



Agency Policies and Procedures

Issue Date: February 29, 2000
Revised Date: August 23, 2007

Policy Number: FMR-1E-01
Page: 1 of 4

Mainframe Access and Systems Security for MAPS, the Information Access Warehouse, and InfoPac/DocumentDirect Reports

Policy Objectives:

Agency policy and procedures for mainframe access and security for the Minnesota Accounting and Procurement System (MAPS), the Information Access (IA) Warehouse, and InfoPac/DocumentDirect Reports are designed to:

- Ensure security profiles are established and maintained appropriately,
- Establish a control process to periodically review and confirm access rights,
- Ensure continued compliance with Minnesota Data Practices Laws, and
- Monitor security violations regularly and resolve incidents involving unauthorized activity.

Background Information:

Access and security for MAPS, the IA Warehouse, and InfoPac/DocumentDirect Reports are essential parts of the comprehensive internal control framework established by the state. This internal control framework must provide assurance that the underlying data in the state's accounting and procurement system are reliable, the state's assets are adequately safeguarded, and that applicable legal and other mandates are followed. A sound framework of internal control is the state's primary defense against fraud.

The Department of Minnesota Management and Budget (MMB) manages MAPS, the IA Warehouse, and InfoPac/DocumentDirect Reports, provides central security administration and management, and regulates all security violations and suspensions.

Admin Financial Management & Reporting (FMR) maintains agency access and security to MAPS, the IA Warehouse, and InfoPac/DocumentDirect Reports.

All information in MAPS, the IA Warehouse and InfoPac/DocumentDirect reports is governed by the Minnesota Data Practices Act (Minnesota Statutes, Chapter 13). Certain vendor file and human resource information contained in the IA Warehouse is private, confidential information. Each user is obligated to ensure that any information which is not statutorily defined as either: 1) public data not on individuals or, 2) public data on individuals is protected from unauthorized use or exposure.

Authority:

- [Minnesota Statutes, Chapter 13, Minnesota Government Data Practices Act](#) – This statute specifies the laws and public employees' obligation to protect information that is not defined as public data, whether on individuals or not on individuals.
(http://www.revisor.leg.state.mn.us/bin/getpub.php?pubtype=STAT_CHAP&year=current&chapter=13)

- [MAPS Operations Manual Policy and Procedures 0102-01, Internal Control](#), establishes the policy that each agency head must develop a plan for establishing, implementing and maintaining an effective internal control system, including restricting access to programs and data that reside on computerized information systems. (<http://www.mmb.state.mn.us/chapter-1/201-201>)
- [MAPS Operations Manual Policy and Procedures 1101-07, Security & Access](#), establishes the policy on MAPS security and access. This policy requires each agency to designate a MAPS security liaison and provides guidelines on avoiding the use of security profiles with incompatible functions. (<http://www.mmb.state.mn.us/chapter-11/336-336>)

Business Risks:

- Without proper system security clearance, Admin employees may not have access to the tools and information necessary to fulfill their job responsibilities.
- Persons may gain unauthorized access to the state's accounting and procurement system, misuse the system for personal gain, or cause damage to, or modification/loss of, data.
- Unauthorized access to MAPS, the IA data warehouse, or InfoPac/DocumentDirect Reports may not be prevented, or detected and remedied on a timely basis.
- Persons with MAPS access may perform incompatible functions that yield opportunities for errors or irregularities to occur without timely detection.

Policies and Procedures:

