



BANGKO SENTRAL NG PILIPINAS

OFFICE OF THE DEPUTY GOVERNOR | REGIONAL OPERATIONS AND ADVOCACY SECTOR

MEMORANDUM NO. 2026-013

For : All Authorized Agent Banks (AABs)

Subject : Transition of the Cash Service Alliance (CSA) Web Application Access to the BSP Virtual Private Network (VPN)

In line with the Bangko Sentral ng Pilipinas' (BSP) continuing efforts to enhance operational resiliency and promote a more secure, reliable, and efficient digital workspace, this is to inform all AABs that the BSP's Information Technology Infrastructure and Operations Department (ITIOD) is initiating the transition of the CSA access from Citrix to a VPN-based platform with a scheduled cutover date on 08 May 2026.

In view of the foregoing, AABs are hereby instructed to undertake necessary actions and participate in the following activities to facilitate the smooth transition of access to CSA from Citrix to VPN:

A. Preparatory Activities

1. AABs shall submit to the designated local system administrators of BSP Regional Offices and Branches (ROBs), the updated and duly accomplished VPN Registration Forms in PDF format not later than 08 May 2026.

The appropriate VPN Registration Form to be accomplished shall depend on the AAB's IT infrastructure capability. Accordingly, AABs are advised to coordinate with their respective IT departments to determine the correct VPN form to be completed.

Copies of the forms are provided in the Remote VPN Form (*Annex A*) and Site-to-Site VPN Form (*Annex B*). Alternatively, the forms may be downloaded from the following links:

- a. Remote VPN Form
[https://www.bsp.gov.ph/PaymentAndSettlement/VPNForm\(Remote\).pdf](https://www.bsp.gov.ph/PaymentAndSettlement/VPNForm(Remote).pdf)
- b. Site-to-Site VPN Form
[https://www.bsp.gov.ph/PaymentAndSettlement/VPNForm\(Site-to-site\).pdf](https://www.bsp.gov.ph/PaymentAndSettlement/VPNForm(Site-to-site).pdf)

Should there be any VPN concerns/queries and/or need for further assistance, our BSP IT Support may be reached through email at BSPSupport@bsp.gov.ph.

2. AABs shall assign responsible point persons to ensure efficient coordination during enrollment, configuration, and testing activities.

B. CSA Configuration and Testing

1. The IT departments of AAB Head Offices shall coordinate with their respective branch offices on the configuration and activation of their VPN connectivity to ensure access to the CSA sites:
 - a. Primary Site
<https://csarobp.bsp.gov.ph/ROBsCashServiceAlliance/>
 - b. Secondary Site
<https://csarobs.bsp.gov.ph/ROBsCashServiceAlliance/>
2. AABs' authorized CSA users shall actively participate in the testing activities that will be conducted by the ITIOD team.
3. During the parallel testing phase, AABs shall access CSA through both Citrix and the CSA Web Portal via VPN. Given the use of two (2) portals, intermittent access issues may be encountered. Nonetheless, the BSP assures that appropriate measures will be implemented to minimize operational disruptions.

As part of the contingency protocol, should VPN access issues arise, the AABs shall be advised by BSP ROBs' local system administrators, upon confirmation from ITIOD, to temporarily revert to Citrix access. Non-compliance with the VPN onboarding requirements by the cutover date may lead to loss of system access and may disrupt operational processes dependent on the CSA ROB application.

The cooperation and timely participation of all AABs are critical to the successful implementation of this endeavor.

Any changes to the above activities will be communicated accordingly.

Should there be further clarifications to the aforementioned activities, your designated representative/s may coordinate with the designated local system administrators of the BSP ROBs or via e-mail at ROSS-SystemAdministration@bsp.gov.ph

For guidance and appropriate action.


BERNADETTE ROMULO-PUYAT
Deputy Governor

31 March 2026

Atts: A/S



BANGKO SENTRAL NG PILIPINAS

VIRTUAL PRIVATE NETWORK (VPN) CONNECTIVITY REGISTRATION FORM (Remote Access VPN)

Company/Institution Name (Registrant)		Complete Address (include zip code)	Date of Request
Registrant's User/Representative <i>(Last Name, First Name, MI)</i>	Position Title	Business Email Address	Business Contact No.

