DEPARTMENT OF VETERANS AFFAIRS (VA)
SALT LAKE CITY HEALTH CARE SYSTEM
Salt Lake City, Utah

MEMORANDUM 142I.27 1/29/2015

AUTOMATED INFORMATION SYSTEMS ACCESS

1. PURPOSE:

This policy establishes guidelines and procedures for requesting and obtaining access to the Automated Information System (AIS) available to members of the VA Salt Lake City Health Care System (VASLCHCS) workforce.

2. POLICY:

a. It is the policy of the VASLCHCS to grant sufficient access necessary to perform assigned duties for all authorized individuals. The establishment of user accounts will be limited to the Facility CIO (FCIO) or designee(s).

b. Requests from new users for access to VASLCHCS computer systems will be made by utilizing the most recent Computer Access Request Form (Attachment A). Assignments of access/verify codes and network logon information will be made only after this written request has gone through the concurrence process as defined in this policy.

c. All users of VASLCHCS AIS will safeguard system accounts and passwords and will only retrieve information necessary to perform duties. Violations of access and security policy may result in appropriate disciplinary action and loss of access privileges.

d. All VASLCHCS AIS users will complete VA Privacy and Information Security Awareness and Rules of Behavior training in VA TMS in accordance with established Medical Center policy. This training is completed before being granted access to the system and on an annual basis thereafter in order to retain information system access.

e. The policy for specific types of access, application menus and categories of users is defined as follows:

(1) Administrator Network Access: Network Administrator access is reserved for authorized OI&T staff as determined by the R1 Elevated Privileges Request approval process

(2) Austin Access (TSO, DSS, etc.): All requests for access to Austin's databases will go through the VASLCHCS request process as defined in this policy and will be coordinated by the VASLCHCS Point of Contact (POC) or Alternate POC for Austin's Automated Customer Registration System (ACRS).

(3) Exchange: Access to MS Exchange/Outlook is granted upon request of user's care team manager/service center director or designee and is included in the Computer Access Request Form (Attachment A).

(4) CPRS access will be limited to those individuals requiring access to patient data in order to complete work assignments. Health care providers requesting access to CPRS are encouraged to complete the 1 hour introductory CPRS course taught by HRL&E.

(5) Fileman Options and File Access: The DIUSER menu option is reserved for authorized OI&T staff as determined by the FCIO. All other users will be granted the standard VASLCHCS Fileman menu upon approval. File access will be limited to only appropriate files needed in performance of assigned duties.

(6) FORUM Access: Access to FORUM will be granted upon request of the users' care team manager/service center director or designee. The FCIO or designee, will maintain FORUM accounts for VASLCHCS users to include establishing new accounts, reactivating existing accounts and deactivating accounts as part of the employee clearing process.

(7) Intranet and Internet Access: All VASLCHCS employees will be granted access to the Intranet and Internet. Users must be familiar with and comply with Center Policy Memorandum 142I.13 "Accessing Networked Information Resources."

(8) Legacy Access: Access to Legacy databases or the Data Warehouse will be based on the guidelines provided by the Office of Information National Database Integration Team and the need as determined by the user's care team manager/service center director or designee.

(9) Programmer Mode/System Manager Level Menus: Only authorized OI&T staff will receive access to programmer menu options, security keys and file access as determined by the R1 Elevated Privileges Request approval process.

(10) Public Key Infrastructure (PKI): Users that distribute data electronically will ensure that reports and other information containing sensitive data are transmitted in a secure manner using encryption. Requests for public/private keys required for encrypting Exchange messages and attachments will be submitted through the VASLCHCS FISO.

(11) Remote Access: Remote access for official purposes is provided and supported by OI&T with the intention of providing a remote method to access local information systems such as VistA, Exchange Mail, Fileman and printing services and remote Intranet access. Approved remote access users are governed under the same local and Department of Veterans Affairs policies and Federal laws and regulations that apply to all local users of VA systems, including and the security and privacy of data. Policy, and procedures for remote access are covered under Medical Center Memorandum 005R5.01.

(12) Subject to the approval of the FCIO authorized users of the VASLCHCS VISTA system may receive access to the VASLCHCS Test Account for the purpose of training and testing by submitting a request in writing to the FCIO.

(13) VMS Access: Only authorized OI&T staff will receive VMS access. VMS accounts will be established, maintained and monitored by the VASLCHCS System Administrators and Regional VMS Staff.

f. Categories of Users:

(1) AMIE: All requests from Regional Office employees for AMIE access will be coordinated by OI&T.

