Commonwealth of Massachusetts

OFFICE OF THE COMPTROLLER

ONE ASHBURTON PLACE, 9TH FLOOR
BOSTON, MASSACHUSETTS 02108
TELEPHONE (617) 727-5000
WWW.MASS.GOV/COMPTROLLER

ANDREW W. MAYLOR
COMPTROLLER

Policy:	**Security**
Issue Date:	**March 23, 2017**
Date Last Revised:	**March 23, 2017**

CTR Statewide Enterprise Systems Security Policy for Contractors Including Staff Augmentation Resources

Executive Summary

This policy applies to all state Department "Contractors", including contract employees, vendors, staff augmentation resources, and any other individual who is not a state employee for whom a Department is requesting temporary access to a Statewide Enterprise System or its data managed by the Office of the Comptroller (CTR), including MMARS, HR/CMS, and any associated repository such as the CIW or a Department or third party hosted repository, or any of these systems' test or backend regions. In addition, use of HR/CMS as a time and attendance or project management tracking tool has the same registration requirements. This policy details the required registration, background check, training and certification requirements and access levels available to Contractors.

A Department Head is responsible for all activity by a Contractor granted system or data access via an Employee ID (EMPLID), Universal Access ID (UAID) or other access, and is required to ensure that strict internal controls are instituted and routinely followed to ensure that Contractor actions comply with all rules, regulations, laws, policies, procedures and other guidance issued by CTR, including the Statewide Enterprise Systems Security Policy. As with all individuals with access to the Enterprise Systems – security access identification and passwords must never be shared. Improper use of passwords or access, suspected or actual fraud or theft will result in immediate termination of system access, and may result in legal or disciplinary action to the fullest extent provided by law based upon the nature of the violation.

Access to Enterprise Systems by persons who are not Commonwealth employees present an additional level of risk to the safety, security and protection of these systems and the data within these systems. As part of CTR's on-going Enterprise Risk Management (ERM) process, potential areas of risk are regularly reviewed and risk mitigation is incorporated into our business practices and policies while working in collaboration with our business partners to meet their needs to the greatest extent possible. It is for these reasons that access to these systems for contractors should be limited, and all Contractor access requests are subject to review and approval by CTR's Statewide Risk Management Team.

Requirement to be Registered in HR/CMS

In order to track Contractor performance hours and security access, all individuals being considered for access to CTR-controlled Enterprise Systems or seeking a UAID for supporting or interfacing systems must be registered in HR/CMS BEFORE the request for security access is made. An individual will be entered as an employee, contract employee or alternatively as a "contractor" contingent worker not compensated by the HR/CMS system. Registration in HR/CMS is a critical CTR security requirement that includes the entry of certain necessary personal information (including date of birth and social security number) by the hiring, employing or contracting department so that CTR has specific, individual identifying information about all users of its Enterprise Systems or those using HR/CMS as a time and attendance or project management tracking tool. For Contractors registered as "contingent workers" the collection of this individual identifying information does not create an employment relationship with the individual but is used solely for validation and security check purposes, and may be used to track accurate hours for staff augmentation resources for agencies that seek to use this feature.

Background Check

CTR requires a background check in the form of a Criminal Offender Record Information (CORI) check on all contractors seeking access to MMARS or HR/CMS. This is to be completed at the time of the request, or for staff augmentation vendors as part of their hiring process, and should be updated when a contract is renewed or after a lapse when the contractor is to be rehired. Departments or staff augmentation vendors must comply with the CORI procedures to conduct the background checks and may not share CORI details with CTR or anyone else as this information is highly confidential. Individuals with returned incidents of theft, cybercrimes, embezzlement, or other fraudulent events may be automatically disqualified from system access. CTR Risk Management staff can provide information about what types of returned incidents disqualify a contractor from access to the Enterprise Systems, but CTR will not ask for names or other details related to any specific individual. As part of the annual certification, Department Heads will have to certify that a background check has been completed and that there is no incident or event that would disqualify the Contractor or raise concerns about security access to Enterprise Systems.

Certification and Training Requirements

CTR requires all contractors seeking access to MMARS and HR/CMS to read and sign a **Contractor Acknowledgment Form** certifying compliance with confidentiality, conflict of interest and other requirements in order to receive security access, in addition to any other training or certifications required by the contracting Department. CTR may at any time require Contractors to take training related to their security roles, or require additional training as risk mitigation evolves and as a condition of continued security access.

Access Levels

For System Technical Support:

For all programming or code access, contractors must be supervised by state employees. For audit purposes all system development, analysis, configuration, or other application programming work, must be recorded and managed through a system/software tracking tool.

For System Processing:
For all system processing, contractors must be supervised by state employees. Administrator Roles allow the individual to validate and "submit" a document to Final status. "Submit" requires evidence of approval by a Department Head Signatory Authority (DHSA).

Roles

MMARS

Department Security Officers should contact the CTR Security Unit for a complete description of all MMARS security roles.

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. This means that there must be evidence of a DHSA signature for each transaction PRIOR to the transaction being submitted that is retained for audit purposes referencing the transaction.

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.

HR/CMS

Of the available roles in HR/CMS, contractors may be eligible to receive Display Only roles in HR/CMS- these roles allow view only access to specific tables.

CIW

Prospectively, CTR will not approve Contractor access to the CIW.

Period of Access

Contractors are considered temporary resources and requests for security access must indicate the period of the need for security access, which will have to be renewed if the need extends beyond the approved period.

How to Submit Access Requests to CTR

In addition to the standard security role forms requesting security roles, Departments must submit a **Contractor Access Request Form**, completed and signed by an individual with Department Head Signatory Authority, for each Contractor that access is requested for. If multiple Contractors are included in the same Access Request Form a, spreadsheet may be included as an attachment to the **Contractor Access Request Form**. CTR has provided a template that must be used when possible.

The **Contractor Access Request Form** requires identification of the specific role requested; an explanation with justification of the specific access requested; and the period of access requested. Each request will be reviewed by CTR's Statewide Risk Management Team, including the Chief Risk Officer prior to approval.

Additionally, each department must submit an **Annual Department Head Certification Form** which is personally signed by the Department Head and submitted once per year to CTR's Statewide Risk Management Team.

All forms should be submitted electronically to CTR's Enterprise Security Team at CTR-Risk.Management.Team@massmail.state.ma.us.