Department/Office/Unit *(Select one)*

- | | | | |
|--|---|---|--|
| ☐ Accounting | ☐ Information Technology | ☐ Trade Services | ☐ Treasury Backroom |
| ☐ Cash Operations | ☐ Remittance | ☐ Treasury | ☐ Trust |

Remote Access VPN

- | | | | |
|---------------------------------------|--|---|---|
| ☐ New VPN User | ☐ Existing VPN User | ☐ Reset VPN Password | ☐ Delete VPN Account |
|---------------------------------------|--|---|---|

Two Factor Authentication (2FA) Details

- | | | |
|--------------------------------------|--|------------------------------------|
| ☐ New Device | ☐ Retire Device | ☐ Reset PIN |
| ☐ Tablet | ☐ Tablet | |
| ☐ Smart Phone | ☐ Smart Phone | |
| ☐ Desktop | ☐ Desktop | |
| ☐ Laptop | ☐ Laptop | |

Device Operating System: Click or tap here to enter text.

Terms and Conditions:

- The requested VPN access to BSP is provided for the exclusive use of Registrant to allow access in PhilPaSS Plus Participant Browser and STP. The request is accomplished by the Registrant's authorized User/Representative and approved and signed by the Registrant's Authorizing Officer.
- The Registrant shall
 - conform to all the technical requirements of the BSP;
 - be responsible for any upgrades on hardware/software, configuration and troubleshooting to establish and support the VPN connectivity, as may be required;
 - Inform the BSP Business Department for
 - the list of active IP addresses and authorized VPN users
 - any changes in the VPN configuration five (5) days in advance to avoid disruption of the services.
- The BSP may revoke, block, or permanently disallow the use of this service without prior notice due to reasons that may compromise internal security.
- Any issues/errors encountered in the system, breach or compromise in the aforementioned application services shall be immediately relayed to BSP Payments and Settlements Department (PSD) through the contact details provided in this form.

I. Agreement

I hereby agree to the above terms and conditions. I also agree to keep confidential all information regarding the VPN. I will not disclose and/or copy the VPN settings onto unauthorized users/computers. Propagating BSP VPN configuration is considered a security breach and is ground for the termination of the account.

(Signature over Printed Name)
Registrant's User/Representative

Date

II. Authorized by:

(Signature over Printed Name)
Registrant's Authorizing Officer

Date



BANGKO SENTRAL NG PILIPINAS

VIRTUAL PRIVATE NETWORK (VPN) CONNECTIVITY REGISTRATION FORM (Remote Access VPN)

To be accomplished by BSP

III. Operational/Business Recommending Approval:

☐ Endorsed

☐ Denied

(Signature over Printed Name)

Date

Head / Approving Officer
BSP Endorsing Department/Unit

VI. Processed by:

(Signature over Printed Name)

Date

Authorized Staff
Technology and Digital Innovation Office

IV. Recommending Approval:

☐ Endorsed

☐ Denied

(Signature over Printed Name)

Date

Authorized Officer
Technology and Digital Innovation Office

Action/s Taken:

V. Approval:

(Signature over Printed Name)

Date

Authorized Approver
Technology and Digital Innovation Office



BANGKO SENTRAL NG PILIPINAS

VIRTUAL PRIVATE NETWORK (VPN) CONNECTIVITY REGISTRATION FORM (Remote Access VPN)

REMINDERS

I. Filling-up the VPN Connectivity Registration Form (Remote Access VPN)

1. Application with incomplete/inaccurate information (e.g., name of Participant user, IP address for Remote Access VPN details, applicable Application Name, etc.) will be returned to the Participant Institution.
2. The Participant Institution must accomplish one (1) VPN Connectivity Registration Form (Remote Access VPN) per user.

II. Guidelines

- A. Assistance may be requested from the IT Personnel (Network/Security) of the Participant Institution accomplishing this section.
 1. Requirements for Remote Access VPN Connectivity:
 - a. Internet Access Service (Minimum 2Mbps)
 - b. Workstation
 - c. VPN client (to be provided by BSP)
- B. Complete the Remote Access VPN and/or Two Factor Authentication (2FA) details:
 - Only one device can be registered.
 - For new VPN request, tick the "New VPN User" and specify the New Device Information for 2FA.
 - For replacement of device for 2FA request, tick the "Existing VPN User" and fill out the New and Retire Device Information for 2FA.
 - For reset of VPN password request, tick the "Reset VPN Password"
 - For deletion of an existing VPN account request, tick the "Delete VPN Account".
- C. Dormant or idle accounts for 90 days shall be deactivated.
- D. If request for reactivation is not received, the account shall be deleted after being dormant for another thirty (30) days from date of deactivation.
- E. Requests for reactivation of dormant accounts shall use the VPN Registration Form.