(2) Auditors: Auditors such as the Inspector General (IG), General Accounting Office (GAO), Joint Commission, Office of Cyber and Information Security (OCS), etc. requesting access to VASLCHCS systems must submit a request in writing to include specific access requirements. All requests for auditors' access will be forwarded to the FISO to facilitate the access process.

(3) Contractor Access: Access requests for contracted employees will be submitted by the Contracting Office(C)/Contracting Officer Representative (COR) to the FISO for review and concurrence. Access assignments will be coordinated with appropriate VASLCHCS staff and will be based on the requirements as written in the contract. Contractors requiring access on a temporary basis for the purpose of troubleshooting medical devices problems or maintaining VASLCHCS computer systems will be coordinated with the FCIO and FISO. Those contractors requiring remote access will do so by following the instructions in Medical Center Memorandum 005R5.01

(4) IT/CWT: Based on the provisions of the Privacy Act, IT/CWT workers will not be granted access to patient data and are not to be allowed unattended in areas where the opportunity to access patient information could arise.

(5) Residents/Students/interns/trainees: Trainees approved for access to VASLCHCS systems must obtain a Without Compensation (WOC) status as required for other non-traditional employees. Trainees are governed under the same policies and regulations that apply to VASLCHCS staff.

(6) VBA (HINQ; IBBA): Employees that require access to HINQ or BDN/BIRLS must have received approval from their care team manager/service center director or designee and submit requests to the facility point of contact for processing.

(7) Veterans/Patients/Family Members: Veterans, Patients, family members and the general public will not be allowed access to VASLCHCS networked computers unless they have authorization by the FCIO and FISO.

(8) VHA Office of Information (OI) Support Staff: Authorized national support staff may obtain access to VASLCHCS computer systems upon approval by the FCIO.

(9) Volunteers and other Non-Traditional Users: Individuals such as volunteers that are not covered under a paid program and work as a VA employee should have a WOC status. Volunteers are governed under the same policies, laws and regulations that apply to all VASLCHCS computer users by submitting a Computer Access Request Form (Attachment A) and completing VA Privacy and Information Security Awareness and Rules of Behavior training.

3. RESPONSIBILITY:

a. The FCIO is responsible for establishing and maintaining user accounts for VASLCHCS systems as defined in this policy.

b. Care Team Manager/Service Center Directors (or designees) are responsible for ensuring that users within their Care Team/Service Center have access to only the information required to carry out their assigned duties and that access privileges of terminating and transferring staff are rescinded. This is accomplished by having the ACCESS REVIEW menu option as described in Attachment B. A Semi-Annual Menu Management review is required and documented per Attachment C. The Semi-Annual Menu Management attachment is forwarded to the FISO for review who then forwards to OI&T for completion.

c. The FISO is responsible for facilitating the access process, and will coordinate the monitoring of systems and user activity.

d. All individuals who use or gain access to VA information systems or sensitive information must adhere to VHA and VASLCHCS policies to include protection of individual user accounts, patient confidentiality, access to sensitive data and appropriate use of the Inter/Intranet and electronic mail.

4. PROCEDURES:

a. Request Process.

(1) New User: A new user who does not already have access to the VASLCHCS Vista or network system will submit a Computer Access Reqeust Form signed by the user's care team manager/service center director. In the case of trainees, the Director of the trainee's training program may sign the request.

(2) The completed computer access form will be forwarded to the FISO's five working days in advance of needing access. The FISO will then forward to the OI&T staff who will enter all pertinent information into the "New Person File". OI&T staff will assign a new user account, user access codes and standard menus for the appropriate job. Signed forms processed by OI&T staff will be kept on file.

(3) Users will obtain their access and user codes in person during New Employee Orientation as outlined in HR Policy 05.03. A valid VASLCHCS identification badge will be needed to obtain these codes.

(4) Existing User/Additional Access: Requests for additional access by users that have an active Vista or network account and need additional access to perform job responsibilities (i.e. menu option, file access, security key, additional database, etc.) by submitting a new Computer Access Request Form (Attachment A) with concurrence by the user's supervisor to OI&T or by the supervisor e-mail to VHASLCAccountManagement. Additional menu options will be assigned by the OI&T Account Mangement staff member responsible for maintenance of the particular package.

(5) Remote Access: All requests for remote access will follow the procedures outlined in Medical Center memorandum 005R5.01.

(6) Austin Access: An Automated Customer Registration System (ACRS) request will be submitted to the FISO for all Austin access needs using form VA9957. This includes: Add New Customer, Modify Existing Customer and Delete Existing Customer. The FISO will then forward the form to OI&T staff for processing.

b. Processing Requests:

(1) The OI&T staff will create a new user account on all systems where access for the user has been approved. Access assignments will be limited to only those that have been approved by the concurring officials.

