OFFICE OF THE COMPTROLLER
ONE ASHBURTON PLACE, 9TH FLOOR
BOSTON, MASSACHUSETTS 02108
(617) 727-5000
MACOMPTROLLER.ORG

Statewide Enterprise Systems Security Access for Contractors Policy

Effective: March 23, 2017
Last Updated: April 9, 2026

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 which a department is requesting temporary access to a statewide enterprise system or data managed by the Office of the Comptroller (CTR). Enterprise systems include the Commonwealth's enterprise financial accounting system ("Mosaic"), the enterprise payroll system (HR/CMS), and any associated repository 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.

Department heads are responsible for all activity by a contractor granted system or data access via an Employee ID (EMPLID), Universal Access ID (UAID or User ID), or other method of access, and must ensure that strict internal controls are instituted and routinely followed to ensure that contractor actions comply with all applicable rules, regulations, laws, policies, procedures, and guidance issued by CTR, including the CTR Statewide Enterprise Systems Security Access Management Policy.

Access to enterprise systems by persons who are not Commonwealth employees presents an additional level of risk to the safety, security, and protection of these systems and data. All contractor access requests are subject to review and approval by CTR's Statewide Risk Management Team. Requests for security roles to replace state employee functions, to access sensitive data or data repositories (such as the Commonwealth Information Warehouse) are not normal contractor access are not routinely granted.

Department heads are required to annually certify that the department has a system of written internal controls, training, and monitoring actively in place as part of daily operations to achieve the department's mission, ensure compliance with CTR's published guidance (PowerDMS, MAComptroller.org, Fiscal Year Memos, CTR Statewide Trainings), and prevent fraud, waste, and abuse of Commonwealth resources. This policy is included in the annual certification.

Requirement for Annual Department Head Certification

Departments who request enterprise security access for contractors must submit an Enterprise Security Access for Contractors - Annual Department Head Certification Form, which is signed by the

department head and submitted annually. This form will apply to any requests for contractor enterprise security access for that annual period.

To ensure protection of the enterprise systems and data, department heads certify full responsibility for any actions or events that occur due to actions or inactions by contractors working under the approved security access, and that strict internal controls, segregation of duties, supervision, and oversight will be maintained to mitigate the risks associated with providing this security access. Department heads certify that all contractors are properly trained for the security roles that are approved, which includes CTR provided trainings and resources posted on PowerDMS. Department heads also certify that background checks have been completed for all contractors and that there is no history of theft, cybercrimes, embezzlement, or other fraudulent events that would disqualify the contractor or raise concerns about their access to enterprise systems.

Requirement for Contractors 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 User ID for supporting or interfacing systems must be registered in HR/CMS before the request for security access is made.

An individual will be entered either as a contract employee or, alternatively, as a contractor contingent worker not compensated through HR/CMS (contingent workers are employees of a vendor or staff augmentation statewide contractor). 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) 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. Registration may also be used to track accurate hours for staff augmentation resources, for agencies that seek to use this feature.

Requirement for Contractors to have Background Check

CTR requires a background check in the form of a Criminal Offender Record Information (CORI) check on all contractors seeking access to the Commonwealth enterprise financial accounting system or HR/CMS. The background check must be completed at the time of the security access request or, for staff augmentation contingent workers, as part of their hiring process, provided the background check is not more than 6 months old.

Departments or staff augmentation vendors must comply with the Massachusetts Criminal Offender Record Information (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 whose CORI shows incidents of theft, cybercrimes, embezzlement, or other fraudulent events must be automatically disqualified from system access by the department.

The CTR Statewide Risk Management and Compliance Team can provide general information or advice about what types of returned incidents disqualify a contractor from access to the enterprise systems.

CTR will not ask for names or other details related to a specific individual. As part of their annual certification, department heads must attest that a background check has been completed for each contractor and that there is no incident or event that would disqualify the contractor or raise concerns about security access to enterprise systems.

Requirement for Contractor Certification and Training Requirements

CTR requires all contractors seeking access to the Commonwealth enterprise financial accounting system or HR/CMS to read and sign an Enterprise Security Access for Contractors - Contractor Acknowledgment Form certifying compliance with confidentiality, conflict of interest, and 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.

Contractors Must be Supervised by State Employees

Department employees must supervise all contractor actions. For audit purposes, all system technical support, programming or code access, system development, analysis, configuration, or other application programming work must be recorded and managed through a system/software tracking tool, or other process to track all contractor actions in the system. Department employees must supervise all contractors who enter enterprise system transactions. Departments may not allow contractors to submit transactions to "final" status.

Mosaic

Contractors are limited to "Train"or "Dept Scan" roles, which are restricted roles that allow limited views and data entry but exclude the ability to submit a document to either "pending" or "final" status. Transactions entered by contractors with the "Train" role remain in "draft" status and must be submitted by a state employee with an Department User (may submit to pending) or a Department Approver role administrator security role. If that state employee has not been delegated Department Head Signature Authorization (DHSA), the state employee must also obtain approval by someone with that authorization.

Contractors will not be approved for an "Approver" role which is the most powerful and riskiest role. "Approver" roles allow a user to validate and submit a document to "Final" status, which acts as the department head's electronic signature and approval of the transaction. CTR will not approve "Approver" roles for contractors, since department heads may not delegate DHSA signature authorization to a non-employee of the department. If a department needs an "Approverr" role, the departments must ensure that a department employee is in place to perform this role.

HR/CMS

Contractors may only be approved for "Display Only" roles in HR/CMS, which allow view only access to specific tables.

Commonwealth Information Warehouse (CIW)

CTR will not approve contractor access to the CIW.

Temporary Period of Contractor Security Access

Contractors are considered temporary resources. Requests for security access must indicate the temporary period of the need for security access. Contractor security access requests for temporary access while a state employee is on leave, or to backfill a position that is in the process of being filled, should be requested for the shortest period of time necessary. CTR reserves the right to limit the period of access to fit the need.

How to Submit Contractor Enterprise Security Access Requests to CTR

Resources and a job aid for submission of contractor enterprise security access requests are posted in the PowerDMS Security folder.

If multiple contractors are included in the same access request form, CTR has provided a template that should be used as an attachment to the Enterprise Security Access for Contractors - Contractor Access Request Form.

The Statewide Risk Management and Compliance Team reserves the right to approve, reject or request modification to any request for contractor enterprise security access.