ("flicker") or by being manually entered on the cardTAN generator, the data are processed in the card chip, and a TAN for authorising the order is generated. This cardTAN must be entered by the customer and then the order is sent to Schoellerbank.

When using the "flicker method", the data required for the generation of the cardTAN are transmitted from the bank server to the customer's monitor in the form of a flickering black and white graphic, which is sent to the cardTAN generator via optical interfaces. The transmitted transaction data are shown on the display of the cardTAN generator for verification by the customer. The customer is required to compare the order data generated on the cardTAN generator with the orders entered in Electronic Banking and may only use the cardTAN if the transaction data match.

A cardTAN is only valid for the execution of the orders for which it was requested. If an order is changed after a cardTAN has been generated for it, the cardTAN becomes invalid and must be regenerated by the cardTAN generator. A cardTAN also becomes invalid as soon as it is used.

Digital signature
Transactions are signed using a digital signature card (e.g. citizen's card function on an e-card, a.sign premium). In order to use this method, the customer must have a local citizen's card system (or equivalent software) including a compatible card reader. For verification purposes, the information about the orders to be completed is also displayed. In the case of transfer orders, the payee's IBAN and the transfer amount or a reference code and control value (total amount of all orders) are included. The customer is required to check that this information matches the submitted order. The signature PIN may only be entered if the information is correct.

4. Use of services

The use of Schoellerbank Electronic Banking services that are secured by a TAN or the use of a digital signature authorises Schoellerbank to execute orders issued in the course of this business relationship for the customer's account.

However, the customer acknowledges that services that do not involve the execution of transactions on his/her accounts or securities accounts, such as checking the account balance and securities account valuations, can be accessed without a TAN or digital signature. Therefore, it is in his/her best interest to keep all personal identifiers strictly confidential.

The Schoellerbank Electronic Banking system is available to customers from 0:00 to 24:00 every day. Maintenance work may be performed on the bank's computers between 0:00 and 06:00, which may limit the use of the Electronic Banking system. If maintenance work has to be performed between 06:00 and 24:00, Schoellerbank will inform customers in advance if possible.

5. Identification

The customer's authorisation to conduct banking transactions via Electronic Banking is always verified exclusively on the basis of his/her personal identifiers.

6. Transactions via Electronic Banking

The customer submits orders to Schoellerbank by sending data in formats defined by Schoellerbank. Incorrect or incomplete data will not be processed or only processed in part by Schoellerbank's data processing centre. For each order (e.g. transfer order, creation of a standing order, securities order), the customer must log into the Schoellerbank Electronic Banking system with the relevant personal identifiers, enter the data required for the desired transaction, and sign the order with a valid TAN.

If the customer uses a digital signature, transactions are signed using an authorisation card and the associated authorisation details (signature PIN) as opposed to entering a TAN.
The time of receipt is the time at which a transaction order is received by Schoellerbank via Electronic Banking. If a transaction is received on a day on which Schoellerbank is not open for business, the transaction will be treated as if it had been submitted on the next business day.
Orders are generally executed on the same day if the information is available for processing by Schoellerbank at the latest at the specified deadline towards the end of a business day for the given order type, which is posted in the teller rooms of Schoellerbank. If an order is submitted after this deadline, it cannot be executed until the next bank business day. In any case, the customer must indicate the execution date for payments that are to be executed in the future.

Any response by Schoellerbank after its receipt of orders only confirms the receipt of the data transmitted but not the execution of the orders that have been submitted. Every order is processed in the course of the bank's ordinary business.

Electronic transfer orders placed in the Electronic Banking system authorise us to debit the accounts in accordance with the application form and in line with the balance or the overdraft facility. Schoellerbank is not obligated to execute orders if the account does not have a sufficient balance or overdraft facility, but it may execute orders issued via Electronic Banking and debit the account in line with its General Terms and Conditions even if there are not sufficient funds in the account.
The customer can specify whether the order should be completed during the next possible internal processing run, or at a future point in time (forward order). If the desired execution date for a forward order is not a business day at Schoellerbank, the order will be treated as if it had been received on the following bank business day. The customer can also combine multiple transfer orders and sign them with a single TAN.

