Name of Standard: CWM Access Control

Responsible Departments
UMMS Office of Management (OoM), and
UMMS IT Information Security Office
OoM Contact: PrivacyandCompliance@umassmed.edu or 508-856-TEAM
IT Contact: 506-856-8643 (IT HelpDesk)

STANDARD STATEMENT

Managing access to Information Systems is one of the most important elements of an information security system. CWM is committed to protecting its applications, information assets, financial systems and IT resources (hereinafter “Information Systems”) from improper or unauthorized access through the implementation of controls and continuous oversight to restrict and monitor such access. No CWM Information Systems shall be accessed by anyone who does not need to access the system, or the information contained in the system to perform the responsibilities associated with the individual’s assigned work. Access to Information Systems must include a process for documenting appropriate authorization before access is provided.

REASON FOR STANDARD

To provide a framework for CWM to control access to Information Systems to avoid fraud or errors and mitigate the risk of threats or incidents that compromise the confidentiality, integrity or availability of Personally Identifiable Information and/or Protected Health Information (collectively referred to as “PII” in this Standard) or non-public information maintained by CWM.

ENTITIES AFFECTED BY THIS STANDARD

All CWM workforce members and any third-party who connect to CWM Information Systems, for which access is provisioned at the CWM unit level or centrally through IT and CWM workforce who connect to Information Systems provisioned by a third party to support CWM work Workforce designated to develop, approve and monitor access to such Information Systems are also covered by this standard.

RELATED DOCUMENTS
CWM Account Access Form
CWM Account Access Form Instructions
CWM System Change Process
CWM Account Recertification Process
UMMS Acceptable Use Policy
UMMS Data Classification
UMMS Confidentiality Agreement
DEFINITIONS: (See Glossary on Office of Management (OoM) website for additional definitions)

Account Access Form (AAF): The approved template used by all Data Security Administrators to provision access to Information Systems.

Account Provisioning: The practice of creating and managing (granting and removing) access to CWM Information Systems involving PII or financial information administered at the business unit level through a combination of a unique username and password or other authentication method.

Authorization Level: A security mechanism to determine access levels or user privileges related to system resources including files, services, computer programs, data and application features.

Data Security Administrator(s) (DSA(s)): The designated representative(s) of each CWM business unit, who is responsible for developing and monitoring Role Based Access Controls for CWM Information Systems involving PII or financial information and provisioning access to information systems administered at the business unit level.

Information Systems: All applications, information assets, databases, financial systems and IT resources involving PII, financial or non-public information.

Least Privilege: The practice of limiting access to CWM Information Systems to the lowest level of user rights essential for the completion of assigned duties or functions.

Manager of Data Privacy and Security: The OoM resource that works with DSAs and monitors the process to ensure it is conducted in compliance with the CWM Access Control Standard.

Provision/De-Provision: The creation, maintenance and deactivation of user accounts to permit authorized access to Information Systems.

Recertification: A review of user accounts, roles and Authorization Levels to verify Access controls are accurate and up to date.

Role Based Access Control (RBAC): The process of granting, restricting, or denying requests based on job function for system Access to prevent unauthorized Access to IT systems.

Separation of Duties (SOD): The practice of ensuring that no one person is responsible for completing or controlling a task or set of tasks from beginning to end when it involves the potential for fraud, abuse, system compromise or other harm and disseminating such tasks among multiple individuals to prevent such fraud, abuse or harm.

SCOPE

This standard establishes requirements for individuals regarding Access to (1) all CWM Information Systems administered at the business unit level or centrally by UMMS IT that involve PII, financial or other non-public information; (2) access to third-party information systems for work performed by CWM Workforce; and (3) the responsibilities of the DSAs for RBAC and OoM for oversight in account access.
STANDARDS

I. Business Unit Access Management

A. Each business unit shall appoint one DSA, and one backup DSA for coverage, to act as the Information System(s) security administrator, responsible for communicating guidelines for logical Access for Information Systems.

B. The DSA shall create and maintain written processes related to account provisioning that includes:
   1. An inventory of all Information Systems that require account provisioning (master user access inventory), which includes an effective way to easily identify all Information Systems to which each Workforce member has access.
   2. A current Account Access Form which incorporates the most recent Business Unit systems.
   3. Storage and maintenance of all completed account access requests, forms, processes, and other documentation in support of regulatory or contractual requirements.

