



Information System Access

- **Well designed access controls achieve segregation of duties in an electronic environment.**
- **Where agencies cannot enforce information system segregation of duties, they must implement compensating controls to reduce the risk of undetected errors or fraud.**

As state employees, we are immersed in a sea of information. The state manages this deluge of data by deploying information systems that collect, process, and distribute information to state employees, legislators, the public, and others.

To preserve public trust, we must maintain the integrity and confidentiality of the information for which we are responsible. Maintaining data integrity requires assurance that data is complete, accurate, and valid from collection through dissemination, and is not subject to unauthorized interference or use.

A strictly enforced access policy is a key control activity in any well-functioning information system. Access controls seek to limit each employee's access to information systems, programs, and data to the activities needed to perform his or her job functions. Strong access controls achieve segregation of duties in an electronic environment by ensuring that the four key functional responsibilities of authorization, recording, custody, and reconciliation are separated within information systems.

For example, the stated objective of Minnesota Management & Budget Operating Policy and Procedure 1101-7, *Security and Access*, is "to maintain effective internal control over accounting and purchasing functions – through system security mechanisms wherever possible, or through compensating controls." The policy identifies five categories of MAPS¹

¹ MAPS is the state's primary financial information system.

incompatible functions:

1. Purchasing and payment functions (authorization, recording, and custody),
2. Contracting and payment functions (authorization, recording, and custody),
3. Encumbering and payment functions (authorization, recording, and custody),
4. Accounts receivable functions (recording and custody), and
5. General cash receipts functions (recording and custody).

Where agencies cannot enforce information system segregation of duties because of size, staffing constraints, or other factors, they must implement compensating controls to reduce the risk of undetected errors or fraud.

Compensating controls typically include more frequent and detailed reviews of the affected transactions by a person independent of the employee with the incompatible access.

Suggested Action Step: Review the access policies for the information systems you use (e.g. for MAPS, see policy [1101-07, Security and Access](#). For SEMA4² security, see policy [HR045](#). Verify that sufficient segregations of duties and/or compensating controls exist in the duties for which you or others in your organization are responsible.

If you have any questions, please contact John Nyanjom, Internal Control Specialist, at (651) 201-8174 or John.Nyanjom@state.mn.us.

² SEMA4 is the statewide payroll, human resource and benefits system.