REMOTE ACCESS POLICY

**Purpose:** The purpose of this policy is to define standards for requesting remote access and utilization of the State’s network resources. This policy applies to remote access connections used to conduct business on behalf of the State of New Hampshire, including application access, reading or sending e-mail and viewing internet/intranet web resources. This policy does not apply to publicly accessible State of NH websites, including those sites that support access to state resources such as e-mail.

**Policy:** Employees must request remote access from their immediate supervisor and receive agency approval from their Agency Head or designee and the Department of Information Technology (DoIT) Agency Software Division (ASD) IT Leader. Remote access is granted for business use only. Accounts will be issued only to individuals; generic and/or shared accounts are not allowed without an approved exception. Remote access accounts for non-state employees will be provided via a vendor VPN domain that provides restricted access to state resources as business justified and approved.

Remote access includes requests for terminal services and Remote Desktop Protocol (RDP) used to access devices in a remote control manner. Users connecting remotely into Payment Card Industry (PCI) environments must utilize the designated Two-Factor Authentication (TFA) solution along with the state provided VPN.

It is the responsibility of New Hampshire State employees, contractors, vendors and agents with remote access privileges to the State’s network to ensure that their remote access connection is given the same consideration as the user's on-site connection. When remote access is no longer required, a Help Desk request to remove the account must be submitted. Requests for non-state remote access must specify an account start and end date. For vendor access to PCI environments, accounts should be enabled only during the time period needed, and accounts should be monitored when in use.

Users must be physically present at the computer when remotely connected. If remote work is idle or the computer is left unattended, the user must exit and log out of all applications and disconnect the session. Computers should not be accessible by others. Passwords must not be shared with anyone at the remote location, whether at home or while traveling. An inactivity timeout, as specified in the referenced configuration standards, is implemented. Remote access/VPN software must be kept in possession of the authorized user and cannot be distributed to any other person.

Remote access is only guaranteed to the extent that the State will ensure availability of the internet components managed by the State and necessary for a VPN connection. The use of non-State-supplied equipment is not allowed except with approved exception or authorized vendor equipment. No support for the use of these devices will be provided.

Management staff can monitor remote access usage; monthly usage reports are common.

The Department of Information Technology (DoIT) has the right to revoke the privileges of the remote access account at any given time if this policy is violated.

**Accountability:** It is the responsibility of all agency heads or their designee to enforce this policy. Employees who do not comply with this policy shall be subject to disciplinary action as outlined in the Administrative Rules of the Division of Personnel.

**Description:** This policy serves to protect State network resources, systems and data.
REMOTE ACCESS POLICY

Reference:  Remote Access Procedure
            Remote Access Request Form
            SSL VPN Configuration Standards (internal)
            Personally Owned Device Policy
            IT Standards Exception Policy