**Security Statement** :

Security Standards Employed by us-and what you can do to stay Safe Online

Bank Simpanan Nasional (BSN) is highly committed in ensuring that all data, materials, information disclosed, shared, stored or used, or any transactions performed via BSNeBiz are kept safe, secure, private and confidential. For this purpose, a security and privacy protection system is in place to ensure that the highest security and confidentiality standards are maintained.

Username and Password

To prevent unauthorised access to our online financial services, every customer is required to select a username and password, which provides access to their financial information. The username must be between 8 to 12 characters in length and consists of alphanumeric elements, which include both alphabets and numbers. The use of special characters (e.g. \* & \_#$) including spaces are not allowed. The password must be 6 to 12 characters in length and consists of at least 3 of these elements: uppercase/lowercase alphabet, numbers and/or special characters.

The username is not case sensitive but the password is case sensitive.

*E.g*: **Username:** ShamShawn73 **Password:** model37\_hensem

You are advised to follow some tips to ensure the integrity of your username and password:

* Do not choose a password that others can easily guess.
* Do not use simple words, your name, birth date, telephone number or names listed in a standard dictionary.
* Memorise your password and do not write it down.
* Passwords should be keyed in when accessing an online account to protect your personal information.
* Sharing your password or PIN with another person is the same as giving that individual authority to use your access in a transaction. It should not be disclosed even if requested by an authorised BSN Officer.
* Change your password frequently.

To create a unique password, you could use the methods as follows:

* Use a combination of unrelated words and numbers *E.g. Car45fisH*
* Use grossly misspell or mistyped words *E.g.commando\*10\* -: komando\*10\**

Information Protection

While we take considerable effort to ensure a safe and secure online experience, we have no control over the computer you use to access BSNeBiz. As an added security feature, we have incorporated an automatic log out function if no activity is detected after a preset time limit.
However, you must ensure that you do not provide anyone the opportunity to gain access to your account information:

* Ensure that no one has access to your computer or records your online activities.
* Always log out of BSNeBiz immediately after completing your transactions and/or before visiting other websites.
* Do not send any information about your account via email.
* Disable the AutoComplete function on your browser to avoid automatic completion of your Username when you type in your Username.
* To turn AutoComplete “On” or “Off” in MS Internet Explorer browser:
* Ensure that no one has access to your computer or records your online activities.
* Always log out of BSNeBiz immediately after completing your transactions and/or before visiting other websites.
* BSNeBiz collects personal information that you voluntarily provide in this website, which may include your name, address, email address, marital status, salary range, number(s) of children, etc. We use this information to communicate with you and to provide you with your requested service or product. If you provide your consent at the time your personal information is collected via this website, we may also provide you with information, special offers, and promotions. Furthermore, we may store some or all of that personal information and use it for marketing purposes and research. Your data will be maintained for as long as you are a customer of BSN.

Data Confidentiality and Intergrity

To ensure data confidentiality and integrity, all information transmitted over the Internet is encrypted using the 128-bit Secure Sockets Layer (SSL) protocol from Verisign Certificate Authority. SSL is a secure way of transferring information between two computers on the Internet using encryption. Strong end to end encryption is also adopted within BSN’s computer networks and resources.

BSNeBiz is WebTrust certified. This certifies our compliance with leading international security standards and Best Practices, as well as our commitment to maintaining a secure environment. WebTrust is an independent corporation that monitors and tests our facilities to assure that we maintain the highest and most current standards in Internet information security and exchange.

Systems Security and Monitoring

BSN has adopted a combination of the following systems security and monitoring measures for online transactions:

Firewall systems, strong data encryption, anti-virus protection and round-the-clock security surveillance systems to detect and prevent any form of illegitimate activities on our network systems.

Regular security reviews of our systems from time to time.

We also take every effort in ensuring collaboration with major vendors/manufacturers to keep abreast of information security technology developments, for possible and future implementation.

Computer Virus Protection

Computer viruses are real and once your computer is infected it can cost you time, loss of information, repair expense, and aggravation. Ensure that your computer has an anti-virus protection program installed to reduce the risk.

We recommend that you purchase a program that automatically upgrades your virus protection on a regular basis. If you currently have a virus protection program on your computer without the automatic upgrade feature, make sure you update your virus detection program at least once a month and/or when you hear of a new virus, to minimise your risk. You can do this by visiting the Internet site of the company that provides your software.

In addition, we advise you to not open attachments from others unless you are absolutely certain you can trust the source. However, it’s best to be cautious. Whoever sent you that attachment may not know that they have carried the virus to you.

Updating your Browser

An Internet browser allows access and the ability to navigate a myriad of information and service resources on the Internet. Most computers come with a browser already installed.

Always update your browser when new versions are released because they often include new security features.

Check your browser for built-in safety features that you may or may not elect to use.

If you use Internet Explorer, update it to IE version 7.0.

You may access the latest security patches.

It is a good practice to always check the site certificate before logging in.

Security Tips

**Protect Yourself and Your Information Online**

Be careful when you do your banking online. There have been cases of copycat websites posing as authentic websites, or emails/phone calls asking you to provide personal or account-related information with the intention of carrying out Internet theft and fraud.

Please take the necessary precautions and be on the alert for suspicious emails or phone calls asking for your personal account information. **Never reveal your Internet Banking and/or account information to anyone.**

**10 easy ways to protect yourself**

* Do not share your password with your spouse, friends, relatives or anyone. Your password is designed to protect the privacy of your banking information. This will only be effective if you keep them private.
* Change your password frequently. If you think your password has been compromised, contact us to reset your password.
* Do not use the “remember password” function because this information can be easily accessed by hackers.
* Do not send any information about your account via email.
* Do not provide your account details or passwords in response to any email or phone call. A bank officer will never ask for this information.
* Don’t open suspicious email attachments.
* Avoid downloading free programs. These may incorporate hacker-friendly software.
* Always log out of BSNeBiz immediately after completing transactions and before visiting other websites.
* Clear your cache (information stored in your computer memory) each time you log out.
* Avoid opening your Internet Banking at public places (internet café). If you have to, clear your cache after logging out.

If you have queries about any email from BSN or are suspicious that someone may be trying to get your password or account information under false pretences, immediately contact BSN Contact Centre (7.00 am to 12.00 am) at 1300 88 1900.