

New User Account Directions

To request a ProjectWise Account at Maryland's State Highway Administration you must complete the "**Third Party Remote Access**" form. Although the form states that it's for a VPN, it's also used for ProjectWise. Do not worry about tokens; those are only for VPNS.

Please follow the directions below to complete the form.

1. Complete the fields for the requestor and the company/organization.
Note: A requestor cannot sign as their Company/Organization Project Manager. If they are the project manager their supervisor should sign for them.
2. Add the requestor's **email** to the form below the **Signature of MDOT/SHA Project Manager** field. There is not a field for their email; just write it in.
3. A SHA project manager must sign off on the form.
4. The SHA project manager should then submit the form to [SHA OHD Computer Support](mailto:shaohdcs@sha.state.md.us) (shaohdcs@sha.state.md.us).
5. SHA OHD Computer Support will give the SHA project manager the requestor's login information.
6. The SHA project manager will give the requestor their login information.



Maryland Department of Transportation State Highway Administration

Maryland Department of Transportation Terms and Conditions for Third Party Remote Access Disclaimer

Access by a Third Party to the Maryland Department of Transportation (MDOT) network will be granted for lawful purposes only, limited to the scope of the service that is being provided to MDOT. Third Party users accessing the MDOT network shall not transmit, retransmit, or store material or data is the property of MDOT in violation of any federal or state laws. Specifically prohibited acts by Third Party users include?

1. Unauthorized access to or use of a computer, data or software.
2. Unauthorized copying or disclosure of data or software.
3. Obtaining unauthorized confidential information.
4. Unauthorized modification or altering of data or software.
5. Unauthorized introduction of false information (public records).
6. Unauthorized disruption or interruption of the operation of a computer.
7. Unauthorized disruption of government operations or public services.
8. Unauthorized denial of services to authorized users.
9. Unauthorized taking or destroying data or software.
10. Unauthorized creating/altering a financial instrument or fund transfer.
11. Unauthorized misusing or disclosing passwords.
12. Unauthorized breaching a computer security system.
13. Unauthorized damaging, altering, taking or destroying computer equipment or supplies.
14. Unauthorized devising or executing a scheme to defraud.
15. Unauthorized obtaining or controlling money, property, or services by false pretense.
16. Unauthorized disclosing of any info regarding MDOT network such as IP addressing, design, etc.

Any hardware or software operated by Third Party users that MDOT determines may cause hazard, interference, or service interruption to MDOT equipment, computers, or the MDOT network must be immediately removed. This equipment will only be reconnected after corrective action is taken and MDOT has determined that the threat has been minimized or eliminated.

The Third Party user, as well as the agency, firm, or organization the user represents, will be held liable by MDOT for any damage caused by intrusion, illegal or unauthorized access originating from the Third Party user, in accordance with Article 27 Section 45a and 146 of the Annotated Code of Maryland. All authorized users during the term of their access and thereafter, shall hold in strictest confidence and not willfully disclose to any person, firm or corporation without the express authorization of the MDOT Chief Information Officer, any information related to security, operations, techniques, procedures or any other security matters. Any breach of security will be promptly reported to the Director, MDOT Office of Transportation Technology Services, designee or security officer.

The Third Party user, as well as the agency, firm, or organization the user represents is responsible for the safety and integrity of any assigned security tokens. If a security token is lost, stolen or made unusable, the Company or User will immediately notify SHA and will reimburse SHA the cost of replacing the token. Current cost is \$65.00 per token.

By requesting a remote access account, I acknowledge that my remote system is protected by a firewall and appropriate virus protection. In addition, I authorize MDOT/MDTA and/or their contractor to test the security of my connection to the MDOT/MDTA network by performing random port scans.

Neither MDOT/MDTA nor any MDOT/MDTA employee is responsible for any operating system or software application problems encountered by any Remote Access User when using the designated applications to connect to the MDOT/MDTA network(s).

I acknowledge that I have read, understand and agree to comply with the foregoing security advisory.

Requestor Name Printed or Typed **DOB** **Requestor Signature** **Date**

Company/Organization Project Manager Name (Print/Type) **Company/Org. Project Manager Signature** **Date**

Company/Organization **Telephone Number**

Company/Organization Street Address **Company/Organization City, State, Zip**

MDOT/SHA Project Manager Name (Printed or Typed) **Signature of MDOT/SHA Project Manager** **Date**

Token Serial Number