Safety of LPB Bank Internet Bank

SAFETY OF INTERNET BANKING

Internet Banking of AS **LPB Bank** (hereinafter referred to as the Internet Banking) is the Bank-supported system that provides Clients with remote access to the Clients' accounts in the Bank and the ability to remotely perform Bank transactions and communicate with the Bank. There is a multi-stage security system that protects users on the Internet Banking system.

1. Secure connection

- **HTTPS** provides a secure data transfer channel between your computer and the Bank. A secure connection is indicated by the lock symbol in the left corner of the browser's address bar.
- **The SSL Certificate** confirms the authenticity of the Internet resource and indicates the highest degree of security of the Internet Banking.
- **The session duration** of the Internet Banking is limited to 5-30 minutes (depending on the individually set session duration). The main purpose of this limitation is to protect the user from unauthorised access to data in cases where the user leaves PC without logging out of the Internet Banking system. After the session is interrupted, you must re-enter all the security parameters.
- **"Registration Log"** is located in the "Profile" section of the Internet Banking. This section reflects information on activities performed in recent sessions, including the date and time of recent sessions, as well as the IP address of the PC from which a connection to the Internet Banking system was established.
- **Password Change** - the Client has an opportunity to choose the frequency of changing the access password to the Internet Banking (5 to 50 sessions).
- **User Blocking** - the Bank blocks the user from accessing the Internet Banking system with an appropriate Identification Tool and/or the Identification Tool itself in cases provided for by the Contract between the Bank and the Client.
- **Temporary access restriction** - when logging into the Internet Banking, using the One - Time Security Code, you must enter a permanent password. If you enter an incorrect password 5 times in a row, the Bank restricts access to the Internet Banking for 1 minute. After 1 minute, access to the Internet Banking system will be automatically renewed. If you repeatedly enter a wrong password 5 times in a row, the Bank restricts access to the Internet Banking for 15 minutes. After 15 minutes, access to the Internet Banking system will be automatically renewed. In event of next 5 successive unsuccessful attempts to enter your correct permanent password, the Bank will restrict access to the Internet Banking for 60 minutes.
- To **obtain a new password,** you have to visit the Bank or call at (+371) 6 777 2 999.
- Various **levels of access** to the Internet Banking system - when entering into the Bank Service Agreement, the Client may set restrictions of user rights, displaying of individual accounts or preparation of payments, allowing one user to enter payment data, but restricting this user's ability to send a payment.

- **Money transfer limits** - for additional user safety, the Bank has introduced the daily and monthly limits for the money transfers to be signed by the One - Time Security Code.

2. Connecting to Internet Banking

When entering into an Internet Banking Connection Agreement, the Client may choose between two different levels of access security:

- **One - Time Security Code** – the One - Time Security Code will be sent as a text message to the mobile phone number specified upon registration.
- **The DIGIPASS Code Calculator** is an electronic device that generates a unique one-time digital code for the authorisation with the Internet Banking system and the confirmation of orders that replaces the authentic signature of the Client in the Internet Banking.

The One - Time Security Code and the one-time numerical code from the DIGIPASS Code Calculator are only valid for a limited time period.

The instruction manual for the use of the DIGIPASS 310 Code Calculator is available here.

As of 01.04.2017, the Bank has ceased issuing new Identification tables. Previously issued Identification tables should be replaced by the Client with the One - Time Security Code by registering the mobile phone number with the Internet Banking on its own or with the help of the Bank's specialists.

2.1 Authentication Tools

The Client's authentication is performed at three levels:

DIGIPASS Code Calculator	Mobile phone
Client's CIF Number	Client's CIF Number
DIGIPASS PIN Code	Password
Generated DIGIPASS Code	One - Time Security Code

The Client's **CIF number** is an individual identification number assigned to each Client (when the contract is concluded), which does not change until the contract's termination. The number is a combination of six characters — Latin letters and numbers. It must be entered upon every authorisation in the Internet Banking system.

Password - when authorising in the Internet Banking, a password must be entered in addition to the Client's CIF number. The first time you log in, you are prompted to change the initial password immediately after the authorisation. The password, mobile phone number or DIGIPASS Code Calculator is attached to the Client's CIF number.

The **PIN Code** is an individual password assigned to the DIGIPASS Code Calculator.

The **One - Time Security Code** is a computer-generated digital code that is sent to the Client's mobile phone.

