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

Statewide Enterprise Systems Security Access Management Policy

Effective: May 20, 2008
Last Updated: May 27, 2026

Executive Summary

This policy outlines security access management responsibilities for the Commonwealth statewide enterprise accounting and financial system ("Mosaic") and payroll system ("HR/CMS"), and other related systems overseen by the Office of the Comptroller (CTR). In accordance with M.G.L. c. 29 and c. 7A, CTR is responsible for maintaining the Enterprise Accounting and Payroll Systems which are the "official record" of fiscal business in the Commonwealth and the basis for the Commonwealth's financial reports. CTR coordinates with other oversight agencies, such as the Executive Office of Technology Services and Security (EOTSS) and the Human Resources Division (HRD), to support security access to the Enterprise Systems.

This policy addresses the responsibilities for the appropriate provisioning of Enterprise System security access, department head and Department Security Officer (DSO) responsibilities, and the requirements, monitoring, and annual review and certification of security access.

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. See the CTR Internal Controls Policy.

Department Head Responsibilities

A department head certifies that the department will conduct all fiscal business in accordance with state finance law including, but not limited to, Massachusetts General Laws Chapter 29 and Chapter 7A and regulations, policies, and procedures issued by CTR. Department heads are responsible for all actions of the department, including fiscal obligations and fiscal activity that are required to be promptly and accurately recorded in the Enterprise Accounting and Payroll Systems as described in this policy. Department heads are also responsible for approving Enterprise System security access roles, the scope of that access, and whether an individual has the authority to approve actions on behalf of a department head.

Department heads are responsible for the following security access management requirements:

Department Head Security Certification

In order for departments to have access to and expend funds in the Enterprise Accounting and Payroll systems, CTR requires that a Department Head Security Certification be on file for each department

head upon appointment. Enterprise Systems security roles will remain in place during any transition period, but should be updated and ratified as soon as the department head assumes their responsibilities. The department head is responsible for personally signing the Department Head Security Certification and may not delegate this responsibility.

Department Security Officer (DSO) designation

Primary and backup DSOs must be appointed directly by the department head, and not by a designee. The department head should give careful consideration when appointing DSOs given the significant responsibilities, accountability, and authority of the position.

The DSO is responsible for assisting the department head in meeting the security access management requirements for the enterprise accounting and financial reporting and payroll systems, and other related systems overseen by CTR. DSO responsibilities include, but are not limited to, assisting department management in identifying the correct security roles for department staff, authorized signatories, and obtaining and maintaining proper designation approval from the department head.

Department heads are advised to appoint individuals to DSO positions who demonstrate reliability, concrete understanding of systems, security, and internal controls, as well as segregation of duties, thereby helping to ensure that Enterprise Systems security is managed well within the department.

A department must have, at a minimum, a primary and a backup DSO, with larger departments having additional back up DSOs. All designated primary and backup DSOs are responsible for being trained and capable of performing all key DSO functions to support department employees requiring security access to the enterprise systems. The Key Contacts Update Docusign PowerForm is used by the department head to appoint a primary DSO as well as backup DSOs.

For more information about DSO responsibilities, please refer to the CTR Key State Finance Law Compliance Roles and Responsibilities Policy as well as the job aids and other security resources published in PowerDMS.

Least privilege

Security access roles must be carefully reviewed for each employee, to restrict access to the minimum needed to perform a role ("least privilege"). Departments should not merely replicate profiles or authorize overly broad security access roles for ease or expediency, which increases risks of fraud and may be flagged in audits. The department head must ensure that the departments' implementation of least privilege is documented as part of their access management protocols.

Segregation of duties

Various steps in a transaction's process must be assigned to different people, with the intent of eliminating instances in which someone could engage in theft or other fraudulent activities by having an excessive amount of control over a process ("segregation of duties"). Security access role assignment must support segregation of duties to prevent a single employee from having the ability to be on "both sides of a transaction" (such as being able to create a vendor and also make a payment to that vendor). Segregation of duties also requires that some departments who may have limited staff, or that have employees with broader security profiles, have multiple employees review a transaction prior to processing it to mitigate the increased risk of mistakes and opportunities for fraud. Before providing access to any employee, the department head is responsible for establishing and documenting a process to determine what access should be given to ensure the requirement of segregation of duties is met.