An authorised transfer order cannot be cancelled once it has been received by Schoellerbank via Electronic Banking. A forward order can be cancelled up until the end of the business day before the agreed execution date directly in the Electronic Banking system using a valid TAN.

Schoellerbank is authorised to execute transactions submitted in the name of a customer not considered a consumer for the purposes of Section 3 item 11 Payment Services Act (Zahlungsdienstegesetz) (hereinafter: entrepreneur) through Electronic Banking using the personal identifiers for the accounts of this customer when the bank, applying a reasonable level of prudence, has no reason to believe that these orders were not submitted properly in the name of the respective customer and when the submission of the improper orders cannot be attributed to Schoellerbank.

The Schoellerbank Electronic Banking system does not distinguish between the account holder and other legitimised users. Therefore, the holder(s) of the account/securities account explicitly accept(s) liability for any overdraft caused by other legitimised users and for any damages caused through their improper conduct.

If a user has single signing authority for an account, he/she also has sole authority to conduct transactions for this account via Electronic Banking. If he/she has collective signing authority, he/she may only conduct transactions via Electronic Banking together with another authorised person.

An order that has been been signed by only one user with collective signing authority using his/her TAN will be irrevocably cancelled in the system without being executed and without further account information being provided by Schoellerbank if it is not signed by a second user with collective signing authority using his/her TAN within 28 days.

7. eps online transfers

Online Banking can also be used to execute eps online transfers. eps online transfers are a simple, secure, and standardised payment process provided by Austrian banks for online purchases and for the use of e-government services. Under this process, the customer is able to directly log into the online banking service of his/her bank on the web site of the online shop or e-government web site using his/her user number, user name, and PIN and make a payment by way of a transfer order. An eps online transfer is signed in the same way as any other transfer in Online Banking by entering a TAN. The ordering process in the online shop is strictly separated from the payment process in Online Banking. None of the customer’s bank-specific data are disclosed or saved during the eps online transfer process, and no bank-specific data of the purchaser are transmitted to the merchant. When the eps online transfer is signed by the customer, the bank guarantees the execution of the transfer to the online merchant or e-government authority, so that the customer cannot cancel this eps online transfer. The eps online transfer process is merely a tool that the customer can use to make an online payment by way of a transfer order in Online Banking. The contractual relationship between the customer and the merchant is not affected by the use of the eps online transfer process, and therefore no objections relating to the underlying transaction may be raised against Schoellerbank.

8. App

Schoellerbank can provide apps for the use of electronic services on selected devices. Such apps must be installed separately by the user via the app store for the given device. The terms and instructions for the app provided in the app store must be taken into account during installation.

Various parameters, such as the device model and operating system version, determine whether an app can be used on a certain device. In light of the multitude of devices available on the market and the changes to these devices due to technical progress, Schoellerbank cannot guarantee that an app will (permanently) function on a given device. In addition, Schoellerbank cannot provide support during the installation or deinstallation of apps on a specific device.

Apps provided by Schoellerbank can enable the user to take advantage of a simplified login using the shortPIN (device integration combined with a user-specific four-digit PIN code). After logging in with the shortPIN, the user is only offered limited functions in the app. In particular, the functionality is limited to read-only access to data. Before signing orders, the user must be fully authenticated with his/her access credentials. In order to use the shortPIN, the user must perform a device integration process on the device after the app is installed. The device integration can be managed by the user via the associated electronic service. Specifically, this allows the device integration to be revoked.

In addition to the shortPIN, some devices support the use of biometric processes, such as a fingerprint/ Touch ID. The use of these biometric processes serves the same purpose and leads to the same result as entering a shortPIN. Schoellerbank has no influence over the security and reliability of the biometric process on a device.

The user should only complete the device integration process and use the shortPIN or biometric process on his/her own devices. The user is responsible for ensuring that only his/her own biometric data are stored on the device. If the user hands over possession of a device on which a Schoellerbank app has been installed – particularly by selling it or giving it away – the user should revoke the device integration and delete all apps and data connected with the electronic services from the device, for example by resetting the device to the factory settings according to the manufacturer’s instructions.

Schoellerbank apps can use push notifications if this is supported by the user’s device and the electronic service and if the user has activated this feature in the electronic service and on his/her device. Push notifications can be used to notify the user of new messages in the app even when the app is not active in the foreground. Because the delivery of push notifications is dependent upon numerous factors that cannot be influenced by Schoellerbank, push notifications merely serve as a supplement to the messages within the app and do not represent a guaranteed communication channel for Schoellerbank.

