Commonwealth of  Massachusetts		
Information Technology Division **One Ashburton Place** **8th Floor** **Boston, MA 02108**	**Human Resources Division** **One Ashburton Place** **Room 301** **Boston, MA 02108**	**Office of the Comptroller** **One Ashburton Place** **9th Floor** **Boston, MA 02108**

MMARS Policy: **Statewide Enterprise Systems Security Policy**

Issue Date: **May 20, 2008**

Date Last Revised: **July 3, 2012**

Statewide Enterprise Systems Security Policy

Executive Summary

This security policy, issued jointly by the Chief Information Officer, Chief Human Resources Officer and the Comptroller, reflects the processes that govern the Annual Security Review and Approval for all statewide enterprise systems by Department Heads and primary Department Security Officers (DSO). This policy also highlights and references guidance on the importance of departments assuring that sensitive and personally identifiable data is secure and protected from inappropriate use.

The Information Technology Division (ITD) manages security for the following Statewide Enterprise Systems: Commonwealth Information Warehouse (CIW), DocDirect, and InTempo.

The Office of the Comptroller (CTR) manages security for the Massachusetts Management Accounting and Reporting System/Labor Cost Management (MMARS/LCM), Human Resources/Compensation Management System (HR/CMS), and PartnerNet functions (Internal Control Questionnaire, Fixed Asset Inventory Review, and GAAP Reporting).

ITD receives Universal Access Identification Code (UAID) requests for access to these systems via the on-line request system InTempo. While internal processes vary slightly based on the system owner, the Approval and Review evidence by Department Heads and Department Security Officers is standardized, collected and retained by the Office of the Comptroller via the respective approval forms. The annual review includes CIW, DocDirect, HR/CMS, Intempo and MMARS/LCM.

Security Reports

Four security reports are available in Luminist for department review and use.

Report IDs: SECMMARS, SECHRCMS, SECCIW, and SECINTEM.

Access to the reports is granted to Department Heads, Chief Fiscal Officers (CFOs), primary DSOs and MMARS Liaisons, assuming these key contacts have a Universal Access Identification Code (UAID). Any key contact can request access to these reports via their security officer once they obtain a UAID from ITD. These reports are run monthly. For MMARS and HR/CMS questions, please call the Comptroller's Help Desk at 617-973-2468. For CIW, DocDirect, and InTempo questions, please call CommonHelp at 866-888-2808.

Considerations

This policy addresses the mandate of annual approval of security for access to statewide enterprise systems by Department Heads and annual review of security by Department Security Officers. CFOs, Chief Information Officers (CIOs), and DSOs are expected to advise Department Heads on security and help to facilitate the Department Head approval of security.

- The creation of UAIDs is managed and controlled by the Information Technology Division (ITD) through InTempo.
- Access to highly sensitive data in CIW, such as Intercept data and related intercept records, is approved by the General Accounting Bureau of the Office of the Comptroller prior to implementation by ITD.

Department Head Responsibilities

- Ensures that the Department conducts all fiscal business in accordance with state finance law, including but not limited to Massachusetts General Laws Chapter 29 and Chapter 7A and laws, regulations, policies and procedures of the Office of the Comptroller.
- Approves changes to Department Head Signature Authorizations (tracked in MMARS) and ensures that these changes are filed as part of the Department's Internal Controls and are communicated without delay to the Comptroller's Security Unit.
- Approves changes to the Key State Finance Law Compliance Roles and ensures that these changes are filed as part of this Department's Internal Controls and are also communicated without delay to the Comptroller's Executive Bureau. See Update Form at http://www.macomptroller.info/comptroller/docs/forms/other/dept-key-fin-law.doc .
- Ensures that all written and electronic communications from the Office of the Comptroller, the Executive Office of Administration and Finance and other applicable oversight departments are disseminated to the appropriate Department personnel in a timely manner.
- Provides yearly approval of CIW, DocDirect, HR/CMS, InTempo and MMARS/LCM Security for staff and provides written evidence of the review to the Comptroller by the end of the Fiscal Year.

