SB Saanen Bank AG
CH-3792 Saanen
tel 033 748 46 46
www.saanenbank.ch

Special Provisions for Digital Banking Services

These Provisions apply equally to all genders and to multiple persons.

These Special Provisions for Digital Banking Services govern the use of the Bank's digital services by both the Contractual Partner and any other authorised Users. The term "**Contractual Partner**" refers to the individual who maintains the business relationship with the Bank. "**Users**" are individuals who use the digital services either as the Contractual Partner or as persons authorised by them.

By accessing the digital services, the Contractual Partner and any Users acknowledge and accept these Special Provisions for Digital Banking Services, along with the Bank's Privacy Policy. The General Terms and Conditions (GTC), Custody Account Regulations and any other agreements between the Bank and the Contractual Partner are binding on all Users. The Contractual Partner is responsible for informing and advising Users about these provisions and any other essential information – particularly for providing risk disclosures.

The Bank reserves the right to amend these Special Provisions for Digital Banking Services at any time.

1. Scope of digital services

Digital services allow the Contractual Partner to manage their banking transactions online and access information. This includes, in particular, viewing account and custody account details, submitting payment and securities orders, accessing card-related information and initiating card changes.

The range of functions available through the digital services is determined by the Bank and may be modified, expanded or restricted at any time.

2. Access to digital services

2.1 Technical requirements

Access is provided via the Internet through a network provider. To access the digital services, Users must have the necessary hardware and software, for which they are solely responsible.

They are also required to implement appropriate security measures – particularly to protect their access devices from unauthorised use by third parties and from cyber threats – and to ensure that the security settings on these devices are kept up to date.

2.2 Authentication checks

Access to the digital services is granted to individuals who successfully authenticate themselves to the Bank using personal identification credentials (such as authentication via the Saanen Bank Mobile App, passwords, identification codes or hardware tokens – collectively referred to as "means of identification"). These means of identification are issued to Users for their intended use only. The Bank may replace or modify them for legitimate reasons at any time.

Where biometric data is used for authentication, the User must ensure that only their own biometric data is stored on the relevant device. The Bank has no access to, and no control or influence over, the biometric data stored on a User's access device. It is the User's responsibility to ensure that the device is protected against unauthorised access.

During the identity verification process, the Bank may disclose the User's means of identification to third parties appointed by the Bank.

2.3 Responsibility for use

The Contractual Partner assumes all risks and is liable for any damage resulting from Users' use of the digital services.

Any person who successfully authenticates using the means of identification may be regarded by the Bank as a duly authorised User, regardless of their internal legal relationship with the Contractual Partner and irrespective of any contrary entries in the Commercial Register, publications or signature regulations. Accordingly, the Bank may accept orders and legally binding communications from such individuals without conducting any further verification of their authorisation. This remains the case even if the person is not actually authorised but has managed to authenticate themselves successfully. The Contractual Partner is accountable for all actions that occur as a result of the aforementioned authentication checks.

The Contractual Partner hereby accepts without reservation all transactions, business dealings, agreements and declarations carried out via the digital services using the User's means of identification. All instructions, orders and communications received by the Bank through such authentication are binding on the Contractual Partner.

2.4 Issuing orders

The Contractual Partner authorises the Bank to execute all orders received via its digital services and to act on instructions and communications, provided that identity verification has been properly completed in accordance with the system's requirements. The Bank may, at its sole discretion, decline to execute individual orders submitted via the digital services.

If a User has not been separately appointed by the Contractual Partner as an authorised representative outside the digital services, and if the Bank has not accepted such appointment, the Bank will not execute any orders or act on instructions submitted by that User outside the digital services.

The Bank also retains the right to refuse to accept any instructions, orders or communications via the digital services at any time and without providing a reason.

If a User submits an order that is not executed, or is only partially executed, they must notify the Bank immediately.