9. Electronic securities orders

Electronic securities orders placed in Online Banking authorise Schoellerbank to debit the user’s accounts in accordance with the “Application for the Use of Online Banking and the Online Execution of Securities Orders” or the “Application for the Use of Online Banking including Portfolio Analysis and the Online Execution of Securities Orders” in line with the account balance or the overdraft facility. Schoellerbank has the right not to execute securities orders without adequate cover.

Schoellerbank notes that when the customer submits electronic securities orders, the bank shall only act as the intermediary and custodian bank and that the orders submitted by the customer shall only be reviewed to determine whether the requested products are appropriate for the customer based on the information provided regarding his/her knowledge and experience in the investment field. However, no review shall be conducted with regards to the customer’s investment objectives and financial risk capacity for such electronic securities orders. If the electronic securities order placed by the customer without prior consultation does not correspond to his/her knowledge and experience in the investment field, Schoellerbank shall be entitled not to execute it.

Orders may only be issued via Online Banking for certain securities selected by Schoellerbank. Schoellerbank reserves the right to change the selection of securities that are available. The customer can obtain information about the securities that are available for placing orders via Online Banking from his/her advisor.

Securities orders placed via Online Banking are forwarded in the same manner as orders placed with the customer's advisor. Therefore, the forwarding method simply depends on the security itself and/or the market for the security. Orders are either forwarded directly to the exchange/contracting party or via the bank's internal systems. Although orders may generally be cancelled, this is only possible if an order has not yet been executed. In order to ensure that orders are not executed twice, the customer must contact his/her advisor to verify whether the cancellation of an order was successful before placing a new order.

10. Due care

Caution: The Electronic Banking system relies on the Internet, which is an open and publicly accessible communication medium. An unauthorised third party could use a customer's personal identifiers to gain access to the Electronic Banking system and complete transactions against the account of the customer. For this reason, customers are strongly advised to exercise particular caution when conducting transactions via Electronic Banking to avoid damages.

With regards to this obligation to exercise due caution, the customer is especially obligated to keep his/ her personal identifiers confidential and not to disclose this information to any other persons. If the customer has reason to believe that other persons have gained knowledge of his/her PIN, he/she must change his/her PIN immediately and notify the Electronic Banking hotline of his/her concerns (see item 13). It is recommended that the customer change his/her PIN regularly. We recommend that the PIN be changed at least every two months.

When using the mobileTAN, cardTAN, or tresorTAN method, the customer must check the order information sent along with the TAN to ensure that it matches the order that he/she wishes to submit and must only use the TAN if the order information matches.

11. Rejection of transfer orders

Schoellerbank may only reject the execution of a transfer order that was submitted by a customer via the Electronic Banking system if

- the customer identifier is incorrect or incomplete; or
- the account does not have the required cover to complete the transfer; or
- the execution of the order would be in violation of bilateral or common market regulations, or of a court or other legal order; or
- Schoellerbank cannot fulfil its duty of due diligence pursuant to Section 6 Financial Markets Anti-Money Laundering Act (Finanzmarkt-Geldwäschegesetz); or
- there is reason to believe that the execution of the order would constitute a criminal act.

Schoellerbank will inform the customer of the rejection of the transfer order as quickly as possible in a form agreed with the customer, including information on how the order can be corrected. The reason for the rejection will only be provided when this is not in violation of bilateral or common market regulations or a court or other legal order.

12. Correction of unauthorised payment transactions

Please refer to item 16 (2) of the General Terms and Conditions of Schoellerbank. If the customer is an entrepreneur, the period defined in this item is reduced from 13 months to 3 months.

13. Blocking

The customer must inform Schoellerbank of the loss, theft, or misuse of his/her personal identifiers (user number, PIN) or any other unauthorised use of the Electronic Banking system immediately as soon as he/she becomes aware of this fact.

Every account holder and authorised signatory can request a block as follows:

- at any time by calling the Electronic Banking hotline at 0800/692265, or from abroad at +43/1/53471-1428, by fax at +43/1/53471-1619, or by e-mail: banking@schoellerbank.at; or
- by informing his/her advisor in person during Schoellerbank's business hours or by sending a letter to any of Schoellerbank's branch offices.

