

State of New Hampshire
New Hampshire Department of Transportation
Oversize/Overweight Permitting Software

RFP 2016-43
ADDENDUM No. 1

Bidders are advised to make the following revisions to the Request For Proposal.

1. NHDoIT IT Standards include the following seven documents:
 1. User Account Maintenance Procedure
 2. User Account Maintenance Policy
 3. User Account and Password Policy
 4. Administrators Account and Password Policy
 5. Application Security Scan Request Form
 6. Application Security Guidelines
 7. Administrator Account Maintenance Policy

USER ACCOUNT MAINTENANCE PROCEDURE

Purpose: The purpose of this document is to establish the standard statewide procedure for the maintenance of user accounts as specified in the User Account Maintenance Policy. This procedure applies to all state employees authorized to approve access to state network resources and the Department of Information Technology (DoIT).

Procedure: All state employees authorized to approve access to state network resources must submit a Help Desk request for user account creations, modifications and deletions. All requests should allow ten (10) business days for completion. Requests for account deletions should be submitted when the termination date is known and must specify the last effective day of employment. If a termination is unanticipated and the agency believes there is a risk with continued access, a request for "immediate termination" should be made to the Help Desk so that domain and external access can be disabled immediately. For account deletion requests, if requested in the ticket, the supervisor will be provided temporary (two week) access to review the account home directory files and mailbox contents prior to deletion. If additional review time is required, a request for an additional two week extension must be made to the Help Desk at least two days prior to the end of the initial two week review period.

A review of the last login date for all accounts will be conducted monthly within the first five business days of each month. Accounts not used in the previous forty-five (45) days will be disabled. System administrators will compile a list of disabled accounts by agency and forward to the DoIT IT Leader and the agency Human Resources (HR) and/or agency Information Security designee. For agency system application user accounts, this list should be sent to the agency information system owner for review and response. The recipients will review the list of disabled accounts to identify any accounts that should be enabled. Recipients should submit requests to enable accounts to the Help Desk. If sixty (60) days after disabling, no Help Desk request has been received to enable an account, the account will be removed and all associated files, including e-mail, will be permanently deleted.

For users identified as being on long-term leave (30 days or more), Agency HR and/or the direct supervisor should submit a Help Desk request to have the account exempt from this maintenance procedure; this will allow the account to be disabled until a request to reactivate the account is made.

Accountability: This procedure applies to all system administrators of state network resources responsible for maintaining user accounts. Enabling or reestablishment of an account must be requested via the appropriate Help Desk.

It is the responsibility of all agency heads or their designee to enforce this procedure in conjunction with the DoIT. 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.

Description: This procedure provides a common approach to the recurring task of user account maintenance.

Reference: User Account Maintenance Policy
IT Standards Exception Policy

USER ACCOUNT MAINTENANCE POLICY

Purpose: The purpose of this document is to establish a statewide policy for the maintenance of user accounts provided to authorized users of state network resources. On-going account maintenance includes the creation, modification and deletion of accounts as well as the routine review of inactive accounts by the Department of Information Technology (DoIT). This policy applies to all user accounts including remote access accounts.

Policy: All state employees authorized to approve access to state network resources are responsible for maintaining user accounts by submitting Help Desk requests for account creations, modifications and deletions. User accounts include those provided to employees and non-state workers such as contractors, vendors or other external entities.

All user accounts will be reviewed monthly. Enabled accounts not used in the previous forty-five (45) days will be disabled. If no requests have been received to enable an account within sixty (60) days after disabling, the account will be removed and any associated files, including e-mail, will be deleted. Accounts identified as exempt from this monthly procedure must be reviewed annually to determine if the exempt status is still valid.

Accountability: This policy applies to all employees authorized to approve access to state network resources and DoIT system administrators responsible for maintaining user accounts.

It is the responsibility of all agency heads or their designee to enforce this policy in conjunction with the DoIT. 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: User accounts are provided to identify authorized users of state network resources and provide access to applications, data and resources as required. In order to protect against unauthorized access, accounts must be maintained as requirements change and inactive accounts routinely identified, disabled and removed.

Reference: User Account Maintenance Procedure
IT Standards Exception Policy

USER ACCOUNT AND PASSWORD POLICY

Purpose: The purpose of this policy is to establish the account login and password policy for accounts, including e-mail addresses, for all authorized users of state network resources. This policy applies to all user accounts including remote access accounts.

Policy: The user login will consist of an account with the naming convention of `firstname.m.lastname` using the legal first name, middle initial (if exists) and last name as depicted in the NHFIRST system.