2.5 Blocking access

Users may block their own access to the digital services or request that it be blocked. The Contractual Partner may also request that the Bank block a specific User's access. Such requests may be made during regular business hours at the Bank's account-holding branch, or outside those hours via the Service Desk. In either case, the request must be promptly confirmed to the Bank in writing.

In urgent cases, Users may block access themselves by intentionally entering incorrect login credentials several times, thereby activating the automatic security lock. This block can be lifted again by the Contractual Partner by making a request to the Bank.

If there is any indication or suspicion that an unauthorised third party has obtained knowledge of a User's means of identification or accessed the digital services, or if misuse is suspected, the User must immediately arrange for access to be blocked and notify the Bank without delay.

The Bank may at any time block a User's access in whole or in part, without giving reasons and without prior notice.

3. Costs and compensation

The Bank's standard services are made available to the Contractual Partner free of charge within the scope of the digital services. The Bank reserves the right to introduce or modify fees for the use of the digital services. Any introduction or change in fees will be communicated to the Contractual Partner through electronic notification, via the digital services or by another appropriate means. Any new or amended fees will be deemed accepted unless the Bank receives a written objection within one month of notification.

The Contractual Partner authorises the Bank to debit any charges and fees from an account held by the Contractual Partner.

SB Saanen Bank AG
CH-3792 Saanen
tel 033 748 46 46
www.saanenbank.ch

SAANEN SB BANK
GSTAAD'S PRIVATE BANK

4. Duties of care

If the Bank issues a password to the User, the User must change it immediately upon receipt. Passwords must also be updated regularly thereafter.

Users are required to keep all means of identification strictly confidential and protect them from any misuse by unauthorised persons. In particular, no changed passwords may be recorded or stored unprotected on the User's computer or disclosed to unauthorised third parties. Passwords must not be based on obvious or easily identifiable data (e.g. names, dates of birth, phone numbers or vehicle registration numbers).

The Bank will not contact the Contractual Partner or any User by electronic means or otherwise to request access credentials or the disclosure of authentication details used for the digital services.

The Contractual Partner will bear all consequences arising from the disclosure and also from the misuse of the User's means of identification.

The User acknowledges that they are solely responsible for entering all orders to be processed via the digital services. As a general rule, orders entered incorrectly cannot be modified. The Bank is under no obligation to monitor the correctness or completeness of orders entered by Users.

5. Electronic account/custody account documents

The Contractual Partner acknowledges that written and electronic notifications are equally binding.

As soon as electronic account or custody account documents are made available to the User within the digital services environment, they are considered to have been delivered to the Contractual Partner. Once accessed, these documents will remain available in the system for a minimum period of three months.

The responsibility for the storage of account/custody account documents lies solely with the User. Any complaints regarding the executed transactions will be subject to the Bank's General Terms and Conditions. The Contractual Partner may request account/custody account documents in paper form at any time. The Contractual Partner hereby agrees to the Bank's applicable fee schedule.

6. Secure communication channel

As part of its digital services, the Bank provides Users with a secure communication channel for the exchange of communications and documents. Communications and documents submitted by Users through this channel are processed during the Bank's regular business hours.

Time-critical orders, such as payment or securities transactions, must not be submitted through the secure communication channel.

Communications and documents are considered delivered to the Contractual Partner as soon as they become available to the User within the digital services environment. The User is therefore responsible for reviewing such communications and documents promptly and ensuring that any relevant information is passed on to the Contractual Partner without delay.

Upon receiving documents through this communication channel, the User is obliged to store those documents outside the digital services.

The Bank reserves the right to delete documents made available through digital services if storage limits are exceeded or after a defined retention period has passed.

7. Electronic signing of documents

Certain documents can be electronically signed through the digital services, in accordance with the applicable signing authorisation. Before signing, the User must carefully review each document for completeness and accuracy. If any discrepancies or omissions are identified, the User must notify the Bank immediately. These documents can be digitally signed. By electronically signing such documents, the customer confirms they have read and understood the contents and fully agree to them. Electronically signed documents are legally equivalent to documents signed by hand. Printed copies that are subsequently signed manually are legally effective only if accepted by the Bank.

