Minnesota Management and Budget
Statewide Operating Procedure

Minnesota Management and Budget, Statewide Systems Security
Issued: July 1, 2011

Number 1101-07.1
Revised: N/A

Agency Security Administrators

Objective

Designation and responsibilities of agency security administrators for statewide systems including FMS (financial management and procurement), SEMA4 (human resources and payroll), Enterprise Learning Management (ELM) and Enterprise Performance Management (the data warehouse). These individuals are authorized to approve requests for access to statewide systems and perform security administration responsibilities delegated to the agency by Minnesota Management & Budget (MMB).

General Procedures

Step	Action	Responsible Party	Timeline
1.	Designate at least two agency security administrators to ensure someone is available to assist the agency's statewide systems users. Agencies with only self-service users or with few administrative users may designate one. Boards and others that have another agency handle their accounting, payroll and human resources functions may arrange to also have staff of that agency designated as their agency security administrator. Agencies are encouraged to select one administrator from the human resources area and one from the accounting/finance area so individuals involved are familiar with the major statewide systems.	Agency Management at a level higher than the designated administrator(s)	N/A
2.	Approve and submit the Designation of Agency Security Administrator for Statewide Systems.	Higher Level Agency Management	N/A

Step	Action	Responsible Party	Timeline
3.	Approve and submit the Designation of Agency Security Administrator for Statewide Systems. • Verify Requests have all necessary agency approval: 1. Accounting director/chief financial officer for FMS and warehouse accounting, payroll and procurement. 2. Human resources director for SEMA4 and warehouse human resources and benefits. 3. Agency ELM key administrator for Enterprise Learning. 4. Agencies may establish additional approval requirements (e.g., user's supervisor, agency chief information officer or chief information security officer). 5. Return form to employee if any required approval is missing or if any signature is not by the correct individual • Compare proposed roles to the incompatible access designations on the MMB website to determine if any pairs of roles requested are incompatible. If so, verify that the user's supervisor intended to assign incompatible access and, if so, is aware of the requirements for establishing compensating controls.	Agency Security Administrator	N/A
4.	Sign completed forms and submit to MMB Statewide Systems Security. An agency security administrator cannot sign a form for changes to his/her own security.	Agency Security Administrator	N/A
5.	Review forms and verify that they are signed by a designated security administrator for the requesting agency. As needed, request input from other MMB staff such as system owners, finance and human resources specialists and technical security staff. Contact the agency security administrator to resolve any issues. Process approved requests.	MMB Statewide Systems Security	N/A
6.	Adhere to MMB procedures and instructions for performing security responsibilities delegated to the agency. Agencies may establish additional requirements and procedures such as limiting certain security functions to specified individuals or requiring supervisor, accounting and/or human resources review before accounts are unlocked or deleted security roles restored. An agency security administrator cannot modify his/her own security record. Changes may be entered by another security administrator for the agency or by MMB statewide systems security.	Agency Security Administrator	N/A

Step	Action	Responsible Party	Timeline
7.	Verify the user's identity before making any changes to security. Unless the requester is personally known to the administrator: • Ask the employee to supply his/her name, phone number and user ID (Employee ID and, if applicable, mainframe User ID). • If the correct name and number do not appear on caller ID, contact the user at the work number from an official source such as the agency phone directory or the Request for Access form. • If the user fails identity verification, the user's supervisor or the agency HR director/designee may confirm the information.	Agency Security Administrator	N/A
8.	Provide direction to agencies for the annual confirmation of agency user security and of agency security administrator designations.	MMB Statewide Systems Security	Annually
9.	Annually review the statewide systems security of agency users to verify that they have only the access necessary to perform their jobs. This includes the review of segregation of duties conflicts described in Procedure 1101-07.2 on Compensating Controls. Submit confirmation and any changes needed to MMB Statewide Systems Security.	Agency Security Administrator	Annually
10.	Annually review and verify designated security administrators for the agency. Submit confirmation and any changes needed to MMB Statewide Systems Security.	Higher Level Agency Management	Annually
11.	Process change requests. Follow up with agencies that have not provided annual confirmations by the established deadline. Remove administrative access to statewide systems and agency security administrator access for users in agencies that fail to submit confirmations as directed.	MMB Statewide Systems Security	Within 30 days after the established deadline

Forms

Request for Access to SWIFT Statewide Systems (https://mn.gov/mmb/accounting/swift/security/security-forms.jsp)

Related Policies and Procedures

MMB Statewide Operating Policy 1101-07 Security and Access (http://mn.gov/mmb-stat/documents/accounting/fin-policies/1101-07-security-and-access-policy.pdf)

MMB Statewide Operating Procedure 1101-07.2 Compensating Controls (http://mn.gov/mmb-stat/documents/accounting/fin-policies/1101-07-02-compensating-controls-procedure.pdf)