



INFORMATION TECHNOLOGY SUB-SECTOR

CONNECTIVITY REGISTRATION FORM

VPN and File Transfer Services

(Kindly refer to the instructions at the back on how to fill-up this form)

Name of Participating Bank (PB) / Institution:		Date of Request:	
Complete Address: <i>(Please indicate Zip Code)</i>		Contact No.:	
A. Type of Service: <input type="checkbox"/> New <input type="checkbox"/> Additional		B. <input type="checkbox"/> PhilPaSS Remit System and File Transfer <input type="checkbox"/> PhilPaSS Participant Browser <input type="checkbox"/> Electronic Funds Transfer Instruction System (EFTIS) <input type="checkbox"/> Others (Please specify) _____	
C. Select Type of VPN Connection:			
<input type="checkbox"/> Site-to-Site VPN <i>(Banks should have existing Enterprise Firewall or IPSEC/VPN-capable Router. Recommended for multiple users/clients.)</i>		<input type="checkbox"/> Remote Access VPN <i>(Subject for Approval)</i>	
D. VPN PEER IP ADDRESS: <i>(PB's VPN Gateway Public IP address):</i>		E. VPN PEER IP ADDRESS: <i>(PB's VPN Gateway Public IP address):</i>	
Primary Site: _____	Remote/Backup Site: _____	Primary Site: _____	Remote/Backup Site: _____
F. CLIENT/HOST IP ADDRESS: <i>(Allowed PCs to access the service)</i>		G. Name of Authorized User <i>(Last Name, First Name, Middle Name)</i>	
Primary Site: _____	Remote/Backup Site: _____	<i>(Please provide separate sheet for more than 1 user w/ their e-mail add.)</i>	
		e-Mail Address:	Mobile No.
H. Name of IT Network Support <i>(Last, First, Middle Name)</i>		e-Mail Address:	Mobile No.
TERMS AND CONDITIONS			
<p>The requested VPN and or File Transfer access to BSP are provided for the exclusive use of PB/Institution users to allow access in the Philippine Payments and Settlements System (PhilPaSS). The request is accomplished by the authorized system user that is approved and signed by the Head of the Institution/ Authorized Signatory.</p> <p>The requesting PB/Institution must abide or conform to the BSP technical requirements. The Institution shall be responsible for any hardware upgrades required to support the VPN connectivity and file transfer. BSP shall provide support for BSP VPN connectivity and file transfer services only. BSP must be informed for any changes in the VPN client side configuration 5 days in advance to avoid disruption of the services.</p> <p>BSP may revoke, block, or permanently disallow the use of this service without prior notice due to reasons that may compromise internal security. Any breach or compromise in PhilPaSS services shall be immediately relayed to the BSP-PSO through the PhilPaSS Customer Contact no. at 400-7071 / 400-7024 or at email address: Payments_Unit@bsp.gov.ph.</p>			
I. Agreement:		II. Approved by:	
<p>I, hereby agree to the above terms and conditions, I also agree to keep confidential all information regarding the VPN, File Transfer and Dial-up access. I will not disclose password information and/or copy the VPN and dial-up settings onto unauthorized users/computers. Propagating BSP VPN, File transfer and dial-up configuration is considered a security breach and is ground for the termination of the account.</p> <p>_____</p> <p>Signature of Authorized User</p>		<p>_____</p> <p>Head of Institution/PB (Signature over Printed Name)</p> <p>_____</p> <p>Date</p>	
(To be accomplished by BSP)			
III. Recommending Approval:		IV. Approved by:	
<input type="checkbox"/> Endorsed <input type="checkbox"/> Denied			
Authorized BSP-PSO Officer (Signature Over Printed Name)	Date	Head of ITSS (Signature over Printed Name)	Date
ITSS – DTS Ref. No.: _____			
Processed by:		Remarks:	
<p>_____</p> <p>Authorized ITIOD Officer (Signature Over Printed Name)</p>		<p>_____</p> <p>Date</p>	

How to fill-up the CONNECTIVITY REGISTRATION FORM (VPN and File Transfer Services):

Section A. Indicate in this section if the IP Address being registered is your new Static Public IP Address from your internet service provider or if it is to be added to your existing registered IP address with BSP.

Section B. Choose which system the IP address will be used for.

Section C. Select the type of connection your institution will be using.

a. Site-to-Site VPN - if you have acquired from your internet service provider a static public IP address and you have an enterprise firewall or an IPSEC/VPN-capable router.

b. Remote Access VPN - if you have acquired from your internet service provider a static public IP address and you don't have the equipments required for the Site-to-Site VPN.

Section D. Use this section only if you chose the Site-to-Site VPN type of connection. Indicate the static public IP address of your institution in the "Primary Site:" and the "Remote/Backup Site:" if you have an existing backup site.

Section E. Use this section only if you chose the Remote Access VPN type of connection. Indicate the static public IP address of your institution in the "Primary Site:" and the "Remote/Backup Site:" if you have an existing backup site.

Section F. Use this section only if you chose the Site-to-Site VPN type of connection. Indicate in this section the IP address of the workstations that are allowed to access the BSP systems from the "Primary Site:" and the "Remote/Backup Site:" if you have an existing backup site.

Section G. Use this section only if you chose the Remote Access VPN type of connection. Indicate the name and contact details of the authorized personnel to access the BSP systems.

Section H. Provide in this section the contact details of your institution's IT personnel who will serve as the point person for BSP's IT personnel to coordinate pertinent network infrastructure installations and/or configurations.

Note: For further clarifications and inquiries, kindly mail us at Payments_Unit@bsp.gov.ph