Information Management Division (IM) Procedure: Logical Access Control

Title: IM Procedure: Logical Access Control

Intent: To establish procedures on Logical Access Control which includes authentication, account management, password management and remote access along with Access Determination Control to restrict access and Acceptable Use requirements.

To establish a procedure for the Department of Medical Assistance Services (DMAS) that will:

A. Ensure that all computer information resources and those handling such resources and computer data and/or those about which such data pertains, including the Agency itself, are fully protected to the greatest possible extent from unauthorized access, use, modification, copying, and destruction.
B. Promulgate guidelines at DMAS which will ensure that access to all information systems within the Agency is fully protected to the greatest possible extent.
C. Allow authorized extraordinary management access to information in the files of Agency personnel on DMAS information systems.
D. Establish procedures at DMAS which will ensure that access to the sensitive data processed in the Medicaid Management Information Systems (VaMMIS) is fully protected to the greatest possible extent.

Scope: Logical Access Control is utilized to protect the confidentiality, integrity and availability of DMAS IT systems and data against compromise (as specified in the DMAS IT Security Policy dated May 21, 2007, Section 3, IT Security Program, 3.1.4 Logical Access Control, page 9 and 3.1.7 Personnel Security, page 10).

Responsibilities: IM staff will follow these procedures as needed to comply with logical access control requirements to protect DMAS.

Designated IM security staff will follow these logical access control procedures to protect DMAS as well as document system access changes made to user accounts.

Sequence of Events:

- IM security staff receives a completed access request form.
- The IM Security Engineer reviews the completed form to verify appropriate approving signatures are in place, to check and determine appropriateness for what is requested to be assigned, and signs off on the paperwork once the request is

completed. Paperwork is filed in the user's access documentation folder.

- This documentation is used by IM to verify access requested, and to demonstrate to auditors that what is assigned is what was requested and approved.
- Access information is logged in the IM Security database to track access assigned.

Change requests follow the same process.

Delete requests are processed by inactivating the user access, then logging the information in the IM Security database, and finally filing the paperwork for audit purposes.

Approvals: The initial completed form is received and processed.

Prerequisites: Employees must have signed all the necessary forms to request logical access to DMAS systems.

Definitions: Resources: Includes all end user access and use, computer systems along with desktops, portable devices, remote devices, workstations or connections to these, along with all data, output, software, and applications, including documentation associated with their use. For the purposes of this procedure, the terms "information resources", "computing resources" and "assets" are synonymous with the term "resources".

Employee: For the purpose of this procedure, the terms "employees", "contractors", "consultants", "temporary employees", "hourly employees", "wage employees", "interns", or anyone who performs work on behalf of DMAS are synonymous.

File: includes any means of storing information an any DMAS information system.

Transaction: VaMMIS screen assigned to a user.

Cluster: a grouping of transactions assigned for a user to access.

Equipment, Tools, Documentation Required:
Employees must have signed all the necessary access request forms to request logical access to DMAS systems.

Warnings: IM staff may not assign access without completed forms in place for documentation purposes.

Precautions: Remember to check for approving authorizing signatures according to the Authorized Supervisor List before assigning access rights.

Remember to check for any requirements that must occur, such as HIPAA security awareness training, prior to assigning network rights to user access.

Remember to refer to the Internal Checklist to ensure compliance with all user rights' assignments.

Procedure Body: The following statements are applicable:

A. The protection of assets and resources is an individual responsibility. All employees are responsible for the assets and resources within their areas of control. Each employee shall monitor conditions affecting DMAS (Agency) assets and resources, identify deficiencies to supervisory personnel, and take action to preclude the damage or loss of the asset or resource.
B. All employees shall read and sign the INFORMATION SYSTEMS SECURITY ACCESS ACKNOWLEDGEMENT AGREEMENT prior to being granted access to any DMAS information resource.
C. Management responsibilities of the managers and directors include assessing Commonwealth, Agency, and Division security policies and the protection offered Agency assets, and taking corrective action where applicable.