For further clarifications and inquiries, contact the concerned BSP Department.

III. BSP End-User Department Contact Details

BSP End-User Department	Application/System	Email Address	Contact No.
Payments and Settlements Department (PSD)	PhilPaSS Participant Browser	Payments_unit@bsp.gov.ph	8400-7071
	PhilPaSS Third Party System		8400-7024
	PhilPaSS Plus Participant Browser and STP		8400-7073
	Foreign Loan Approval and Registration System (FLARes)		
	Personal Equity and Retirement Account (PERA)		
Financial Markets - Domestic Market Operations Department	Monetary Operations System (MOS)	BSPTD-MMOS@bsp.gov.ph	8708-7020
	Liquidity Forecasting System (LFS)		8708-7042 8708-7038 8708-7047 8708-7024
Greater Manila Regional Office (GMRO)	Cash Services Portal (CSP)/ Integrated Currency Management System (ICMS)	Csd_icms-gp@bsp.gov.ph csa@bsp.gov.ph	9884-8286
	Cash Service Alliance (CSA)		8988-4853
			8708-7452
Department of Supervisory Analytics (DSA)	Financial Stability Coordinating Council – Information Sharing	fsf-eis@bsp.gov.ph	306-2889
Department of Loans and Credit	Loans and Credit Management Information System (LCMIS)	eRS@bsp.gov.ph	TL: 8708-7701
		lcmis@bsp.gov.ph	Loc 2807 or 2351
Cyber Security Group (CSG)	Governance Risk and Compliance (GRC) System	clong-iko@bsp.gov.ph	87087701 loc. 2113
Technology Risk and Innovation Supervision Department (TRISD)		mplabasan@bsp.gov.ph	87087701 loc. 2135
		macatangayds@bsp.gov.ph	



BANGKO SENTRAL NG PILIPINAS

VIRTUAL PRIVATE NETWORK (VPN) CONNECTIVITY REGISTRATION FORM (Site-to-Site VPN)

Company/Institution Name (Registrant)		Complete Address (Include zip code)	Date of Request
Registrant's User/Representative <i>(Last Name, First Name, MI)</i>	Position Title	Business Email Address	Business Contact No.
Department/Office/Unit <i>(Select one)</i>			
☐ Accounting ☐ Information Technology ☐ Trade Services ☐ Treasury Backroom ☐ Cash Operations ☐ Remittance ☐ Treasury ☐ Trust			
Site-to-Site VPN			
☐ Add IP Address		☐ Delete IP Address	
		Preferred Date of Deletion:	
A. Primary VPN Gateway Client/Host IP Address _____		A. Primary VPN Gateway Client/Host IP Address _____	
B. Secondary VPN Gateway Client/Host IP Address _____		B. Secondary VPN Gateway Client/Host IP Address _____	
C. DR VPN Gateway Client/Host IP Address _____		C. DR VPN Gateway Client/Host IP Address _____	
D. Test VPN Gateway Client/Host IP Address _____		D. Test VPN Gateway Client/Host IP address _____	
Terms and Conditions:			
1. The requested VPN access to BSP is provided for the exclusive use of Registrant to allow access in PhilPaSS Plus Participant Browser and STP. The request is accomplished by the Registrant's authorized User/Representative and approved and signed by the Registrant's Authorizing Officer.			
2. The Registrant shall - conform to all the technical requirements of the BSP; - be responsible for any upgrades on hardware/software, configuration and troubleshooting to establish and support the VPN connectivity, as may be required; - Inform the BSP Business Department for - the list of active IP addresses and authorized VPN users - any changes in the VPN configuration five (5) days in advance to avoid disruption of the services.			
3. The BSP may revoke, block, or permanently disallow the use of this service without prior notice due to reasons that may compromise internal security.			
4. Any issues/errors encountered in the system, breach or compromise in the aforementioned application services shall be immediately relayed to BSP _____ Payments and Settlements Department (PSD) _____ through the contact details provided in this form.			
I. Agreement		II. Authorized by:	
I hereby agree to the above terms and conditions. I also agree to keep confidential all information regarding the VPN. I will not disclose and/or copy the VPN settings onto unauthorized users/computers. Propagating BSP VPN configuration is considered a security breach and is ground for the termination of the account.			
(Signature over Printed Name) Registrant's User/Representative		(Signature over Printed Name) Registrant's Authorizing Officer	
Date		Date	