(2) The user will be assigned an access code and the user will assign his/her own verify code. These will then be the standard codes for that user in all appropriate VISTA systems at VASLCHCS. The System Access Administrator(s) will establish new and reactivated VISTA accounts to include, at a minimum, the following information.

(a) Name in the following format: LAST NAME, FIRST NAME, MI.

(b) Social Security Number

(c) Initials

(d) Nickname (first name of user)

(e) Title

(f) Mail Code

(g) Primary Menu

(h) Care team/Service Center

(i) Timed Read

(j) Office Phone

(k) Person Class (if needed)

(l) Termination date for users with a temporary or volunteer status

(3) Network Account: OI&T will establish network accounts for new users to include the following information:

(a) Username - Follow VHA standards

(b) Full Name - LASTNAME, FIRSTNAME Ml

(c) Comments - (Drives)

(d) Title: Appropriate Title

(e) Extension: Phone extension

c. Distribution of Access and Verify Codes:

(1) Access codes will be provided by OI&T to the user in a secure manner. Users will be required to establish a new verify code (also known as passwords) upon first entering the system, and must be in a format determined by the FCIO. Verify codes are required to be changed every ninety days.

(2) OI&T staff will verify the demographic and access information contained on the request with the user to ensure accuracy.

(3) All users must complete VA Privacy and Information Security Awareness and Rules of Behavior training prior to receipt of assigned codes.

(4) Users will be instructed to assign their own electronic signature upon receipt of assigned codes.

(5) Users are responsible for protecting their individual Network account by preventing unauthorized access and are required to log off the system before leaving work areas unattended.

(6) Time-out: To prevent unauthorized access to unattended work stations Timed Read will be set as follows:

(a) Individuals not engaged in direct patient care - 600 seconds

(b) Health care providers not in mental health – 900 seconds

(c) Health care providers in Mental Health – 2700 seconds

(d) Exceptions will be handled on a case-by-case basis, require justification and should be submitted to the FISO for concurrence.

(7) Menu Options: The OI&T staff will assign appropriate menu options at the time access and verify codes are assigned. See paragraph 4.a. (4) above for requesting additional menu options.

d. Removing System Access (Transfers/Terminations)

(1) Terminations: The care team manager/service center director or designee is responsible for notifying OI&T personnel when the user has been removed from his/her position or assigned to a new position. OI&T will be included in the facility-wide clearance process per Policy 05.11 to ensure the prompt removal of access. User accounts inactive for more than ninety days will be deactivated in accordance with VHA policy. Access privileges can be revoked at anytime without warning in the event that the integrity of VASLCHCS systems or data is compromised.

(2) Emergency terminations will be communicated to the FISO and FCIO by a Pentad Member or HRL&E Manager.

(3) Transfers: To ensure menus reflect current responsibilities, Service Chiefs or their designee will notify the OI&T staff when the user has been removed from, or assigned to, another position. Access no longer needed at the time of transfer will be removed from all systems where an active account exists (i.e. Vista, Legacy systems, Austin, etc.)

(4) It is OI&Ts responsibility to promptly deactivate accounts on all systems the transferred/terminated user has access to.

(a) VISTA Accounts: Deactivation of VISTA accounts will include deleting menus, security keys and e-mail.

(b) Network Accounts: Exchange mail will be deleted and network accounts will be terminated.

(5) OI&T Employees and Special Users: The clearance procedures for staff that have high level access (i.e. programmers, computer room access, etc.) include the following in addition to the established clearance procedures for all users.

(a) Users of VMS accounts will be deleted.

(b) VISTA accounts will be terminated and programmer security keys and File Manager Access Code removed.

(c) Access codes will be disabled and keys allowing physical access to computer room, telecommunication closets and demarcation points will be retrieved.

(d) VMS configuration management passwords will be changed at the time a System Manager clears.

(e) Appropriate network passwords will be reset for all administrator-level accounts the clearing network administrator has access to.

(f) Office of the Inspector General Information Security Officer will be notified that the Certificate of Eligibility granted to those holding sensitive positions can be revoked.

e. Name Changes: When a user undergoes a legal name change, the system administrator, or designee, will make appropriate modifications to all accounts where the user has access. The user's former name will be added as an alias name whenever possible. Name change is to be verified with user's SF50 from HRL&E.

f. Unknown Social Security Number (SSN): A paid user that has not yet received an official SSN will need to have a pseudo-SSN assigned by Human Resources before the user account is created. The user's account will be updated by the system administrator, or designee, to include the official SSN when it is available.