2.2 Benefits of the DIGIPASS Code Calculator

- **Time limit** and **authorisation algorithm**. A limited period of time starting from the time a code is received by the cell phone to the time it is entered provides additional protection against unauthorised access to your data. The DIGIPASS Code Calculator provides the highest degree of safety when working in the Internet Banking system.
- The DIGIPASS Code Calculator generates a unique code available only to its users - a one-time password for the Client's authentication (for access to the system) and a document authorisation password (equivalent to an electronic signature). For document authorisation, a **HASH Code** is calculated and should be entered in the DIGIPASS Code Calculator, which in turn calculates the value of the electronic signature. Therefore, when changing at least one digit in the document, the HASH value also changes. This safety feature guarantees the highest level of security for the Client.
- **VASCO Patented Algorithm** - the Bank grants its Clients the safety of access to the Internet Banking and the security of transaction data owing to one of the safest producers of code calculators, whose quality has been recognised by banks of Latvia and worldwide.
- **The DIGIPASS Code Calculator is protected by a PIN code** - each DIGIPASS Code Calculator has been assigned a unique PIN code that must be entered to access the code calculator. **Do not keep PIN code together with the Code Calculator!**
- The DIGIPASS Code Calculator **is blocked** after five attempts to enter an incorrect **PIN code**, which is a particularly important factor in case of theft or loss of the DIGIPASS Code Calculator.
- **Unlimited money transfers** — when choosing the DIGIPASS Code Calculator as a security tool in the Internet Banking, the amounts of your e-transactions are not limited.
- **Reliable standard** — currently, the DIGIPASS Code Calculator is recognised as the safest way to protect electronic data worldwide.

3. Confirmation of orders in the Internet Banking

The authorisation of documents in the Internet Banking is based on the chosen security tool - the One - Time Security Code or the DIGIPASS Code Calculator:

Mobile phone	DIGIPASS Code Calculator
One - Time Security Code	DIGIPASS Order Confirmation Code

4. Security recommendations to the user

1. PC safety:
   - Set and periodically change a trustworthy password for an access to your computer.
   - Use a screen saver with a password to block third-party access to your computer while you are away.
   - Use licensed software and update it in a timely manner.
   - Antivirus software - the primary purpose of these applications is to check whether your PC's software is infected with viruses, and to identify, isolate, and eliminate detected viruses. Antivirus software needs to be updated regularly to ensure its maximum efficiency.
   - Firewall - protective software that regulates the flow of information between your computer and Internet by filtering data, thus preventing unauthorised access.
2. Make sure that you have a "secure connection" to the Internet Banking system.
   - Getting started — use the Internet Banking at https://ib.lpb.lv or click on the link listed on the website http://www.lpb.lv/. Do not use any links you have received by e-mail from other users. Do not hand over the user ID, password or other identification or financial information to third parties. Make sure you are on the correct site.
   - The Internet Banking system in the browser with a "secure connection", as evidenced by HTTPS at the beginning of the Internet Banking's address in the browser's address bar. The SSL Certificate indicates the highest degree of security of the Internet Banking.
3. When using the Internet Banking in public places, make sure that no one is watching you during entering the Internet Banking access data. Do not use the Internet Banking at the places where you are unsure about the safety of the computer network, and where there is a high probability of viruses and recording devices.
4. Do not leave the Internet Banking session unattended.
5. If you are suspicious of the unauthorised use of your Internet Banking, check the status of the last session with the Internet Banking system. In the Profile section of the Internet Banking, you'll find the "Registration Log" section, which shows information regarding the last connection, including the date and time of the last session, the actions taken, and the IP address of the PC from which the connection to the Internet Banking system was established.
6. To safely shut down the Internet Banking, click the Log Out button and close the browser window.
7. Do not leave the Internet Banking identification information in the places accessible to third parties. If you suspect that the Internet Banking identification information has become known to third parties, please contact the Bank. Change your password if you suspect that it has been acquired by unauthorised persons.
8. Password — do not use a password associated with your name or personal information, or the names or personal information of your loved ones. Regularly change your password!

9. Always contact the Bank in case of any suspicions. If you have any questions or loss of access data to the Internet Banking, as well as in case of disclosure of confidential information, please contact the Bank's customer service specialists by calling: (+ 371) 6 777 2 999 or sending e-mail to info@lpb.lv.

Important! The Bank has never sent and will never send requests for a password change by e-mail, phone or other electronic means!