BANGKO SENTRAL NG PILIPINAS

VIRTUAL PRIVATE NETWORK (VPN) CONNECTIVITY REGISTRATION FORM (Site-to-Site VPN)

To be accomplished by BSP

III. Operational/Business Recommending Approval:

☐ Endorsed

☐ Denied

(Signature over Printed Name)

Date

Head / Approving Officer

BSP Endorsing Department/Unit

IV. Recommending Approval:

☐ Endorsed

☐ Denied

(Signature over Printed Name)

Date

Authorized Officer

Technology and Digital Innovation Office

V. Approval:

(Signature over Printed Name)

Date

Authorized Approver

Technology and Digital Innovation Office

VI. Processed by:

(Signature over Printed Name)

Date

Authorized Staff

Technology and Digital Innovation Office

Action/s Taken:



BANGKO SENTRAL NG PILIPINAS

VIRTUAL PRIVATE NETWORK (VPN) CONNECTIVITY REGISTRATION FORM (Site-to-Site VPN)

REMINDERS

I. Filling-up the VPN Connectivity Registration Form (Site-to-Site VPN)

1. Application with incomplete/inaccurate information (e.g., name of Participant user, IP address for Site-to-Site VPN, applicable Application Name, etc.) will be returned to the Participant Institution.
2. The Participant Institution may use one (1) VPN Connectivity Registration Form for all the end-users IP addresses. Use separate sheet for additional IP addresses as necessary.

II. Guidelines

A. Assistance may be requested from the IT Personnel (Network/Security) of the Participant Institution accomplishing this section.

1. Requirements for Site-to-Site VPN Connectivity:

- a. Internet Access Services (Minimum 2Mbps)
- b. Static Public IP address provided by Internet Service Provider
- c. Enterprise firewall or an IPSEC/VPN-capable router

B. Complete the Site-to-Site VPN details:

1. Indicate the static Public IP address of your Primary, Secondary and DR VPN Gateway.
2. Specify the static Public IP address assigned to your institution or assign one (1) Private IP address for all the participants of the system. Please refer to table below.

Private IP address range	10.0.0.0 – 10.255.255.254
	172.16.0.1 – 172.31.255.254
	192.168.0.1 – 192.168.255.254

For further clarifications and inquiries, contact the concerned BSP Department.

III. BSP End-User Department Contact Details

BSP End-User Department	Application/System	Email Address	Contact No.
Payments and Settlements Department (PSD)	PhilPaSS Participant Browser	Payments_unit@bsp.gov.ph	8400-7071
	PhilPaSS Third Party System		8400-7024
	PhilPaSS Plus Participant Browser and STP		8400-7073
	Foreign Loan Approval and Registration System (FLAREs)		
	Personal Equity and Retirement Account (PERA)		
Financial Markets - Domestic Market Operations Department	Monetary Operations System (MOS)	BSPTD-MMOS@bsp.gov.ph	8708-7020
	Liquidity Forecasting System (LFS)		8708-7042 8708-7038 8708-7047 8708-7024
Greater Manila Regional Office (GMRO)	Cash Services Portal (CSP)/ Integrated Currency Management System (ICMS)	Csd_icms-gp@bsp.gov.ph csa@bsp.gov.ph	9884-8286 8988-4853 8708-7452
	Cash Service Alliance (CSA)		
Department of Supervisory Analytics (DSA)	Financial Stability Coordinating Council – Information Sharing	fsf-eis@bsp.gov.ph	306-2889
Cyber Security Group (CSG)	Governance Risk and Compliance (GRC) System	clong-iko@bsp.gov.ph	87087701 loc. 2113
Technology Risk and Innovation Supervision Department (TRISD)		mplabasan@bsp.gov.ph macatangayds@bsp.gov.ph	87087701 loc. 2135