Domain accounts and state email addresses are provided only to state employees. Contractors, vendors and other non-state staff will be provided restricted access to state resources via agency approved VPN accounts.

Example: `joseph.l.smith` or `joseph.smith`. User logins are not case sensitive, but can be entered with case such as `Joseph.L.Smith` or `Joseph.Smith`.

- If there is a generational qualifier such as Jr., it will be appended to the end of the lastname. Example: `richard.l.smithjr` or `Richard.L.SmithJr`
- Names containing an apostrophe and/or hyphen will be retained in the user login. Examples: `Richard.L.O'Connor` and `Richard.A.Smith-Jones`
- Names containing periods will be ignored. Example: `Richard L. St. Pierre` would have a user login of `Richard.L.StPierre`
- In the event of a duplicate name including middle initial, the second character of the middle name will be added. Example: `john.ro.doe` or `John.RO.Doe`
- In the event of a duplicate, both without a middle initial, the account will be created with a sequential number appended to the end of the last name. Example: `john.doe2` or `John.Doe2`

Generic and/or shared accounts are not permitted without an approved exception request.

The user e-mail address will match the user login first and last name omitting the middle initial. Example: network login `John.A.Smith` and e-mail name `John.Smith@dot.state.nh.us`. In cases where duplicate names exist, the middle initial will be used. If further uniqueness is required, the rules listed above will be used.

In the event an individual is not known by their name as depicted in NHFIRST such as `Belinda.Smith` or `Seigfried.SmithJr`, one additional SMTP address may be created upon request for that person, such as `Linda.Smith` or `Sig.Smith`. Requests for this additional address should consider that an increase in daily spam notifications is likely.

A password change will be required at initial login and subsequently on a quarterly basis. Password resets also require a password change at first login.

The table below defines the password criteria and policy:

Password Criteria	Policy
Minimum password length	10 characters
Password Format	Passwords must contain three of the following four: <ul style="list-style-type: none"> • Uppercase character(s) • Lowercase character(s) • Number(s)

Page 1 of 2

NH Department of Information Technology - Office of the Chief Information Officer (CIO)
Effective - 05.04.2006

ADMINISTRATOR ACCOUNT AND PASSWORD POLICY

Purpose: The purpose of this policy is to establish uniform administrator accounts for authorized Department of Information Technology (DoIT) system administrators.

Policy: A separate account is required to perform administrative functions on network technical resources such as infrastructure devices, servers, desktops, printers, accounts, and data files. This administrator account must consist of an account with the naming convention of lastname.m.firstname using the legal last name, middle initial and first name as depicted in the Government Human Resources System (GHRIS.) All administrator accounts must be configured to provide the minimum administrative rights required to meet job responsibilities.

Due to the potential risk of unauthorized access, administrators must use this account only when performing tasks requiring an elevated level of privileges. For all other work functions, the user account must be used. Administrator accounts should be logged into monthly, at a minimum, to validate access.

The minimum password length is fifteen (15) characters. The password must contain at least one (1) upper case letter, one (1) number and one (1) special character such as !, &, and @. The password cannot contain repeating characters or any part of the account name. The password must be unique to this administrator account; it cannot match the password used for the user account. No portion of the password should contain any name easily associated with the administrator such as a nickname, family, pets, hobbies, dates, address, etc.

Accountability: This policy applies to all authorized administrators on state networks.

It is the responsibility of each DoIT Division Director and Bureau Chief 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: Administrator accounts, providing elevated rights to network resources and data, present a potential security risk to state resources and data. Separate administrator accounts and strong account passwords are designed to protect against unauthorized access to state resources and mitigate the threat of account identification and password guessing or cracking.

Reference: User Account and Password Policy
Network Administrative Privileges Use Agreement

APPLICATION SECURITY SCAN REQUEST FORM

The assessment will allow developers the opportunity to ensure that the application deployed to production meets security standards and policies established by the Department of Information Technology (DoIT).

Instructions:

Web Application Security Assessment's initial, in-depth scan shall take place in a test environment prior to moving the application into production. This is critical as parts of the scan may result in the application recording and logging events, sending emails, or adding data to the test database.

Submit the completed form as well as the findings from the Application Security Procedure to the Web Services Division (WSD).

Required Information:

Application Name:

Application URL:

Server environment (select one) Development Testing Production

Application Functionality:

Please give a quick synopsis of each distinct task within the application.

Application Access:

For each role/permission level in the application a test user account must be created for the scan. Add as many accounts as necessary.

