

Online Banking Security Policy

As part of its commitment to its customers, Multibank is interested in offering access to its banking products and services in an efficient and secure way.

For this purpose, it relies on safety measures oriented to protect the privacy and the integrity of the personal and financial information that it handles; these measures include the interaction of the customer with the Bank from the time the session is initiated until it is terminated.

Online Banking Service

1. In order to use Multibank's Online Service, the URL www.multibank.com.pa must be accessed.
2. In order to perform the transactions required by the Online Banking user, the following conditions previously indicated in the Single Banking Services Agreement must be fulfilled and the credentials must be entered, which consist of a User and a Password that are delivered in person and are personal and nontransferable.

Every time a new Password is delivered, it must be obligatory changed the next time the session is started.

3. The Password is a series of characters known only by the user of online banking which consists of a minimum number of characters.
4. For the purposes of guaranteeing the proper access of the users to the online banking service some validations such as the following are performed:
 - The blockade of the passwords after repeated unsuccessful attempts to register the credentials correctly (user and Password). In this case, you should communicate with your account officer or visit the nearest branch so that your password can be enabled.
 - Denial of reuse of a same password that has been used.
5. For security reasons, the Online Banking service expires automatically after a period of time in which the computer of the user remains inactive. In the screen will appear an explanatory message that will require restarting the session.
6. In case that you forget your password, you must request the change of password to your account officer or at the nearest branch.
7. The Online Banking service is subject to periodic revisions and monitoring, in order to detect attempts of attacks to the service.
8. Multibank does NOT request updates of the confidential information of its customers such as: User, Key or Password, account numbers, credit card numbers, code cards, etc.

Confidentiality of the Information

9. In order to guarantee the authentication, certification and encryption of the electronic transactions, Multibank uses Digital Certificates which are represented by two components: a padlock closed in the bottom of the screen, which indicates that it is operating in a safe mode; and the Internet address (URL) that begins with "https" instead of "HTTP".
10. The bank uses technological resources to protect and limit the non-authorized use of your Online Banking Service.
11. The bank relies on services of permanent monitoring on the use of the illegal access of its trademark as well as of virus protection.
12. To guarantee the confidentiality and integrity of the information, the bank uses additional elements that will allow the validation of the identification of the users' identity at the moment they make transactions, such as the secure connection card.

Responsibility of the users of Online Banking

13. To choose a strong password that is difficult to decipher by third parties, and which only is known by him/her. Some considerations on the subject are:
 - Not to include the user as part of the Password
 - Not to use key dates or information from private life, relatives, children, or professional life such as dates of birth, wedding, beginning of work, etc.
 - Not to include personal or work telephone numbers.
14. To protect the computer with an updated antivirus that allows detecting and fighting malicious programs.
15. To maintain the confidentiality of the password, to avoid to write it in any place or unsafe means or within the reach of other people.
16. To immediately change the password whenever you suspect that it could have been exposed to:
 - Someone that could have seen it.
 - When you suspect or are certain that someone else (family, fellow worker, etc.) knows the password.
 - If you have not use it for more than 30 days.
17. To make sure to that you have logged out correctly from Online Banking after finishing using the services.
18. To change the password whenever the system asks for it or is considered advisable.
19. NOT to store credentials in the browsers.
20. To monitor your accounts and the historical detail of the historical transactions.

Reservations of the Bank

21. The bank reserves the right to block the access to the users that have provided false information or for any other security reason.
22. The bank reserves the right to make changes, modifications or updates of these Policies at its sole discretion.