C. For each Information System included on the AAF, the DSA shall follow the access management process to ensure that accounts are accurately established, modified, and terminated. The Account Access Process includes:
   1. A responsible individual in the business unit for creating, approving and documenting the distinct roles existing in each Information System and the corresponding job function.
      a. For new Information Systems, the business unit shall ensure the designated CWM New Information Form is completed and submitted. The DSA shall work with the Business Unit to ensure the Business Unit defines security roles and such roles are reviewed and approved by appropriate representatives of Finance, IS, and/or OoM.
      b. For modifications to roles for existing Information Systems, the DSA shall submit the request to UMMSDataAccessRequests@umassmed.edu for IS, Finance and/or OoM review and approval.
   2. Role and Authorization Level assignment and approval by the responsible manager for each Information System.
      a. Assignment of roles must ensure appropriate Segregation of Duties.
      b. Authorization Levels may vary according to the sophistication of the technology, but may include view only, run reports, create and edit, delete and configure (system administration).
      c. Ensure that Authorization Levels are appropriate and aligned with the approved roles and adhere to the principle of Least Privilege.
   3. Authorized approval of individual account access request. The approval is based on job function and Authorization Level required. No supervisor/manager/authorized approver or DSA may approve access on his or her own behalf. The submission must include:
      a. Date of approval.
      b. Identification of individual approving access, including job title.
      c. Description of access privileges requested – system, role, and level.
      d. Description of why access privileges are required.
      e. Submission of completed and approved AAF to the DSA.
4. Upon appropriate completion and approval of the AAF, the DSA shall Provision or request the Provision of account access. If the Information System is managed centrally, the DSA shall review the AAF then forward it to the IT Helpdesk by email. Only the designated DSA(s) for the business unit using an AAF is authorized to send an access request to the IT Helpdesk.

5. Storage of all completed forms with approvals in secure library for use in Recertification and monitoring of process.

6. Timing and process to address role or functional changes relating to access.
   a. Supervisors/managers/authorized approvers must submit a new AAF to DSA for any modifications to an individual’s access.
   b. Each role or functional change must be approved and documented in the same manner as the initial provisioning of account access.

7. Timing and process to ensure expeditious access termination (de-provisioning). Access must be terminated as follows:
   a. Non-voluntary terminations: immediately
   b. Voluntary terminations: immediately but no later than five business days from the date of termination.

Supervisors/managers/authorized approvers shall submit an AAF requesting access termination when a user:
   a. leaves CWM;
   b. changes roles and no longer requires access, or;
   c. is suspended or removed for security reasons.

8. Recertification of accounts occurs two times per twelve-month period in accordance with the CWM Account Recertification Process.

II. DSA Oversight Responsibilities
The DSA shall be responsible for:
   A. Maintaining current lists of roles, accounts and Authorization Levels for each internally supported Business Unit Information System.
   B. Retaining records within a secure library of all documentation related to the access and recertification process for a minimum of six years.
   C. Ensuring that account passwords comply with Information Technology’s Password Policy for dissemination, expiration and construction, as permitted by the Information System.
   D. Authorizing user access according to RBAC, least privilege (minimum necessary), and segregation of duty principles.

III. OoM Oversight Responsibilities
A. Serving as a resource to the DSAs in developing their business unit access management process.
   B. OoM shall be responsible for:
      1. Collaborating with Finance and IS on requests for new or modified roles defined for each Information System.
      2. Providing input into the AAF.
      3. Overseeing and reviewing the account Recertification process.
      4. Periodically reviewing the provisioning process, identifying gaps and working with the appropriate area to address gaps and mitigate risk.
      5. Escalating to OoM leadership and the UMMS ISO identified risks that are not timely addressed.
IV. Information Security and Finance Oversight Responsibilities
IS and Finance shall be responsible for:
A. Serving as a resource to OoM in the Access Control process.
B. Approving, in collaboration with OoM, Information System new and modified security roles.