Revocation of access upon termination, separation of service or leave

Establishing and maintaining strict internal controls and operational steps to ensure that security access roles are suspended or revoked within 24 hours of transfer, suspension, termination, extended leave, or other significant change of a user's employment status. Departments must ensure that HR/Payroll staff report any personnel changes immediately to the DSO when a status or role will change or has changed, to support immediate security access revocation to the Enterprise Systems within 24 hours of the planned or actual change in status. Merely revoking access to department equipment or network access is insufficient. It is expected that Enterprise Systems security access is also revoked within 24 hours. Auditors will audit the date of termination or change in employment role and the date of termination of Enterprise Systems security access.

Restricted access to data that triggers privacy, confidential and personally identifiable information (PII) compliance requirements

Establishing and maintaining strict internal controls and operational steps to ensure that security access roles which allow employees to view or access highly sensitive data, personal data, personally identifiable information (PII), and system security data are highly restricted, regularly monitored, and staff are properly trained on the restrictions for viewing, accessing and handling this type of data.

Routine monitoring

Establishing and maintaining strict internal controls and operational steps to ensure that security access roles are reviewed on an ongoing basis. The department must conduct two annual assessments, including the DSO mid-fiscal year annual review and the department head annual review.

Delegation of Department Head Signature Authorization (DHSA) and Associated Security Access Roles

A department head may delegate Department Head Signature Authorization (DHSA) to employees who will act on behalf of the department head, including approving legal obligations and payments. See the CTR Department Head Signature Authorization Policy.

For audit and access management compliance purposes, every department employee delegated DHSA to represent or act on behalf of the department head, including the approval of any legal or fiscal obligations or operations, must be assigned a security access role in the Enterprise Systems with a DHSA role or flag for the type of DHSA authorization granted, even if that employee will not be entering transactions in the systems.

The department's internal controls must also identify any additional transaction, amount limits or other restrictions, segregation of duties or requirements for employees with DHSA roles. Users with DHSA roles or flags may "approve" fiscal transactions, which acts as the department head's electronic signature.

Annual Enterprise Security Access Approval

Security access management requires consistent monitoring and review by the DSO, department management, and the department head. Security access to the Enterprise Systems is a significant department responsibility due to the access to fiscal activity as well as a significant amount of department information, including sensitive information and PII. The Statewide Risk Management

Team manages annual mandatory oversight review of the security access roles in the Enterprise Systems. DSOs are required to complete a mid-fiscal year review and approval of security access roles and assist the department head annually at the close of the fiscal year to review and ratify security access roles in the Enterprise Systems. The DSO and department head reviews and certification include:

- Review that all staff who access the Enterprise Systems, or who approve transactions or obligations that will be reflected in the Enterprise systems, have security access roles assigned and recorded in the Enterprise Systems appropriate for the roles that the staff perform, and support the requirements of least privilege and segregation of duties;
- Review that any staff who are delegated DHSA are recorded with appropriate security access roles in the Enterprise Systems appropriate for the DHSA role performed, that the roles are up-to-date, and have been personally approved by the department head;
- Review that the department's internal controls reflect any additional individual staff, transaction, amount limits or other restrictions, segregation of duties or requirements for security access roles for any staff, including security access for staff with DHSA who may not process transactions in the systems, but approve fiscal business through system workflow or electronic signatures; and
- Review of security access with broader or cross-functional access (such as staff with roles to submit both encumbrances and payments) have been reviewed, access levels are confirmed as appropriate, and that sufficient internal controls and segregation of duties are in place;

The Statewide Risk Management and Compliance Team may conduct additional desk reviews or other periodic reviews related to security access management and make recommendations for remediation or mitigation.

Contact

- CTR Solution Desk