To issue the necessary certificates for electronic signatures, the User provides the Bank with the requisite personal data (e.g. first name, surname, date of birth, nationality, type of ID and ID number). The User authorises the Bank to forward this information to a certification service provider appointed by the Bank for the purpose of issuing the certificate.

Documents signed digitally are made available to the User for a limited period within the digital services environment. The User is responsible for saving these documents outside of the digital services.

The Contractual Partner expressly recognises the binding nature and legal validity of the certificates and electronic signatures issued by the Bank's designated certification service providers as evidence of all transactions and actions carried out between the Contractual Partner and the Bank.

8. Notification services

As part of its digital services, the Bank offers Users the option to receive notifications about certain events via electronic channels (such as text messages, e-mails or push notifications). By activating these notification services, the User expressly consents to the delivery of the selected messages. The Contractual Partner and the User acknowledge that personal data and information covered by banking secrecy may be transmitted through these notifications. Such transmissions may occur over unsecured channels that are not controlled by the Bank.

For technical reasons, the Bank assumes no responsibility for ensuring that these notifications actually reach the User. Such issues may result from delays, incorrectly routed messages or service disruptions.

9. API interface to third-party service providers

9.1 Scope

The Bank offers the Contractual Partner and Users the option to exchange account and custody account-related data and information with third-party service providers (e.g. fintech companies) for the purpose of enabling specific services ("information exchange"). This exchange takes place via a secure Application Programming Interface (API) provided by the Bank. The API allows Users to integrate third-party software, technical solutions or services with the Bank's digital services. The User alone is responsible for carefully selecting and monitoring any third-party service provider. The Bank does not assume any responsibility to oversee, verify or monitor these providers.

Data is transmitted to the third-party service provider strictly in accordance with the User's instructions. The User must select and activate the relevant third-party service provider.

Data exchange occurs indirectly via the bLink platform operated by SIX BBS AG (SIX) ("platform"). The Bank's obligation is limited to the transmission and receipt of data ("use cases") through this interface. The Bank publishes the currently supported use cases on its website.

Once access to the interface has been approved by the Bank, it will respond to data requests and accept corresponding "service calls" from authorised third-party providers. If a service call includes an order to the Bank – such as a payment instruction – additional authorisation may be required within the Bank's digital services.

Data exchanged via the API may differ from data or documents transmitted by the Bank through other channels. For example, transaction values may be recorded based on the transaction date rather than the value date.

The Bank reserves the right to modify the scope of its API services at any time. This may include the introduction of new use cases, as well as changes to or the discontinuation of existing ones.

9.2 Identification key
Once the User activates the information exchange function in the Bank's digital services using valid means of identification, the Bank will generate and issue an electronic identification key ("token"). This token is transmitted by the Bank to the third-party service provider via the platform. The Bank has no control over how the third-party service provider uses the token and cannot ensure its lawful or proper use. If a service call from a third-party service provider or the platform includes the corresponding token, the Bank will respond accordingly. The third-party service provider is solely responsible for the secure handling, management and processing of any data it receives or provides. The Bank assumes no monitoring or other obligations in this regard.

9.3 Special duties of care
If the User wishes to end the exchange of information between the Bank and a third-party service provider they have previously selected and activated – or limit access to specific devices – they must delete or restrict the information exchange with the relevant third-party service provider. Termination or restriction of the information exchange must be carried out by the User within the Bank's digital services. Until such deletion or restriction is completed, the Bank will continue to respond to service calls from the third-party service provider.

The third-party service provider verifies the User's access rights using the authentication credentials it has issued. The User is responsible for keeping these credentials confidential and protecting them from unauthorised use, in accordance with the third-party provider's guidelines.

The Contractual Partner acknowledges that all Users may establish API interfaces with third-party service providers.

9.4 Approved third-party service providers
Users are free to choose which third-party service providers they wish to activate. However, only those providers that have been approved by both the Bank and the platform may be selected. The Bank reserves the right to exclude specific third-party service providers at any time, without providing reasons.