Department Head Designation of Department Security Officer

The Department Head should give careful consideration when appointing a Department Security Officer, given the significant responsibilities, accountability and authority of the position. Primary and backup Security Officers must be employed by the Department for which they are designated. The Security Officer is the gatekeeper for security access to all electronic applications including the expenditure of funds and payroll. Security is the foundation of Internal Controls and good fiscal management. As electronic "approval" acts as the electronic signature of the Department Head, the Security Officer performs a key role within the department. Appointments of individuals who demonstrate reliability, concrete understanding of systems, security, and internal controls, as well as segregation of duties, helps ensure that enterprise systems security is managed well within the department. The Designation of Department Security Officer Form is used by the Department Head to appoint a primary Security Officer as well as backup Security Officers.

Department Head Signature Authorization / Electronic Signature

The state accounting system (MMARS) is the "official record" of fiscal business in the Commonwealth. Electronic signatures will be used to "certify" transactions as official records. MMARS Security supports the Department Head Signature Authorization delegation process. The Department Head is automatically an Authorized Signatory by virtue of the title. All other Authorized Signatories must obtain MMARS access to be identified and tracked through security. Some authorized signatories may not be on-line users but are signatories on contracts or other supporting MMARS documents and they will still need a MMARS UAID to be set up as an Authorized Signatory.

The designation of the Administrator Role enables department personnel to process fiscal documents to a final status even if they do not have Department Head Signature Authorization. Departments must document additional staff delegation in their Department Internal Controls, update it on a regular basis to support the department's need for processing MMARS business and ensuring consistency between the Administrator Role and electronic security. Department Heads decide to what extent they want to delegate signature authorization.

Security Officer Responsibilities

- Obtain UAIDs (Universal Access Identification Codes) for users in the department via the ITD InTempo security request application.
- Assist Department Management in identifying the correct security roles for Department personnel.
- Assist Department Management in identifying individuals as Authorized Signatories and obtain evidence of the Department Head approval prior to, or at the time of, the request for such designation.
- Request access and assign roles for HR/CMS, CIW, and DocDirect via the ITD InTempo application.
- Request access and assign roles for MMARS using the UDOC MMARS transaction.
- Process role and DHSA changes using the UDOC MMARS transaction. DHSA changes require Department Head signature.

- Attend all Security related meetings and training sessions, train staff as part of the assignment and ongoing maintenance of security roles, and periodically reminds staff of the responsibilities related to security access, Administrator role responsibilities, electronic signatures for MMARS documents and the duty to comply with state finance law.
- Maintain communication with the Security Administration Unit in the Office of the Comptroller (CTR) on all MMARS and HR/CMS security related issues.
- Maintain communication with ITD on all CIW, and DocDirect security related issues.
- Monitor the Department's organization for any changes that should impact a user's access, such as termination of an employee or changes to an employee's duties.
- Notify CTR of any situation which requires immediate de-activation of a user's access to MMARS and HR/CMS.
- Notify ITD of any situation which requires immediate de-activation of a user's access to CIW, InTempo, and Doc Direct.
- Perform password resets for users in the department as needed.
- Complete the Annual Department Security Officer Review of Enterprise Security Systems for staff access. Evidence of the review must be provided to the Office of the Comptroller Security Unit at the end of the calendar year within 30 days of the notification.
- Facilitate the Annual Department Head Approval of Enterprise Systems Security during the Close/Open period. Evidence of the approval must be provided to the Office of the Comptroller Security Unit within 30 days of the notification.

Policy

Department Heads - Annual Security Approval

The Department Head must approve security access to all statewide enterprise systems by his/her staff. The collection of Department Head approval evidence assures that access to all statewide enterprise systems, security roles, and Department Head Authorized Signatory Designations (DHSA) are up-to-date and personally approved by the Department Head **prior to** opening the subsequent fiscal year business. The Department Head annual approval occurs in the spring as part of the Closing/Opening tasks. New Department Heads must also approve security access to all statewide enterprise systems by his/her staff within 30 days of appointment. The Department Head should rely on the CFO and the Security Officer to facilitate the annual approval process.

The Annual Security Approval by the Department Head prior to opening the Fiscal Year certifies that Enterprise System Security Reports have been reviewed and approved by the Department Head. Specifically, the approval will document the following:

- Staff with MMARS Fiscal Administrators roles (DFISC) or other cross-functional access (such as staff with roles to submit both Contracts and Payments) have been reviewed and confirmed.