PART ONE – ACQUIRING ACCESS

1. Designation of Agency Security Liaison Officer - The financial management director has authority to designate a Financial Management and Reporting Division (FMR) employee as a security liaison officer. This individual's responsibilities include, but are not limited to, the duties detailed in steps 2 through 5.
2. Process to Obtain Mainframe Logon Identification (ID)
 - A. Supervisor/manager evaluates the employee's tasks and responsibilities to determine the need for a mainframe logon ID and clearance to MAPS, the IA Warehouse, and/or InfoPac/DocumentDirect reports.
 - B. Supervisor/manager notifies the security liaison officer of the need for a mainframe logon ID and systems security clearance. Notification must be done by e-mail or written request (e-mail is preferred) to provide documentation supporting the request. The supervisor/manager must submit this request to the security liaison officer with sufficient lead time prior to when the employee needs mainframe and system access to perform his/her assigned duties to allow the security liaison officer time to complete processing the request.
 - C. Security liaison officer retains a copy of the original e-mail or written request for his/her internal records.
 - D. Financial management director or security liaison officer submits a logon ID request via Office of Enterprise Technology's (OET's) password-protected web request form. OET does not accept logon ID requests via e-mail, fax, or mail.
 - E. OET Security Services Team replies to the request via e-mail within one or two working days that contains the service request number and a link to a page on the OET web site that shows the logon ID and password.
 - F. Security liaison officer informs the supervisor/manager of the logon ID and initial password.
 - G. Supervisor/manager advises employee of the newly-assigned logon ID, the need to change the temporary password, and the requirements regarding passwords.
3. Process to Obtain MAPS Access
 - A. Supervisor/Manager evaluates the employee's tasks and responsibilities to determine the level of MAPS clearance that is needed to perform assigned tasks.
 - B. Supervisor/Manager submits a written request, including a completed [MAPS Security Questionnaire](#), to the agency security liaison officer for the employee to obtain MAPS security clearance. This request must be submitted with sufficient lead time prior to when the employee needs access to perform his/her assigned duties to allow the security liaison officer time to process the request. This request should list the MAPS activities that the employee will perform.

- C. Security liaison officer identifies the proper security profile for the employee based on the activities listed.
 - D. Security liaison officer completes a [Request for Basic Access Minnesota Accounting and Procurement System](#), form FI-00502, and forwards it to the MMB Information Services Division.
 - E. Security liaison officer retains a copy of the completed form for reference.

 - F. When the MAPS access request form is sent to MMB, the security liaison officer notifies the supervisor/manager that the request has been submitted.
 - G. MMB security officer notifies the Admin employee that s/he is authorized to use MAPS.
4. Process to Obtain Information Access (IA) Warehouse Clearance for MAPS
- A. Employee needing access to the IA Warehouse completes a [Request for Clearance Information Access Warehouse](#), form FI-00540. The employee's supervisor/manager reviews and, if appropriate, signs and submits the completed form to the security liaison officer for processing.
 - B. Security liaison officer reviews form. If request includes human resources/payroll access, submits form to human resources for signature, if appropriate, and returns to security liaison officer.
 - C. Security liaison officer signs and submits the form to MMB.
 - C. Security liaison officer retains a copy of the completed form for reference.
 - D. Security liaison officer notifies the employee that the request has been submitted.
 - E. MMB security officer notifies Admin employee that s/he is authorized to use the IA Warehouse.
5. Process to Obtain Access to InfoPac/DocumentDirect Reports
- A. Employee needing access completes a [Request For Access to DocumentDirect Reports](#), form FI-00569. The employee's supervisor/manager reviews and, if appropriate, signs and submits the form to the security liaison officer for processing.
 - B. Security liaison officer signs and, if appropriate, submits the form to the InfoPac/DocumentDirect Security unit at MMB. If request includes human resources/payroll access, submits form to human resources for signature, if appropriate, and returns to security liaison officer.
 - C. Security liaison officer retains a copy of the completed form for reference.
 - D. Security liaison officer notifies the employee that the request has been submitted.
 - E. MMB security officer notifies the Admin employee that s/he is authorized to use InfoPac/DocumentDirect Reports.