The Contractual Partner and Users acknowledge that the access rights granted by a third-party service provider may differ from those granted by the Bank. Since the third-party service provider delivers its services independently and without the Bank's involvement or oversight, it is the sole responsibility of the Contractual Partner or User to monitor the access permissions granted and to adjust them as needed.

9.5 Use of data by third-party service providers
The Contractual Partner and Users acknowledge that by transmitting data via the platform to third-party service providers, they are granting those providers access to the relevant data. In doing so, they release the Bank from its confidentiality obligations and expressly consent to the disclosure of such data. The data is exchanged via a service call, which the third-party service provider sends indirectly to the Bank through the platform.

The transfer of data to the third-party service provider or from the third-party service provider into the User's systems, as well as the provider's use of the data, are governed solely by the third-party provider's agreements, particularly its privacy policy. Responsibility for ensuring data security and compliance with applicable data protection laws rests entirely with the third-party service provider. The Bank has no influence or control over how the third-party service provider uses the data or which security measures it applies. Data processed by the third-party service provider may also be stored abroad, in which case it will not be subject to Swiss legal protections, including banking secrecy regulations. The third-party service provider acts solely as an auxiliary person engaged by the User. The Bank therefore disclaims any duty to monitor or control and any other responsibility for the actions or omissions of the third-party service provider.

9.6 Use of data by the platform
The data of the Contractual Partner or User may be processed and stored by the operator of the platform. The platform operator may use this data for the following purposes:

- Operating the platform
- Supporting and monitoring data queries and orders
- Further developing the information exchange functionality

The Bank has no control over how the platform operator uses the data.

9.7 Use of data by the Bank
The Contractual Partner and the User agree that the Bank may use data received from third parties through the information exchange for the purpose of providing comprehensive advisory services, reviewing the data and reusing it in accordance with applicable legal requirements.

9.8 Liability when using the information exchange
The Bank has no influence over the information exchange, nor over the services provided by third-party service providers or the platform operator. The Bank does not assume any monitoring or supervisory responsibilities with regard to the third-party service provider or the platform operator and expressly disclaims any warranty or liability for their actions or omissions.

10. Multi-banking
10.1 Scope
Multi-banking enables Users to instruct the Bank to retrieve data from third-party banks and to forward orders to them. For this purpose, the Bank provides the necessary interfaces or may use third-party platforms such as bLink from SIX BBS AG.

The Bank reserves the right to decline integration with third-party banks that do not meet its internal standards. Additionally, the Bank may refuse to process data transmissions that are incomplete – for example, payment orders lacking required information.

10.2 Identification key
The activation process and all subsequent data exchanges between the Bank and a third-party bank account connected via multi-banking are conducted using a token. This token is linked to the means of identification that are valid for accessing the digital services.

10.3 Special due diligence obligations when using multi-banking
The User is responsible for verifying the accuracy of data transmitted to third-party banks – such as payment orders – and must immediately notify the third-party bank of any discrepancies.

10.4 Data protection when using multi-banking
The Contractual Partner and the User agree that the Bank may use data received from third parties through multi-banking for the purpose of providing comprehensive advisory services, reviewing the data and reusing it in accordance with applicable legal requirements.

10.5 Liability when using multi-banking
The Bank accepts no liability for the platforms of third-party service providers, third-party banks or any auxiliary persons engaged by them. While the service is provided with the level of care customary

in the banking sector, the Bank has no influence over nor any monitoring function in relation to the platforms of third-party service providers, the third-party banks or any third parties engaged by them.

11. Electronic invoices (eBill)

The Bank offers Users the option to participate in the eBill invoicing system, allowing them to receive and pay electronic invoices. Invoices may be approved individually or through collective or standing approvals, as defined by the User's settings.

To participate in the eBill invoicing system, the Contractual Partner must authenticate themselves via the Bank's digital services and complete a one-time registration with SIX through the eBill portal.