- The Department's Internal Controls reflect individual restrictions, segregation of duties and limitations by user/UAID.
- Staff with Department Head Signature Authorization (DHSA) is approved.
- The Enterprise Security Reports (CIW, DocDirect, HR/CMS, InTempo and MMARS) for the Department have been reviewed by the Department Head, the Security Officer and other Administrators.

The CTR Security Unit coordinates collection of approval on behalf of CIO, Chief Human Resources Officer, and the Comptroller. Approval evidence must be received by the CTR Security Unit by the end of each Fiscal Year.

Approval Evidence can be an email, with the approval form attached, sent from the Department Head's account or a hard copy of the form with the Department Head's signature. Electronic documentation should be forwarded to securityrequest@massmail.state.ma.us. A hard copy should be mailed to:

Office of the Comptroller
Attn: Security Unit
One Ashburton Place – 9th floor
Boston, MA 02108

Primary Department Security Officers – Annual Security Review

The Department Security Officer (DSO) must review their department's staff security access to MMARS, HR/CMS, CIW and InTempo. Security access review evidence assures that access to all enterprise systems, security roles, and Department Head Authorized Signatory Designations (DHSA) are up-to-date and have been approved by the Department Head. The Security Officer annual review takes place at the end of each calendar the year.

The Annual review by the DSO will certify that:

- Staff with MMARS Fiscal Administrators roles (DFISC) or other cross-functional access (such as staff with roles to submit both Contracts and Payments) have been reviewed and confirmed.
- The Department's Internal Controls reflect individual restrictions, segregation of duties and limitations by user/UAID.
- Staff with Department Head Signature Authorization (DHSA) has the personal approval of the Department Head.
- The Enterprise Security Reports (CIW, DocDirect, HR/CMS, InTempo and MMARS) for the Department have been reviewed and approved by the Department Security Officer.

Review Evidence can be an email, with the review form attached, sent from the Primary Security Officer's account or a hard copy of the form with the Primary Security Officer's signature. Electronic documentation should be forwarded to securityrequest@massmail.state.ma.us . A hard copy should be mailed to:

Office of the Comptroller
Attn: Security Unit
One Ashburton Place – 9th floor
Boston, MA 02108

Guidance for Statewide Enterprise Systems Security Access

Massachusetts Management Accounting and Reporting System / Labor Cost Management (MMARS/LCM)

Department Head Security Certification

The Office of the Comptroller (CTR) requires that a Department Head MMARS Security Certification be on file for the department. Designation of key contacts is a distinct activity, different from the annual certification of enterprise systems security access. The Department Head, not a designee, must sign this certification. When the Department Head changes, the new Department Head must update this form and list any changes to key contacts for the department.

MMARS Security Roles

MMARS security allows flexibility to choose roles that support specific business areas, such as Accounts Receivable, Accounts Payable, Fixed Assets, etc. Users may be assigned one or more roles within one UAID, depending upon the functions performed. It is the granting of multiple functional areas to a single UAID without mitigating external procedures for proper internal controls that must be avoided.

MMARS Security also supports two levels of access for each business area:

- The **Administrator Role** is the more powerful role, it allows the individual to validate and "submit" a document to a Final status, which acts as the electronic signature of the employee to whom the UAID is assigned and evidence of DHSA is maintained external to MMARS.

- The Administrator Role is enhanced when the UAID is designated as a Department Head Signature Authority in which case the electronic signature acts as that of the Department Head.

- The **User Role** is more restricted and allows the processing of documents but excludes the ability to "submit" a document to a final status. Documents entered with the "user role" must be submitted by someone with administrator security. See the MMARS Security Roles and Documents Processed for complete description of all MMARS security roles.

Guidance on Selecting High-level MMARS Security Roles

While the use of high-level security roles may be needed, a large number of staff with high-level security roles increases the risks to internal controls, since individuals can process related transactions without

oversight, i.e., staff who have the ability to set up vendors and encumber should not also make payments or receive revenue. CTR recommends the following best practices to mitigate department risk:

- Provide periodic review of all high-level 'Administrator' type security roles and promote staffing models that truly segregate duties. If segregation is more difficult (e.g., for small departments), establish a process to require two individuals to be part of the review of transactions to be approved.

- Include supporting narrative for all security decisions, 'Administrator' role justifications, DHSA Designations, and the annual approval evidence in your Internal Control Plan.