V. Users
CWM users shall be responsible for complying with UMMS Information Security Policies and Procedures related to the use of Information Systems. This includes, but is not limited to:
A. Only Accessing or attempting to Access Information Systems to which the user is authorized to Access according to the business unit access management process.
B. Not exceeding or attempting to exceed the Role or Authorization Level for which the user is approved.
C. Not allowing another individual to Access such systems pursuant to the user’s account approval, regardless of whether the other user is also approved to Access the Information System.

VI. Reporting Unauthorized Access
A. Anyone who is aware of unauthorized Access to Information Systems shall immediately report such unauthorized Access to OoM using the Privacy, Compliance and Ethics Hotline at 508-856-TEAM or by email at PrivacyandCompliance@umassmed.edu.

Anyone found in violation of this standard may be subject to disciplinary action up to and including termination.

RESPONSIBILITIES

<table>
<thead>
<tr>
<th>Task</th>
<th>DSA/ System Business Owner</th>
<th>Supervisor/ Manager/ Authorized Approver</th>
<th>User</th>
<th>OoM</th>
<th>ISO</th>
<th>Finance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Written inventory of all Information Systems administered at the Business Unit as detailed on the AAF</td>
<td>Maintain an updated master inventory stored in a secure library</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Approval of new and modified system security roles for Information Systems</td>
<td>Establish or modify Information System roles in collaboration with System Business Owner and make notifications</td>
<td></td>
<td></td>
<td>Review and approve</td>
<td>Review and approve</td>
<td>Review and approve</td>
</tr>
<tr>
<td>Task</td>
<td>DSA/ System Business Owner</td>
<td>Supervisor/ Manager/ Authorized Approver</td>
<td>User</td>
<td>OoM</td>
<td>ISO</td>
<td>Finance</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>----------------------------</td>
<td>-----------------------------------------</td>
<td>------</td>
<td>-----</td>
<td>-----</td>
<td>---------</td>
</tr>
<tr>
<td>Develop a management process to ensure that RBACs are effectively implemented and monitored</td>
<td>Develop process incorporating input from Business Unit for the relevant Information System –levels of access and process for approving and provisioning access to the system</td>
<td>Approve the Role and Authorization Level for each user for which an account is requested</td>
<td>Provide oversight and review and approve the final process document</td>
<td>Provide guidance, as needed</td>
<td>Provide guidance, as needed</td>
<td></td>
</tr>
<tr>
<td>Educate Business Unit on process for requesting access to Information Systems</td>
<td>Work with business unit leads to educate users on the process</td>
<td>Reinforce training at Business Unit Level</td>
<td></td>
<td></td>
<td>Assists DSAs with training</td>
<td></td>
</tr>
<tr>
<td>Maintain an Account Access Form (AAF) Template</td>
<td>Review during Recertification process and submit to OoM</td>
<td></td>
<td></td>
<td>Review Updates</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Account Access Form (AAF)</td>
<td>Use AAF to identify and provision access</td>
<td>Complete and approve the AAF and submit to DSA</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provision of account access</td>
<td>Review the approved AAF and Provision or requests the Provisioning of access from the appropriate system owner</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recertification</td>
<td>Follow the CWM Account Recertification Process.</td>
<td>Work with the DSA to review and update systems</td>
<td></td>
<td>Monitor and review the CWM Account Recertification Process</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maintain current list of all Information Systems to which individual users have access and their authorization levels</td>
<td>Maintain and document process and current list</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Task</td>
<td>DSA/ System Business Owner</td>
<td>Supervisor/ Manager/ Authorized Approver</td>
<td>User</td>
<td>OoM</td>
<td>ISO</td>
<td>Finance</td>
</tr>
<tr>
<td>------</td>
<td>-----------------------------</td>
<td>----------------------------------------</td>
<td>------</td>
<td>-----</td>
<td>-----</td>
<td>---------</td>
</tr>
<tr>
<td>Storage of AAF and RBAC process documents</td>
<td>Store all documentation and process documents in a secure library.</td>
<td></td>
<td></td>
<td>Monitor and review submissions and provide feedback to DSAs as a group or individually</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**DOCUMENT HISTORY**

Effective Date: 6.1.2015
Revision Date(s): 2.10.2016; 3.31.2017; 12.01.2018
Review Date(s)

**APPROVAL**

---

_G.J. Campbell_

Gerry Campbell
UMMS Senior Privacy Officer
Office of Management