STATE OF NEW HAMPSHIRE
DEPT OF INFORMATION TECHNOLOGY
TECHNICAL SUPPORT SERVICES

REMOTE ACCESS PROCEDURE

Standard #:	NHS0068.08.2022.V5
Impact:	Statewide
Effective Date:	05/15/2006
Created Date:	05/15/2006
Last Reviewed Date:	08/31/2022
Last Revised Date:	08/31/2022
Status:	FINAL
Owner:	TSS

1. PURPOSE

The purpose of this standard operating procedure is to establish a consistent procedure for requesting the use of terminal services, the Remote Desktop Protocol (RDP), or Citrix to access State of New Hampshire (SoNH) network resources or for requests to telework from devices not owned by SoNH and managed by the Department of Information Technology (DoIT). The procedure does not apply to users with SoNH owned and DoIT managed devices who have been authorized by their agency to telework. It does not apply to personal devices used strictly for multifactor authentication or for publicly accessible SoNH websites such as those that provide access to Exchange Online, OneDrive, SharePoint online, and other SoNH Microsoft 365 and Azure resources.

2. PROCEDURE

The requester must be a State of New Hampshire employee.

For users with devices managed by DoIT, requests for terminal services, RDP, or Citrix must be submitted in a fully executed Remote Access Request Form to the Helpdesk via standard agency processes for requesting system access. No DoIT approval is needed.

For requests to telework, for terminal services, for RDP, or for Citrix for users with devices not managed by DoIT:

a. Requesters must complete the Remote Access Request Form available on DoIT's Intranet. Access to Payment Card Industry (PCI) environments must be specified on the form.
b. Requesters must complete the Mobile Device User Agreement.
c. Requesters must email the completed forms to their supervisor with the subject line "Remote Access Request."
d. The supervisor must sign and email the forms to the Agency Authorized Approver.
e. The Agency Authorized Approver will:
f. verify the form for completeness and accuracy
g. Validate requested access is required and appropriate
h. Forward the forms with their authorization to the Helpdesk for ticket creation and assignment to the DoIT Cyber Security Group (CSG) for review and approval.
i. If approved, CSG will assign the ticket to the appropriate technical teams for account activation, testing, and fulfillment.

3. ACCOUNTABILITY

It is the responsibility of DoIT staff and all agency heads or their designee to enforce this procedure. Violation of this procedure may result in the denial or revocation of remote access rights to SoNH resources. Employees who do not comply with this procedure shall be subject to disciplinary action as outlined in the Administrative Rules of the Division of Personnel.

4. REFERENCE

Mobile Device Security Policy
Mobile Device User Agreement
Personally Owned Device Policy
Remote Access Policy
Remote Access Request Form