Role/Permission	Username	Password

Application Interoperability:

If the application process flow(s) and functionality depends on the actions within another application please provide:

Application name and function(s):

The person(s) who can facilitate those actions

Name (First and Last)	Phone Number	Email Address

Session Identifiers

Cookies

Parameters

Login URLs, specify all pages by their URL that contain login forms:

Logout URL, specify the page by the URL where users go when logging out of the session:

Registration URL, specify the page by URL where a new user may register to use the application:

Change Password URL, specify the page by URL where a user may change password information:

Contact personnel for questions regarding application:

APPLICATION SECURITY GUIDELINES IN THE SDM

Purpose: The purpose of these guidelines is to ensure that security is built into the application from project concept through implementation for all applications administered by the Department of Information Technology (DoIT).

Guidelines: The guidelines listed below shall be used to consider security requirements during the planning, design, and implementation of new or enhanced applications. Applications require different levels of security; therefore all the activities below may not be necessary for any given application. The documentation requirement of each phase, however, is required for all projects.

Project Concept Phase

During the project concept phase, a risk assessment shall be made of the proposed application to determine the appropriate level of security needed to meet the business requirements of the system. The specific project needs, including security, shall be documented and approved by the agency

DoIT, in cooperation with the agency, shall evaluate the business purpose of the system for the following concerns:

- a) Identify legal and policy requirements
- b) Identify potential losses arising from accidental or unauthorized activities, poor decisions based on unreliable information, or business costs due to system unavailability
- c) Identify potential adverse customer reactions arising from system unavailability or unreliable information
- d) Document the issues identified

Project Design Phase

During the project design phase, the business needs for security must be integrated into the system design. The project's technology and processes for using the system should be examined for their ability to support the confidentiality, integrity, authorization and availability objectives identified in the Project Concept Phase. The security considerations and recommended control measures shall be documented in the project specifications and be approved by the agency.

DoIT shall conduct an analysis of the functional and design specifications to address the following concerns:

- a) Ensure individual accountability for all transaction actions
- b) Ensure incoming data are complete, accurate, and authorized before completing the transaction
- c) Assign program function and data access privileges to users on a need-to-know basis and segregation of duties principle
- d) Identify critical operations or confidential data that require special handling
- e) Ensure auditability of transactions from origination to destination
- f) Ensure audit trails meet the business and/or regulatory requirements
- g) Establish data retention/destruction requirements and provide backup and recovery procedures to satisfy business continuity requirements
- h) Document security design and specifications

ADMINISTRATOR ACCOUNT MAINTENANCE POLICY

Purpose: The purpose of this policy is to establish the uniform and secure maintenance of administrator accounts for authorized Department of Information Technology (DoIT) system administrators.

Policy: Administrator accounts will be reviewed monthly during the first full week to identify accounts not used or validated in the previous thirty (30) days. In accordance with the Administrator Account and Password Policy, administrator accounts are to be logged into monthly at a minimum to validate access. Administrator accounts not used are to be disabled and the account owner notified; the account owner and supervising manager must provide approval to enable the account.

When an administrator has a change in job duties or is reassigned to a new position, the supervising manager must review the need for and requirements of an administrator account. Accounts no longer required should be deleted. If administrator rights are still required, the account must be modified to provide the minimum rights needed to perform new job duties.

When a DoIT staff member with an administrator account terminates employment, immediately upon termination the supervising manager must submit a request to the Help Desk to have the administrator account deleted.

The built-in domain administrator account, which has been renamed per the Domain Administrator Account Policy, is to be used only when absolutely necessary. The account login and password will be entrusted to administrators on an as-needed basis. The password for this account will be changed whenever anyone who has been entrusted with the password has a change in job duties, is reassigned, terminated or no longer needs access to this account.

Accountability: This policy applies to all authorized administrators on state networks.

It is the responsibility of each DoIT Division Director and Bureau Chief 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: Administrator accounts are a target for those seeking to gain unauthorized access to network resources and data, and as such presents a potential security risk to state resources and data.

Reference: Administrator Account and Password Policy
Domain Administrator Account Policy
Network Administrative Privileges Use Agreement

2. Replace Page Nos. 27 and 49 with the revised pages respectively.
3. Replace Table C-1 with revised Table C-1. Revisions to Table C-1 included reordering of the requirements. Vendors should note that responses to Vendor inquiries pertaining to Table C-1 requirement numbers reference the requirement number in Table C-1 issued with the RFP release and may not reflect the numbering in the revised Table C-1 issued with Addendum No.1.