



---

**Financial Management and Reporting**

**Agency Policies and Procedures**

**Issue Date: March 15, 2000**  
**Revised Date:**

**Policy Number: FMR-1E-02**  
**Page: 1 of 3**

---

## **Control and Security of Customized Financial-Related Systems**

### **Policy Objectives:**

Agency policy and procedures for control and security of customized financial-related systems within each division are designed to:

- Ensure each division has a person responsible for system security and control,
- Ensure continued compliance with Minnesota Data Practices Laws,
- Ensure cost-effective control and security measures are in place to safeguard data against known vulnerabilities,
- Monitor the effectiveness of control and security measures on an on-going basis, and
- Enhance internal controls of customized financial-related systems.

### **Background Information:**

Each specific division is the owner and manager of their customized financial-related system (system). Each division is responsible to provide central security administration and management.

All information in these systems is governed by the Minnesota Data Practices Act (M.S. § 13). Certain information contained in these systems is private, confidential information. It is the obligation of each user to ensure that any classified information is protected from unauthorized use or exposure.

### **Authority:**

- **Minnesota Statute**  
[M.S. § 13 Minnesota Government Data Practices Act](https://www.revisor.leg.state.mn.us/statutes/?id=13) – This statute specifies the laws and public employees' obligation to protect classified information.  
(<https://www.revisor.leg.state.mn.us/statutes/?id=13>)
- **MAPS Operations Manual Policy and Procedures 0102-01** specifies that agencies are responsible for maintaining access controls by limiting direct physical access to computer systems.  
(<http://www.mmb.state.mn.us/chapter-1/201-201>)

### **Business Risks:**

- Without system security clearance, division employees may not have access to all of the tools and information necessary to fulfill their job responsibilities.
- Unauthorized access may result in misuse of these systems for personal gain, or damage/modification/loss of data.
- System users may cause errors and irregularities that can amount to costly losses for a division. Errors and irregularities may adversely impact the integrity, confidentiality, and availability of system data. These activities may cause strained business relationships between a division and its customers, or may diminish public confidence in the agency.
- Unauthorized access to these systems may not be prevented, or detected and remedied on a timely basis.

- Persons with system access may perform incompatible functions that may cause errors or irregularities to occur without any timely detection.

### **Policies and Procedures:**

1. Designation of a System Administrator - The manager of each division is responsible for designating an employee as a system administrator. This individual's responsibilities include, but are not limited to, the following duties detailed in steps 2 through 4 below.
2. Identify and Classify System Data
  - A. It is essential for security purposes that each system administrator identifies and maintains a complete list of the data contained in the financial-related system. Whether this information is gathered for an automated or manual system, this list should document each data type, who is accessing the data, and how often it is used.
  - B. The division manager is responsible for classifying the data consistent with Minnesota Data Practices Laws. The division manager may involve the data owners and end users in this process.
3. Identify Vulnerabilities - The system administrator should identify and document the types of vulnerabilities associated with each system. Examples of vulnerabilities include:
  - A. Human errors and irregularities - System users may perform accidental or intentional acts, such as errors, omissions, modifications, destruction, misuse, disclosure, fraud, sabotage, and negligence.
  - B. Internal threats - Disgruntled employees pose a serious threat to a valuable system; with legitimate access, a disgruntled employee may modify or destroy a system.
4. Identify, Select, and Implement Cost-effective Security and Control Measures - It is the responsibility of division management, in partnership with the system administrator, to identify, select, and implement cost-effective protective measures to guard against the vulnerabilities identified in step 3 above. Protective measures may include, but are not limited to, the following items:
  - A. Control and security-conscious environment - Employees represent the front-line of defense against control weaknesses and security threats to a system. Training in system controls and security should be provided so as to help create an environment of this type.
  - B. User access classification - System users should be identified as having limited or unlimited access. This will facilitate access control decisions. The system administrator must keep an updated roster of all users and their security profiles. Any changes to this roster must be routed to the system administrator.
  - C. Access controls - Access to the system should be restricted to those individuals who need it to perform specific assigned duties. Users should obtain security clearance from the system administrator before being granted access to sensitive or protected data.
  - D. Integrity controls - Control mechanisms should be used to:
    1. Prevent all users from modifying the software application, or updating and deleting historical data,
    2. Protect the system from power failures, computer crashes, or corruption from viruses,
    3. Enable rapid recovery of data and operations in the event of a disaster, and
    4. Ensure the availability of consistent, reliable, and timely data to the users.
5. Evaluate the effectiveness of control and security measures - Division management is responsible for taking appropriate actions to evaluate the effectiveness of control and security measures on an ongoing basis. These evaluations should determine whether the measures are operating effectively as designed. Evaluations require careful analysis, testing, verification of results, and reporting and correcting problems that come to one's attention.

6. Internal Control Issues for Security of Customized Financial-Related Systems

- A. Password protection is imperative for all systems. Each user is responsible for the information entered, observed, retrieved, or printed from a system. 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. It is each division's responsibility to ensure that only public information is provided to the requestor.
- C. The supervisor/manager of an employee with system access is responsible for ensuring that a separation of duties exists with user access classification and security profiles. If the supervisor/manager needs assistance in determining proper employee access classification, he/she should contact the system administrator.