<u>DIRECTORS AND MANAGERS SHALL:</u>

A. Communicate to employees a positive security attitude to ensure their recognition of the importance of security.
B. Maintain employee security awareness and understanding of their security responsibilities through frequent communication, counseling, and appropriate remedial action where security infractions occur.
C. Ensure proper classification and control of all company information in accordance with Commonwealth, Agency, and Division security policies.
D. Conduct timely reviews of asset protection programs in areas of control and initiate prompt corrective action when security exposures are identified.
E. Contact organizational unit responsible for security assistance as required.

F. Investigate and report to DMAS management serious security violations ensuring that all assets are returned, and appropriate corrective action taken.
G. Notify the Information Management Division (IM) of persons transferring within or leaving the Agency to ensure that their security logon IDs and/or authorizations are suspended/deleted from the security control systems in a timely fashion. The Human Resources Division is responsible for notifying the IM Division of any vacating employees and their employment end date.

SYSTEMS ADMINISTRATORS OF EACH PLATFORM IN USE AT DMAS SHALL:

A. Ensure use of access control mechanisms to restrict user access to appropriate system resources (i.e., subsystems, applications systems, data files, tapes (or other media), commands, utilities, etc.).
B. Not grant access to applications or data without the expressed authorization from the owning division along with the appropriate authorizing signatures on the security request form.
C. Establish and enforce necessary procedures for internal and external users to access agency information resources.
D. Establish and provide to each user unique and individual access mechanisms to information resources.

EMPLOYEES ARE ACCOUNTABLE TO THE FOLLOWING:

A. Any person who possesses sensitive information, or who uses a computer system to process sensitive information (in any way and in the broadest possible sense), shall be responsible for the safeguarding of that information and shall be accountable as such to the appropriate authority.
B. Any person who uses a computer system that processes sensitive information, whether or not that individual is himself processing sensitive information, shall be responsible for ensuring that his actions, or any other actions taken with his knowledge, do not serve to degrade or otherwise compromise the integrity of the computer system so as to lead to violation of this or any other approved policy regarding computer or information security.
C. The use of computer systems to process sensitive information is intended to augment human capability, but it is in no way intended to replace, circumvent, or otherwise render obsolete the basic concept of an individual's human accountability, and the appropriate authority shall certify that the spirit of this concept has been retained to the maximum extent possible.

D. Each person who is assigned a sign-on (logon) ID and password is responsible for all use of that sign-on and should not loan it to other individuals. Loaning includes signing on under your ID and password for someone else's use on a particular workstation. Each user must change all passwords at least once every 30 days, more frequently if deemed necessary.
E. All employees shall read and sign the INFORMATION SYSTEMS SECURITY ACCESS ACKNOWLEDGEMENT AGREEMENT prior to access to any internal or external DMAS information resource or the granting of logon IDs and passwords.
F. All employees that are users of the Virginia Information Technologies Agency (VITA) host computer system shall abide with VITA policies. Included in this, all employees shall read and sign the Information Security Access Agreement (VITA Form ISAA) prior to access to any VITA information resource or the granting of logon IDs and passwords.

COMPLIANCE:
Access to, and use of, information systems is restricted to appropriately identified, validated, and authorized users. DMAS information systems are to be used only for DMAS Agency business unless explicitly authorized by appropriate management. All users must submit a DMAS Information Systems Security Access User Acknowledgment Agreement form prior to gaining access to any DMAS information system.

All identification, passwords and other access means to computing resources are proprietary and confidential to DMAS. Holders of such access means are accountable for unauthorized or negligent disclosure or use of access means under their control. No individual may use access means in his/her possession to access data or other information systems that are not authorized for that individual on a need-to-know basis.