- Department Head and Secretariat Signature Authorization should ensure that there are sufficient Department employees authorized to approve contracts, transactions, payroll and other critical business needs during staff vacations, maternity leave, sick leave or other leave. Departments must balance the need for adequate coverage with the risk of having too many employees with Administrator or Department Head Signature Authorization by developing steps to minimize risks for abuse.

The CTR Security Unit will reject all requests for the DFISC role (Department Fiscal Administrator) unless justification is provided. Security Officers should work closely with department management to determine the appropriate roles for users.

Questions about MMARS Security, Signature Authorization, best practices, or security role selections should be directed to the Comptroller Security Unit via the Help Desk at 617-973-2468. Security staff will assist you over the phone or by meeting with you and your Department administrators.

MMARS Log In User Certification

The MMARS Login Screen contains language to which the user certifies:

"By entering a UAID and password and initiating a log on to the MMARS system, you understand that your UAID is being recorded for any entries made in the system."

By submitting a document for final processing, the users agree that they are certifying under the pains and penalties of perjury that:

- It is their intention to attach an electronic signature approval and date to the MMARS document
- They are either an authorized signatory of the Department with authorization to approve the MMARS documents, or that the document being processed with supporting documentation has been approved by an Authorized Signatory of the Department head, secretariat and any other approval Department, and that a copy of these approvals is available at the Department referencing the MMARS document number.

- The authorized Department and secretariat signatory approvals of the MMARS document with underlying supporting documentation operate as certifications that these documents are accurate and complete and comply with all applicable general and special laws, regulations and policies including public record retention and disposal requirements.”

Human Resources Compensation Management System (HR/CMS)

HR/CMS provides more than **35** roles that can be assigned to an individual based on his/her job responsibilities. Given the sensitivity of HR/CMS data (SSN, disability data, etc.), it is critical that users be granted access only to screens needed to complete their job responsibilities. Access to modify an individual's pay, enter time and attendance data, or enter other additional compensation, must be balanced by internal controls that assure that personal and compensation data are not changed without authorization. Reports should be monitored by management to assure that no unauthorized changes are executed.

The HR/CMS Security Roles have been constructed to support the various levels of access for each business area.

- The **Correction Mode – Control Users** is limited to control departments only.

- The **Operational User Role** is used by Higher Education, Constitutional Officers, Independents and the Administrative Office of the Trial Court departments which have responsibility for processing business activities specific to their departments' operational needs.

- The **End User Role** is a more restricted role and allows the processing of Human Resources, Payroll, Benefits, and Time & Labor transactions pertaining to the individual department's data. See the HR/CMS Security Guidelines and Procedures for a complete description of all HR/CMS security roles. Requests for disability data must be approved by the State Office of Affirmative Action. Requests for the Public Records Exemption data must be routed through and authorized by the Department Human Resources Director due to the confidential nature of the exemption status.

If you have any questions about HR/CMS Security, Signature Authorization, best practices, or security role selections, please call contact the Comptroller Security Unit via the Help Desk at 617-973-2468.

Commonwealth Information Warehouse (CIW)

CIW Access: The Commonwealth Information Warehouse consists of data from HR/CMS, e*mpac (UMS payroll), PMIS/CAPS, MMARS, LCM and Classic MMARS Source Systems. There are several levels of access to data in the Commonwealth's Information Warehouse such as Department level or Statewide. Some CIW views contain Personally Identifiable Data that could be damaging to individuals as well as to the

Commonwealth if the data were compromised. Given the sensitivity of the data such as SSN, disability data, etc., it is critical that users be granted access only to the data needed to complete their job responsibilities.

The CIW provides several roles that can be assigned to an individual based on his/her job responsibilities.

Personnel Related Data (HR/CMS, e*mpac and PMIS/CAPS):
Human Resource and Payroll systems and the CIW data extracted from those systems contain Social Security Number or National ID for each employee. The National ID field in HR/CMS and e*mpac has been masked to only display the last 4 digits of the SSN. SSN is protected data under both state and federal laws. For CAPS and PMIS data, SSN was the key to an employee's record prior to the implementation of an Employee ID with HR/CMS and cannot be masked; access to this data should be restricted to one or two individuals who need this information.

