

4. Request for Account Creation of Virtual Private Network Access of PSA Personnel

For requests for new accounts (for requesters who do not have existing accounts for the same system).

Office or Division:	Infrastructure and Systems Management Division	
Classification:	Complex	
Type of Transaction:	G2G - Government to Government	
Who may avail:	PhilSys Registry Office	
CHECKLIST OF REQUIREMENTS	WHERE TO SECURE	
<p>1. Accomplished PhilSys Account Request Form (PARF) with the following information:</p> <p style="margin-left: 20px;">I. Type of Request</p> <p style="margin-left: 40px;">a. New Account</p> <p style="margin-left: 40px;">b. Account Updating</p> <p style="margin-left: 40px;">c. Account Reactivation</p> <p style="margin-left: 40px;">d. Account Deactivation</p> <p style="margin-left: 20px;">II. Account Holder Information</p> <p style="margin-left: 40px;">a. Last Name</p> <p style="margin-left: 40px;">b. First Name</p> <p style="margin-left: 40px;">c. Middle Name</p> <p style="margin-left: 40px;">d. Suffix</p> <p style="margin-left: 40px;">e. Designation</p> <p style="margin-left: 40px;">f. Province/Region</p> <p style="margin-left: 40px;">g. Office/Company</p> <p style="margin-left: 40px;">h. Unit/Division/Service</p> <p style="margin-left: 40px;">i. Employee ID No.</p> <p style="margin-left: 40px;">j. Contact No.</p> <p style="margin-left: 40px;">k. Email Address</p> <p style="margin-left: 40px;">l. Employment Status:</p> <p style="margin-left: 80px;">1. COSW</p> <p style="margin-left: 80px;">2. Regular</p> <p style="margin-left: 80px;">3. External/Non-PSA</p> <p style="margin-left: 20px;">III. Selection of Required Access</p> <p style="margin-left: 40px;">a. PhilSys Information System Account</p> <p style="margin-left: 40px;">b. System name</p> <p style="margin-left: 80px;">1. VPN for Step (RegClient)</p> <p style="margin-left: 80px;">2. VPN for Digital Card Service</p> <p style="margin-left: 80px;">3. VPN for Manual Verification System</p> <p style="margin-left: 80px;">4. VPN for Manual Adjudication</p>	<p>Infrastructure and Systems Management Division through the PhilSys tracking system.</p>	

5. VPN for ID Authentication System 6. Others (Please specify)	
2. Accomplished ePARF	ePARF link.

CLIENT STEPS	AGENCY ACTIONS	FEES TO BE PAID	PROCESSING TIME	PERSON RESPONSIBLE
1. Submit the filled-out ePARF (Google Form) and upload the signed PARF.	1.1. Monitor responses in the Google Form link.	None	5 minutes	Computer Maintenance Technologist I
None	1.2. Print the PARF.	None	1 minute	Computer Maintenance Technologist I
None	1.3. Check the completeness and assess the accuracy of the information in the PARF. Note: If the information is incorrect and/or incomplete, return the PARF to the requestor for correction/ completion.	None	2 minutes	Information Systems Analyst II / Computer Maintenance Technologist II
None	1.4. Endorse the PARF to the Office of the Division Chief.	None	1 minute	Administrative Assistant
None	1.5. Approve/ disapprove the received PARF and return the form to the AA for dissemination.	None	4 minutes	Information Technology Officer II and Information Technology Officer III
None	1.6. Distribute the approved PARF to designated personnel for appropriate action.	None	1 minute	Administrative Assistant

	Note: If the request is disapproved, return the form to the requestor via email.			
None	1.7. Validate details in the PARF compared to e-Responses.	None	3 minutes	Computer Maintenance Technologist I
None	1.8. Using the account monitoring sheet, transfer and label the needed information in the appropriate sheets.	None	3 minutes	Computer Maintenance Technologist I/ Computer Maintenance Technologist II/ Information Systems Analyst I
	1.9. Create Light Weight Directory Access Protocol (LDAP) account.	None	5 minutes	Computer Maintenance Technologist I/ Computer Maintenance Technologist II/ Information Systems Analyst I
None	1.10. Record the action taken, username, and the processor's name, signature, and date in Section IV of the PARF.	None	3 minutes	Computer Maintenance Technologist I/ Computer Maintenance Technologist II/ Information Systems Analyst I
None	1.11. Forward the PARF to the assigned systems administrator for Virtual Private Network (VPN) access.	None	1 minute	Computer Maintenance Technologist I
None	1.12. Provide VPN access rights using Firewall policy.	None	3 minutes	Computer Maintenance Technologist II/ Information Systems Analyst II

2. Receive the login credentials.	2.1. Send the login credentials - to the email address provided in the PARF.	None	2 minutes	Computer Maintenance Technologist I
None	2.2. Record the action taken, username, and the processor's name, signature, and date in Section IV of the PARF.	None	3 minutes	Computer Maintenance Technologist I/II
None	2.3. Forward the PARF to the assigned systems administrator sending the FortiToken activation code.	None	1 minute	Computer Maintenance Technologist I
None	2.4. Assign the FortiToken activation code via Firewall. The system automatically emails the QR code.	None	2 minutes	Computer Maintenance Technologist II/ Information Technology Officer I
None	2.5. Record the action taken, username, and the processor's name, signature, and date in Section IV of the PARF.	None	3 minutes	Computer Maintenance Technologist II/ Information Technology Officer I
3. Receive the FortiToken code via email.	3.1. Notify the requestor to download and install the FortiToken Mobile application to the user's mobile phone (Apple/ Android) and inform the requestor to use the VPN credentials and Fortitoken code to access the system.	None	3 minutes	Computer Maintenance Technologist II/ Information Technology Officer I
TOTAL:		None	46 minutes	