Internet access can be granted to authorized users of DMAS Computer Networks under the following conditions:
A. Each employee acknowledges receipt of the DMAS Human Resources Policy No. 10, Use of Internet and Electronic Communications Systems, dated December 5, 2007 (or latest);
B. Internet access is exclusively for DMAS business use as defined in the Policy 10 mentioned above;
C. Usage of DMAS systems and Internet activity is monitored and a security firewall is in place to provide data security for the network;

D. Users provided with Internet access agree to comply with the highest standards of professional conduct in Internet activity;
E. Users agree to limit access to the minimum required to perform their job functions, are conservative in network resources used in this activity;
F. All users must submit the Internet Access Request Form prior to using Internet resources.

All computer programs, software, and electronic information that are part of information systems are proprietary to DMAS and must not be copied or disclosed unless explicitly authorized by appropriate management.

No software or its related documentation, licensed to DMAS, may be copied unless explicitly authorized by the software developer. With regard to use on local area networks or multiple machines, employees shall use the software only in accordance with the license agreement.

No hardware or any type of telecommunications device can be connected to any part of the DMAS information systems network, computers, terminals, or telecommunications lines unless explicitly authorized by appropriate management and in conformance with other DMAS security policies, standards and procedures.

No software program or information can be added to, or removed from any operating system, database or file unless explicitly authorized by appropriate management and in conformance with DMAS security policies, procedures, and standards. Additionally, software that bypasses (in any manner) approved DMAS security software or controls, may not be written, installed or utilized.

Employees shall not disclose any secret or confidential information unless this is properly required in their job function, or except as authorized in writing pursuant to DMAS policy. Such information includes technical and business information about the Agency, information systems or software development, and products or software licenses disclosed on a confidential basis by third parties to DMAS.

Upon termination of employment, employees must surrender all property and information managed by DMAS to the appropriate cognizant authority and notify the IM Security Engineer or Agency Information Security Officer of their last date of employment, in order that user access is suspended/deleted in an efficient and timely manner. This notification can be from the employee,

supervisor, manager, DMAS Contract Monitor, Division Director and/or Human Resources Division.

EXTRAORDINARY MANAGEMENT ACCESS:
Authorized extraordinary management access is accorded in three levels:

(A) Granting file access: The Agency Director, Chief Deputy Director, and/or Deputy Directors have the authority to grant access to any DMAS file for the purpose, as determined by the person fulfilling one of the aforementioned positions, of safeguarding DMAS and Agency assets. Managers and supervisors may request access to any file(s) of personnel under their direct authority. Access to a person's file(s) outside of a supervisor's or manager's authority shall be approved by the Division Director responsible for the files (known as the system or data owner), a Deputy Director, Chief Deputy Director or Agency Director.

Access shall be modified by using the following procedures:
(1) In order to request to revoke a logon ID to the DMAS information systems for a user, the Requester will be in the direct supervisory chain of that user.
(2) Supervisors of personnel are the originating authority for personnel access to DMAS information systems. Supervisors have the authority to revoke access at any time to safeguard DMAS information systems by using the following procedures:

The requester will submit a signed memo or send an email message (and any other supporting documentation necessary, such as a signed Systems Security Access Request Form, if required) to the IM Security Engineer or Agency Information Security Officer, the systems administrator, the IM DP Operations Manager, or the IM Division Director. The IM DP Operations Manager and/or the IM Division Director will forward the request to the IM Security Engineer, Agency Information Security Officer or the systems administrator to have the action requested performed. The requester will provide the user's name, systems affected, and, if needed, date of revocation and date to restore logon access.

Revocation of Logon Access – for the IM Security Engineer, Agency Information Security Officer or Systems Administrator

1. To revoke a logon access to DMAS information systems for a user, the IM Security Engineer, Agency Information Security Officer or systems administrator shall ensure the requester is in the direct supervisory chain of that user.