5. REFERENCES:

a. VA Handbook 6500, Risk Management Framework for VA Information Systems
b. Medical Center Memorandum 142I.13, Accessing Networked information Resources
c. Medical Center Memorandum 005R5.01, Remote Computer Access Policies and Procedures
d. Medical Center Memorandum 05.03, Employee Identification Badges

6. RESCISSIONS: Center Policy Memorandum 142.27, “Automated Information Systems Access Policy,” dated December 9, 2014.

7. AUTOMATIC RESCISSION DATE: 1/29/2018

8. FOLLOW-UP RESPONSIBILITY: Facility Chief Information Office (142I)

/S//
STEVEN YOUNG, FACHE
Director

Attachments:
A. Computer Access Request Form
B. Access Review Menu Otpions for Supervisors/Managers
C. Semi-Annual Menu Management

ATTACHMENT A
COMPUTER ACCESS REQUEST FORM

Computer Access
Request Form.pdf

ATTACHMENT B

ACCESS REVIEW MENU OTPIONS FOR SUPERVISORS/MANAGERS

Menu [ARF ACCESS REVIEW] ACCESS REVIEW -

This option will show all the menus key and mail groups that someone has. You can only look up one person at a time
NAME: XUSERINQ MENU TEXT: User Inquiry
TYPE: inquire CREATOR: LUDEMA,JOHANNES
HELP FRAME: XUUSER-INQ
DESCRIPTION: This option displays various user attributes. If the user is currently signed on, it displays the job and device numbers, the sign-on time, and what option is being executed. Otherwise, it displays the last sign-on time. It also displays which keys are held by this user.
DIC {DIC}: VA(200, DIC(0): AEMQ
FLDS: [XUSERINQ] IOP: HOME
DIC {DIQ}: VA(200, TIMESTAMP: 54921,52897
TIMESTAMP OF PRIMARY MENU: 61836,30119
UPPERCASE MENU TEXT: USER INQUIRY

This option will show all of the keys a person has as well as keys that the user can delegate.
NAME: XQLISTKEY MENU TEXT: Show the keys of a particular user
TYPE: run routine CREATOR: LUDEMA,JOHANNES
DISPLAY OPTION?: YES
DESCRIPTION: This option will list the keys held by a particular user.
ROUTINE: LIST^XQ6 TIMESTAMP OF PRIMARY MENU: 61486,27644
UPPERCASE MENU TEXT: SHOW THE KEYS OF A PARTICULAR

This option will show all of the EMPLOYEES that have a certain key.
NAME: XQSHOKEY MENU TEXT: List users holding a certain key
TYPE: run routine CREATOR: LUDEMA,JOHANNES
DISPLAY OPTION?: YES
DESCRIPTION:

This option will display all the holders of a certain key.
ROUTINE: SHOW^XQ6 TIMESTAMP OF PRIMARY MENU: 61802,32440
UPPERCASE MENU TEXT: LIST USERS HOLDING A CERTAIN K

This option will list all users that can access an option
NAME: XUOPTWHO MENU TEXT: Option Access By User
TYPE: run routine CREATOR: LUDEMA,JOHANNES
HELP FRAME: XQOPTWHO
DESCRIPTION: This option prompts for a menu option, then prints of a list of which users can access this option. The list can be printed with or without the menu paths to the option.

ATTACHMENT C

GEORGE E WAHLEN VA HEALTHCARE SYSTEM
SEMI-ANNUAL MENU MANAGEMENT
VISTA AND NT SYSTEMS

Service:_____

Fiscal Year: Quarter: Mail Code:

I certify that a Menu Management review has been conducted for all employees in the above service, and that all employees within the service currently hold computer access limited only to those menu options required to do the job to which the individual is assigned. To accomplish this, the following changes were required:

☐ The review was completed and no changes were necessary.

☐ The following employees have been submitted for deletion – VistA or network:
*(list names or attach a separate document**; indicate which system to deactivate**)*

☐ The following employees have transferred to another service. *(list names or attach a separate document).*
☐ I have attached a list of users/options for OI&T action.

☐ The following employees require menu/security key changes as a result of this review:
(list names or attach separate document)
☐ I have attached a list of users/options/keys for OI&T action.

☐ I have reviewed all users within the service for accuracy of Person Class and Degree Field designations. I have requested changes through OI&T as necessary.

_____ _____
Reviewer Date Service Chief Date