|  |  |  |  |
| --- | --- | --- | --- |
|  | STATE OF NEW HAMPSHIRE  DEPT OF INFORMATION TECHNOLOGY  TECHNICAL SUPPORT SERVICES  REMOTE ACCESS REQUEST FORM | Standard #: | NHS0069.08.2022.V9 |
| 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 |

# INSTRUCTIONS

Requestors must complete this form to use terminal services, the Remote Desktop Protocol (RDP), or Citrix to access State of New Hampshire (SoNH) network resources or to telework from devices not owned by SoNH and managed by the Department of Information Technology (DoIT). The requester must fill out the form in its entirety and email it to their supervisor. Do not send a hardcopy. Accounts will be subject to the User Account Maintenance Policy; accounts inactive for 45 days will be disabled then deleted following 60 additional days of inactivity.

# APPROVAL WORKFLOW

1. The requester must email the completed Remote Access Request Form to their supervisor with the subject line “Remote Access Request.”
2. For devices not managed by DoIT, the request must include a completed Mobile Device User Agreement.
3. If the supervisor (must be a state employee) approves the form(s), they must email them to the Agency Authorized Approver.
4. If the Agency Authorized Approver approves the Remote Access Request form, they must email both forms to the DoIT Helpdesk.
5. The Helpdesk will create a ticket and assign it to the DoIT Cyber Security Group (CSG) for review and approval.
6. If CSG approves the request, they will route the ticket to the appropriate technical teams for account activation, testing, and fulfillment.

|  |
| --- |
| **SECTION 1: User Information** |
| State Employee  Non-State Employee  State Device  Non-State Device |
| Agency:       Supervisor:  First Name:       MI:       Last Name:       Phone: |
|  |
| **SECTION 2: Non-State Device Description (go to Section 3 if using DoIT Managed Devices)** |
| Business justification for remote access from non-State owned, DoIT managed equipment:    Completed Mobile Device User Agreement provided  Computer Make:       Model:       Operating System:  Security Software:  SoNH CrowdStrike Sensor  Vendor Managed Anti-Virus  Describe the equipment’s maintenance standards and procedures:  Automated or managed monthly OS and application security updates/upgrades  Audit logging enabled  Hard drive encryption  Multi-Factor Authentication (MFA)  Other: |
| **SECTION 3: Access Requested** |
| VPN  Terminal Services  Remote Desktop  Citrix  Telework  Do you need access to a PCI environment (Requires token-based MFA)  Do you need access to other regulatory compliance environments requiring token-based MFA |
| **What devices (Hostname and IP) do you need remote access to?**    **What resources do you need to access on these devices?**  System Administration:       Applications:       Folders:       Other: |
| **SECTION 4: Approvals** |
| **Effective dates**: Start       End       (if known)  **Access Times and Days** (Required for PCI environments):  Begin Time:       End Time:       (Example: 9:00 am - 5:00 pm)  **Monday  Tuesday  Wednesday  Thursday  Friday  Saturday  Sunday**  **Supervisor:**  **Agency Authorized Approver:**  **Cyber Security Group:**       (not needed for SoNH owned, DoIT managed devices) |

# REFERENCE

Mobile Device User Agreement

Remote Access Request Policy

Remote Access Request Procedure

User Account Maintenance Policy

User Account Maintenance Procedure