The customer can also block his/her PIN online in the Schoellerbank Electronic Banking system. If an incorrect PIN or TAN is entered four times in a row, the user number will be blocked immediately after the fourth incorrect entry.

In case of the loss or theft of a signature card, or if there is reason to believe that the confidential PIN is no longer secure, the relevant certificate must immediately be revoked with the A-Trust revocation service.

A request to block a user code that is submitted to Schoellerbank during its business hours or at any time via the Electronic Banking hotline becomes effective immediately. Written block requests received by Schoellerbank outside of its business hours will be processed immediately and will take effect by no later than one hour after the next opening time.

Schoellerbank is authorised to block a user number without the customer's involvement if

- there are objective grounds to do so with regards to the security of the personal identifiers or the systems for which they can be used;
- there is reason to believe that unauthorised orders have been submitted using the personal identifiers, or that the personal identifiers have been misused in some other way;
- there is a significant risk that the account holder will not be able to fulfil his/her payment obligations to Schoellerbank arising from the use of his/her personal identifiers.

Schoellerbank will inform the customer of the block and also the reasons (when this is not in violation of bilateral or common market regulations, a court or other legal order, or objective security concerns) in the form agreed with the customer before the block is enacted if possible, or immediately after the block is enacted.

A block may only be lifted by the customer in person or upon his/her express written order - by way of a letter addressed to Schoellerbank that bears the personal or authorised signature of the customer.

14. Information about individual payment transactions (account statements)

Information about individual payment transactions (account statements) is updated by Schoellerbank on a daily basis and made available for the customer to access in PDF format in his/her electronic mailbox. The account statements are deemed delivered when they are accessed by the customer.

The customer is aware that account statements contain important information and may require the customer to make queries, complaints, objections, or statements within a specific period of time. Therefore, the customer will retrieve the information in his/her electronic mailbox on a regular basis, and in any case at least once a month.

The customer will notify Schoellerbank if he/she is unable to access the account statements in his/her electronic mailbox for a longer period of time.

Schoellerbank shall accept no liability for damages incurred by the customer due to the failure to retrieve this information or the delayed or improper retrieval of this information.
In addition, the customer can request to have this information mailed to him/her once a month, subject to the reimbursement of the postage fees.

15. Expiration and termination of the Agreement

When an account is terminated, all Electronic Banking authorisations for the account expire automatically. The Electronic Banking authorisation of an account holder or authorised signatory also expires when he/she is no longer authorised to sign singly on the respective account.

Every customer can terminate the Agreement in writing at any time with a period of notice of one month. Every account holder may revoke the Electronic Banking authorisation of an authorised signatory in writing or in person at any of Schoellerbank's branch offices.

Schoellerbank can terminate the Agreement at any time without justification in writing with a period of notice of two months. In this case, the customer must be informed of the termination in writing or by means of any other agreed permanent data medium.

The Agreement can be terminated immediately without a period of notice by the customer or Schoellerbank for good cause. Good cause shall be deemed to exist if the customer makes his/her personal identifiers available to another person.

16. Liability

a) Liability for electronic payment transfers

If the customer is not a consumer pursuant to Section 3 item 11 Austrian Payment Services Act, he/she shall be liable to fully compensate Schoellerbank for any damages incurred through the misuse of a payment instrument, even in the case of the slightly negligent violation of the obligations and conditions defined in Section 44 (2) 1 and 2 Austrian Payment Services Act.

b) Liability for electronic securities orders

If an electronic securities order is based on the misuse of the customer's personal identifiers, the customer shall be liable for any resulting consequences and disadvantages if he/she facilitated the use of his/her personal identifiers by third parties through his/her own negligence. In such cases, the customer shall be obligated to compensate Schoellerbank for any damages incurred.

17. Permitted use of Electronic Banking

The customer may use the software via a web browser for the purposes defined in this Agreement. He/she may use the Schoellerbank Electronic Banking services for private purposes without limitation. Any reproduction, sale, or any other transfer of the information and services received through Schoellerbank Electronic Banking as well as any commercial use whatsoever is subject to our express written consent. We explicitly note Schoellerbank's copyright with respect to the layout, charts, HTML, and any other page components.