2. The IM Security Engineer, Agency Information Security Officer or systems administrator shall receive a signed memo or email message (and any other supporting documentation necessary, such as a signed Systems Security Access Request Form if required) from the requester. The requester will provide the user's name, systems affected, and, if needed, date of revocation and date to restore logon access
3. The IM Security Engineer or Agency Information Security Officer will keep on file the memo or email message (and any other supporting documentation necessary, such as a signed Systems Security Access Request Form) submitted for at least three years or audit, whichever is first.
4. The IM Security Engineer, Agency Information Security Officer or systems administrator will direct any inquiries from the user or any other personnel about the loss of access to their immediate supervisor, manager, or Division Director as appropriate.

(B) Authorized Extraordinary File Management Access – for the Requester

1. To request access to a user's file(s), the requester shall be in the direct supervisory chain of that user or have the approval of the Division Director, Deputy Director, Chief Deputy Director or Agency Director.
2. The requester shall submit a signed memo or email message (and any other supporting documentation necessary, such as a signed Systems Security Access Request Form if required) to the IM Security Engineer, Agency Information Security Officer or systems administrator. The requester will provide the user's name, systems affected, files, and date range when the extraordinary access is needed. Unless explicitly instructed in the memo (or email message and/or supporting documentation) to do otherwise, the user will be notified of the granting of this access. The non-notification of the user will require Division Director, Deputy Director, Chief Deputy Director or Agency Director approval.

(C) Authorized Extraordinary File Management Access - IM Security Engineer, Agency Information Security Officer or Systems Administrator

1. To request access to a user's file(s), the IM Security Engineer, Agency Information Security Officer or systems administrator shall ensure that the requester is in the direct supervisory chain of that user or has the approval of the Division Director, Deputy Director, Chief Deputy Director or Agency Director approval.

2. The IM Security Engineer, Agency Information Security Officer or systems administrator shall receive a signed memo or email message (and any other supporting documentation necessary, such as a signed Systems Security Access Request Form if required) to the IM Security Engineer, Agency Information Security Officer or systems administrator. The IM Security Engineer, Agency Information Security Officer or systems administrator will require the user's name, systems affected, files, and date range when the extraordinary access is needed.

   Unless explicitly instructed in the memo (or email message and/or supporting documentation) to do otherwise, the IM Security Engineer, Agency Information Security Officer or systems administrator will notify the user of the granting of this access. The non-notification of the user will require Division Director, Deputy Director, Chief Deputy Director or Agency Director approval.

3. The IM Security Engineer or Agency Information Security Officer will keep on file the memo or email message (and any other supporting documentation necessary, such as a signed Systems Security Access Request Form) submitted for at least three years or audit, whichever is first.
4. The IM Security Engineer, Agency Information Security Officer or systems administrator will direct any inquiries from the user or any other personnel about the granting of access to their supervisor or Division Director as appropriate.

VIOLATION OF THIS PROCEDURE

A. It is the responsibility of every employee to report any suspected or confirmed violations of this procedure to his or her manager or to the Information Management Division. Reports may be oral or written.
B. Any employee violating security access is subject to the Commonwealth's Code of Conduct. In addition, there may be cases in which an employee may be subject to civil or criminal legal sanctions when a violation occurs.

LOCAL AREA NETWORK (LAN):

A. System Software Controls: System software controls will apply to the Local Area Network (LAN) operating system and associated software, including security software and communications software. These controls are executed by the system administrators and cover granting access, program security and data file security.

B. Network Development: The LAN Administrator develops plans for the hardware, software, and design; both physical and logical. Contact the Information Management (IM) DP Computer Operations Manager for identification of the systems administrators and/or any of the HelpDesk staff.

C. File Access Security: Users of the DMAS LAN have Read, Write, Create, Erase, Modify, and File Scan capabilities in their assigned Home directories which are mapped as N:. Likewise, Shared Groups on the LAN have Read, Write, Create, Erase, Modify, and File Scan capabilities in their own shared Group directories which are mapped as J:.

