DELIVERING TECHNOLOGY
THAT INNOVATES

Always On VPN (AOVPN)

Benefits Expected from AOVPN

Improved speed to connect to state services through state-issued devices
Always connected to the State network
Direct Access to resources
Improved device management
Minimal impact on users
Multi-factor authentication
Reduced Risk

AOVPN is a solution that allows our remote workers to establish a secure VPN connection with a single login. It is a seamless and persistent connection, and like an "in the office" login experience. AOVPN is only available for State-maintained Windows10 devices issued to remote workers.

Non-ITC Agencies

AOVPN is optional. If your Agency chooses to opt-in, each device must be managed and configured appropriately to maintain security requirements. The devices must have Bitlocker, KACE, and CrowdStrike installed and have all Microsoft released patches applied monthly. A Memorandum-Of-Understanding (MOU) is required for Non-ITC'd agencies that choose to opt-in for AOVPN. The MOU is intended to describe the purpose, functioning roles, and responsibilities between DTI and the Agency.

The Agency's Information Resource Manager (IRM) can reach out to your Customer Engagement Specialist/Manager (CES) if you would like to move forward with AOVPN. The CES will work with DTI's Enterprise-Desktop-LAN (EDL) Team to have a resource assigned to help your Agency's IT staff understand the AOVPN onboarding procedure and process.

ITC Agencies

State-maintained Windows 10 devices issued to remote workers will be configured with AOVPN by EDL. EDL has systematically begun updating devices that meet the AOVPN criteria. However, if there is an urgent need for a device to be AOVPN enabled, reach out to your Customer Engagement Specialist/Manager. They will work with EDL staff to prioritize the request.