PART TWO – SECURITY MAINTENANCE

1. Supervisor's/Manager's Routine Periodic Review of Employees' MAPS, InfoPac/DocumentDirect Reports, or IA Warehouse Access
- A. Each supervisor/manager is responsible for his/her employee's system access for inquiry or processing purposes, and must notify the agency security liaison officer *immediately* by e-mail or in writing when any of the following conditions occur:
 - 1. The employee's system-related duties or responsibilities change (are reduced or expanded, but are not eliminated),
 - 2. The employee is no longer assigned system-related duties or responsibilities,
 - 3. The employee transfers to another Admin division,
 - 4. The employee transfers to another state agency or department,
 - 5. The employee terminates state service, or
 - 6. The employee is placed on administrative or investigative leave.
 - B. Agency security liaison officer prepares the appropriate form(s) and forwards the completed form(s) to MMB for further processing. These forms may include any or all of the following:
 - 1. [Request for Basic Access Minnesota Accounting and Procurement System](#), form FI-00502,
 - 2. [Request for Clearance: Information Access Warehouse](#), form FI-00540
 - 3. [Request For Access to DocumentDirect Reports](#), form FI-00569.
 - C. MMB processes the form(s) submitted by Admin to make the requested systems access changes.

2. Partnering with OET and MMB to Monitor Employee Access to MAPS, the IA Warehouse, and InfoPac/DocumentDirect Reports
 - A. Annually, the security liaison officer receives a report from OET with all logon identification numbers and their status (i.e. active, suspended, or marked for deletion). MMB distributes a certification report, usually annually, which lists all MAPS identification numbers and the security clearances assigned to each number.
 - B. Security liaison officer reviews these reports and advises Admin managers/supervisors of those employee logon IDs that are suspended or designated for termination.
 - C. Security liaison officer requests that Admin supervisors/managers complete new security questionnaires annually for all employees who require MAPS access.
 - D. Supervisors/managers review the system-related duties and responsibilities of their employees and confirm any changes to be made to each employee's security profile or the necessity for suspension or termination.
 - E. Supervisors/managers submit completed security access questionnaires to security liaison officer.
 - F. Security liaison officer prepares the appropriate form(s), listed in Part 2, item 1.B. above, changes an employee's system-related security profile and sends e-mail or forwards the completed form(s) to MMB for further processing.
3. Suspended Logon ID – A mainframe logon ID can be suspended by entering the wrong password three (3) or more times. It can also be suspended if it is not used in a 90-day period. If this occurs, the employee with the suspended logon ID contacts Administration's security liaison officer or the MMB's MAPS Security Unit to request that the logon ID be unsuspended.
4. Internal Control Issues for Security of MAPS, InfoPac/DocumentDirect Reports, and the IA Warehouse
 - A. Password protection is imperative for all systems. Each user is responsible for the information entered, observed, retrieved, or printed from any of the systems. Users are prohibited from sharing passwords or displaying them where others will see them.
 - B. Each employee is responsible for ensuring that public requests for information are forwarded to appropriate personnel for approval of the release of the information to the public in accordance with Admin's *Department Communications Guidelines*. Each division is responsible to ensure that only public information is provided to the requestor.
 - C. The supervisor/manager of an employee with MAPS access is responsible for ensuring that a separation of duties exists with user profiles. If the supervisor/manager needs assistance with user profiles, he/she should contact the security liaison officer.

Forms:

FMR-010-01, MAPS Security Questionnaire

(<http://www.admin.state.mn.us/fmr/documents/Policies%20&%20Procedures/Reference/MAPS%20Security%20Questionnaire.doc>)

FI-00502, Request for Basic Access: Minnesota Accounting & Procurement System

(<http://www.mmb.state.mn.us/doc/maps/forms/fi50204.doc>)

FI-00540, Request for Clearance: Information Access Warehouse

(<http://www.mmb.state.mn.us/doc/maps/forms/requestforclearance.pdf>)

FI-00569, Request for Access to DocumentDirect Reports

(<http://www.mmb.state.mn.us/doc/maps/forms/fi56901.doc>)

See Also:

MAPS Operations Manual Policy and Procedure 1101-01, Requesting a Mainframe Logon ID

(<http://www.mmb.state.mn.us/chapter-11/334-334>)

MAPS Operations Manual Policy and Procedure 1101-02, Requesting Basic Access to MAPS

(<http://www.mmb.state.mn.us/chapter-11/335-335>)

Department Communications Guidelines,

(http://www.mainserver.state.mn.us/admin/Communications_guidelines.html)