18. Schoellerbank Business Banking (HBP)

These Terms and Conditions govern the acquisition of the single, non-transferrable right to use the “Schoellerbank Business Banking (HBP)” software product as well its use for the accounts/securities accounts managed by Schoellerbank to the extent agreed.

Schoellerbank Business Banking essentially corresponds to the “Multi Bank Standard” (MBS), which allows the customer to manage all Austrian bank accounts that support MBS using a single software product.

The customer is not permitted to copy the Schoellerbank Banking Software and share it with third parties. The creation of a back-up copy to facilitate operational security is excepted from this rule. The ownership of the intellectual property comprising the software and documentation and the associated rights are retained by Schoellerbank. Schoellerbank makes no guarantee for the proper functionality of the software. The installation and use of the software occur at the user’s own risk.

19. Updates and technical modifications / MBS

Schoellerbank may implement updates and modifications in the area of data transmission or to the user interface at any time in line with technical progress and additional security measures. Any software modifications and enhancements will be communicated on a fully automated basis in the communication with Schoellerbank. The customer is obligated to ensure the proper installation of software updates. Schoellerbank may also extend the scope of the features available in Electronic Banking, provided that this does not result in additional costs or obligations for the customer.

In order to use Schoellerbank Business Banking, the customer must ensure that unrestricted data transfer via the URL hob.banking.co.at is not obstructed, for example by a firewall. Ports 3048, 443, and 80 are also required. Technical support will only be provided for the most recent version. Schoellerbank Business Banking supports the MBS standard.

As a cross-sector software solution, Multi Bank Standard Service (MBS Service) makes it possible to access multiple accounts at different banks using a single program.

Customers can also use MBS through the software products of other banks that permit a connection to be established with Schoellerbank’s data processing centre. Depending on how these software products manage user permissions, the user(s) and any parties with read-only authorisation can access data and information pertaining to the registered accounts. The hotline of the bank that provided the main licence for MBS is responsible for responding to customer queries regarding this application.

20. Fees

The applicable fees for the Schoellerbank Electronic Banking service will be communicated separately or by way of the price list. Please refer to items 43–46 of the General Terms and Conditions of Schoellerbank. The customer shall receive the price list and the General Terms and Conditions of Schoellerbank at the same time as these “Terms and Conditions for the Use of Electronic Banking”. If no separate fee is charged for the use of Schoellerbank Electronic Banking at the time the Application for the Use of Schoellerbank Online Banking, Business Banking, or MBS Service is signed, Schoellerbank AG shall be entitled to charge such a fee after providing appropriate notice.

The telephone charges and fees charged to the customer by his/her network provider shall be borne by the customer. This shall not affect the account maintenance fees. The customer authorises Schoellerbank to debit the applicable fees from his/her account.

21. Amendments of the Terms and Conditions

Any amendment of these Terms and Conditions shall become legally binding for all current and future use of Electronic Banking 2 months after the customer is informed of these amendments unless the customer files a written objection to the amendment with Schoellerbank. The customer may be informed by any means agreed with him/her under the business relationship (especially via written notice on an account statement or electronic notice through the Electronic Banking service). Any agreement made with the customer on the delivery of statements and declarations from Schoellerbank also applies to information on amendments of these Terms and Conditions.

When informing the customer of the amendments, Schoellerbank will inform the customer that amendments have been made and that failure to file an objection within 2 months from the date on which he/she was informed of the amendments represents the tacit acceptance of the amendments, and that he/she has the right to terminate the agreement without a period of notice at no charge before the amendments take effect.

In the case of fee changes for consumers, Schoellerbank may make an adjustment in line with the development of the national Consumer Price Index 2000 published by Statistics Austria (increase or decrease), with the amounts being rounded to the nearest whole cent. If, for whatever reason, the fees are not raised in the event of an increase in the index, this does not forfeit the right to increase fees in subsequent years. The customer is entitled to terminate the master agreement immediately at no charge before the amendment goes into effect. The credit institution will also inform customers who are consumers of this right in the notification regarding the amendment.

In the case of changes in fees and services for entrepreneurs, item 43 of the General Terms and Conditions of Schoellerbank shall apply. Primary services of Schoellerbank cannot be changed in this manner.