HR/CMS / e*mpac data in the CIW includes human resource and payroll related roles as well as special roles that require certain levels of approval. A standard role is available for users to access a certain set of views, which should be sufficient for most HR and payroll users. CIW also provides an additional role for users who need more access to data that contains more detailed information and is suited to HR and Payroll managers and staff who need to report at a higher level.

Some data with restricted access requires a special role and written authorization from HRD or Department HR Directors such as Disability data and Public Records Exemption data. Department Security Officers must forward this written authorization to the ITD Information Security Unit prior to user access being granted to the data.

The Department Security Officer must review the type and level of access to be requested. It is the responsibility of the Department Security Officer to obtain other department signatures for approval as required by the type of access requested. CTR and HRD review and approve or deny user requests for access to special roles that require such approval.

MMARS, LCM and Classic MMARS Data:
There are several levels of access to financial data in the Commonwealth's Information Warehouse. Users can request Departmental or Statewide access to MMARS data. For LCM and Classic MMARS data access can be requested for Departmental, Multiple Department, Secretariat, Branch of Government. LCM can also be restricted at the Department pay organization level. Statewide access to LCM and Classic MMARS data is restricted to departments with statewide financial responsibility.

Data in the CIW is segregated into views, some of which have data that is not public information. Access to intercept data is heavily restricted at both the department and statewide level. The Comptroller's Accounting Bureau must approve all requests for intercept data other than a DSO requesting the standard intercept role

for the individual department's staff. This access must be approved by the department head as needing access to the department's individual intercept data.

Please visit the CIW Website www.iw.state.ma.us for a complete description of all Commonwealth Information Warehouse security roles.

Internal Controls

Security for all enterprise systems is managed by the department to support Internal Control concepts and guidelines for both transaction processing and access to Sensitive Data. The DSO and the Department's Internal Control Officer should coordinate activities to assure appropriate use of systems:

- Users must be trained on relevant policies and use of Personally Identifiable Data.
- Executive Department Agency Heads confirm compliance with Executive Order 504 through submission of an electronic security plan (ESP) and an annual self-audit questionnaire (SAQ).
- Department work should be set up to segregate duties whenever possible to assure that state resources and sensitive data are protected.
- Personnel and system policies should highlight that sharing of security system IDs (UAIDs, passwords, etc.) is prohibited.
- Delegation of signature authorization to managers and staff should be at appropriate levels and reflect the internal controls of the department. The Department Head must approve all delegation of signature authorization – this approval cannot be delegated.
- Staff financial activity should be monitored on a regular basis using standard transaction and department generated reports from the source systems (HR/CMS, MMARS/LCM) and Commonwealth Information Warehouse.

Violation of State Finance Law

Any department head or designee who knowingly violates state finance law, authorizes or directs another officer or employee to violate any provision of M.G.L. c. 29, or any rule or regulation promulgated there under, or any other provision of law relating to the incurring of liability or expenditure of public funds shall be punished by fine of $1,000 or imprisonment for one year, or both. See M.G.L. c. 29, § 66.

Information Sources

Legal Authority:

- M.G.L. c. 7A (Office of the Comptroller); M.G.L. c. 29 (State Finance Law);
- M.G.L. c.29, § 66 (State Finance Law Violations)
- MGL c. 66A Fair Information Practices Act
- 801 CMR 3 Privacy and Confidentiality
- MGL c.214 s. 1B Right to Privacy
- MGL c.214 s. 3B Violations of Chapter 66A; Statute of Limitations

Related Policies:

- Key State Finance Law Compliance Appointments and Responsibilities
- Department Head Signature Authorization and Electronic Signature for MMARS Documents
- ITD Security Policies

Attachments:

- Department Head Annual Approval Form
- Department Security Officer Annual Review Form
- Designation of Department Security Officer Form
- Department Key State Finance Law Compliance Update Form
- HR/CMS Security Guidelines and Procedures
- ITD Security Access Request Form
- Payroll Public Records Exemption Policy
- Contacts – CTR Help Desk
- CommonHelp

Revisions:

November 20, 2008 - Updated links to reflect changes to HR/CMS security.

April 6, 2011 – Updated to include UDOC/UDOCPR MMARS Transactions. Removed reference to MMARS Security Request Form. Consolidation of MMARS Security Policy with Enterprise Systems Security Policy.

July 3, 2012 – Updated to change HR/CMS security references from ITD to Office of the Comptroller.