Electronic invoices received through the eBill system can be approved or rejected directly by the User within the digital services. The User is responsible for verifying the accuracy and completeness of all payment orders before approval.

The Bank does not guarantee the correctness or completeness of electronic invoices. Any complaints relating to an invoice – such as delivery method, content or amount – must be addressed by the Contractual Partner to the invoice issuer.

The eBill service is provided by SIX Paynet AG.

12. Special rules for banking transactions via the Internet and the public telecommunications network

Data received and sent by the Bank in connection with the use of digital services is encrypted by the Bank, with the exception of information on the sender and recipient, in so far as this is permitted by the technical procedures used in each case.

The Contractual Partner acknowledges that the Internet and public wireless networks are global and open systems accessible to all. Digital services traffic between the User and the Bank takes place via public facilities that are not specifically protected. This applies both to instructions sent by the User and to messages transmitted by the Bank. The data to be transmitted over the Internet may leave the territory of Switzerland in an unforeseen manner, even if the sender and recipient are located in Switzerland. As the sender and recipient are not encrypted within the scope of digital services, unauthorised third parties may be able to read the relevant information. Unauthorised third parties can therefore draw conclusions about a client relationship between the Bank and the Contractual Partner both in Switzerland and abroad.

Using the Bank's digital services from abroad or through private gateways (e.g. a VPN) is done entirely at the User's own risk. The Bank expressly disclaims any liability for risks or consequences resulting from such access.

13. Liability of the Bank

The Bank applies the usual standard of care when providing digital services and operating its data centre. Where possible, the Bank will give prior notice of any foreseeable operational interruptions. Operational interruptions for maintenance purposes, for the expansion or modification of the Bank's system or in the event of suspected or identified threats to operational safety are expressly reserved and do not give rise to any legal claims by the Contractual Partner. Processing interruptions will be remedied as quickly as reasonably practicable. Processing interruptions do not give rise to any compensation claims by the Contractual Partner. The Bank does not provide technical access to its services. This is the sole responsibility of the User. The User specifically acknowledges that the Bank does not typically sell the specific security software needed for digital services. The Bank therefore accepts no liability for the providers or for the security software.

Furthermore, the Bank assumes no responsibility for the accuracy or completeness of any data or information displayed or transmitted as part of the digital services. In particular, information on accounts and deposits (balances, statements, transactions, etc.) is provisional and non-binding. Similarly, none of the communications within the scope of the digital services constitute binding offers unless they are expressly marked as being binding. Furthermore, information about foreign exchange or exchange rates is always non-binding.

The Contractual Partner acknowledges that the Bank is not responsible for the transmission of electronic data from the User to the Bank's data centre, and from the Bank's data centre to the User; this is to be arranged by the User themselves or by third parties engaged by them. The transactions made on the Bank's system, as reflected in electronic records and any computer printouts provided by the Bank, are always binding for the Bank. The Bank is not liable for any damage incurred by the Contractual Partner as a result of transmission errors, technical deficiencies, disruptions or third-party interference in the data transmission infrastructure.

The Bank will not be held liable for any damage incurred by the Contractual Partner as a result of the non-fulfilment of its contractual obligations or the contractual obligations of the User, nor for indirect damage and consequential damage, such as lost profits or third-party claims.

The Bank accepts no liability for orders not executed on time or in full and any related losses, in particular due to price losses, provided that the usual standard of care has been applied.

14. Authorisation provisions

A User's authorisation to access and use the digital services remains valid until a written revocation thereof is sent to the Bank, regardless of any public publication and/or entries in the Commercial Register. This revocation must be made in writing, although the Bank may but does not have to accept a verbal revocation. This authorisation does not lapse in the event of the death, legal declaration of disappearance or loss of legal capacity of the Contractual Partner, nor in the event of a User's incapacity.

15. Termination

The digital banking services agreement may be terminated at any time – by the Bank without notice, or by the Contractual Partner through written notice.