The DMAS Agencywide Shared Group, DMAS-Share, has Read, Write, Create, Erase , Modify, and File Scan to the shared Agencywide "public data" directory (K:).

D. Passwords: Every user on the LAN must maintain an individual password. All passwords are encrypted, and not even the System Administrator can access them. The following password criteria are:

1. Passwords must be 8 characters in length, and expire after 39 days, at which time the user must supply a new, unique password.
2. Users are given five "grace" logons from the time their password expires to establish a new password.
3. The password field will not allow the user to repeat the last password used.
4. After the grace logon period, users are prohibited from accessing the LAN and must contact the DMAS HelpDesk for assistance to re-gain access to the DMAS LAN.

E. Logon Attempts: If a user unsuccessfully attempts to logon five times within thirty minutes, he/she is locked out from accessing the DMAS LAN, and a message is given in the error/intruder lockout file. The HelpDesk must take action for that user to be allowed to use the LAN. Contact the IM DP Computer Operations Manager for identification of the systems administrators and/or any of the HelpDesk staff.

F. Protected Root Directories: All directories on the LAN created by the System Administrator have been both delete inhibited and rename inhibited. This prevents directories that are critical to the LAN from being removed or renamed. Should a directory of the file somehow become removed, backups are performed on a nightly basis and can be used for restoration purposes.

VaMMIS ACCESS COMPLIANCE:
Access to and use of the Medicaid systems is restricted to appropriately identified, validated and authorized users.

(A) The Requesting Agency Responsibilities: To be an authorized user, the supervisor and security officer of the requesting agency surveys the employee's need to determine what transactions he/she needs to perform (update or inquiry) in VaMMIS.

The supervisor, security officer and the employee needing access to the systems are required to complete the DMAS VaMMIS Security Access Request Form. (This form is available online or can be obtained by contacting the DMAS IM Security Engineer.) Once the form is completed, it is to be sent to the address on the form, or if the sender is in the local area, can be sent via sealed inter-office mail courier to the DMAS IM Security Engineer for review and processing.

The originating supervisor and/or originating agency information security officer (ISO) is responsible for providing initial training information to the approved user.

(B) DMAS IM Security Engineer Responsibilities: The DMAS IM Security Engineer will:

1. Verify the accuracy and completeness of the Security Access Request form, including validating the security officer's name, and will review the transactions requested for appropriateness.
2. Provide approving signatures for continuation to the next step of the process.
3. The approved request form is processed, a cover memo requesting what actions are needed is created and the package is forwarded to the Fiscal Agent's Security Administrator for final inclusion in the ACF2 Security System.
4. Will return account information to the security officer, supervisor, and/or employee along with related security instructions for use of the account.
5. Handle password resets of suspected or confirmed password violations, account suspensions and cancellations of logon IDs, and resolve any access problems the intended user may have.

Emergency Access: This is to establish and implement as needed, emergency logical access to obtain necessary electronic protected health information (PHI) access during an emergency, (i.e., system downtimes of less than 12 hours). DMAS Management will take manual action to verify user requests for logical access using the latest version of DMAS' List of Authorizers for Systems Access Control. This Authorizers List provides the authority for DMAS Management to identify who may or may not be granted logical access on a normal or emergency basis.

In the case of a power failure, though, DMAS would wait until such time as power has been restored to the Computer Center, then initiate restore procedures (as listed in the Backup Procedure) as needed.

Exceptions: Any exceptions will be made on a case-by-case basis, will be documented and approved by DMAS Management prior to implementation.

Recommended Date: **January 22, 2008**

Required Signature: _____
Theresa L. Fleming
IM Security Engineer

Reviewed by:

Required Signature: _____
Craig J. Goeller
DP Operations Manager, AITR

Authorized by: **January 22, 2008**

Required Signature: _____
Sylvia E. Hart
Division Director, Information Management

Effective Date: **January 22, 2008**

Review to occur every 2 years from date of issue or major systems upgrade / change.