



# MINNESOTA STATE STANDARD

From the Office of Carolyn Parnell  
Chief Information Officer, State of Minnesota

**Version:** 1.00  
**Approved Date:** 4/29/2011  
**Approval:** Signature on file

---

## Enterprise Information Security Training and Awareness

### Standard Statement

Government entities must institute information security awareness and education that provides:

- General security awareness for all employees and contractors
- Specific role-based security training for information system users, technical staff, and security professionals
- Evidence of individual information security training activities and reporting as required

### General Information Security Awareness

Government entities must develop and provide general information *security awareness training* for all individuals with access to entity information and information systems. The content includes, at a minimum:

- A basic understanding of the need for information security
- The individual's broad responsibilities in protecting entity information and information systems
- Appropriate actions for responding to suspected security incidents

Security awareness training and materials must be provided:

- As part of initial user training
- As required based on changes in business processes, environments, technology, or role
- At intervals to meet entity-specific requirements or at least once every two years

### Role Specific Information Security Training

When government entities develop *individual training and development plans* (IDPs), they must include relevant information security training and data practices requirements for information handling.

### Aggregate and Report Results

Government entities must maintain records of individual information security training activities including both basic awareness and individual information security training.

Aggregate results must be reported to the Office of Enterprise Technology (OET) on a periodic basis.

## Reason for the Standard

In order to create a security conscious workforce, ensure appropriately trained personnel for organizational security roles, and to comply with the Enterprise Security Operational Control Policy, OC05 – Awareness and Training, the minimum requirements for security awareness training are identified in this standard. These requirements are designed to help ensure individuals possess the required knowledge and competence for their role related to the security of information and information systems.

## Roles & Responsibilities

Role	Responsibilities
Office of Enterprise Technology (OET)	<ul style="list-style-type: none"> <li>• Maintain this document and related templates and guidelines</li> <li>• Fulfill the Government Entity roles and responsibilities for the Office of Enterprise Technology</li> <li>• Provide general awareness and training materials that are applicable to all employees and contractors of the enterprise</li> </ul>
Government Entity	<ul style="list-style-type: none"> <li>• Integrate the security awareness and education requirements of this standard into established business processes</li> <li>• Maintain the necessary processes to address the requirements of this standard</li> <li>• Report on training results as necessary</li> <li>• Implement additional training and education as necessary to address entity specific regulatory requirements</li> <li>• Implement security training as part of training programs mandated by MMB's Administrative Procedure 21</li> <li>• Periodically review security awareness efforts for effectiveness</li> </ul>

## Applicability and Exclusions

This standard is applicable to the government entities in the Executive Branch identified in the Enterprise Security Program Applicability Standard 2009-06. It is also offered as guidance to other government entities outside the Executive Branch.

Agency Heads, Chief Information Officers, Chief Information Security Officers, Data Practices Compliance Officials, and their designees who are responsible training and educating users on their security roles and responsibilities must be aware of this standard.

The requirements of this standard must be incorporated into agreements with third parties to ensure that all individuals with access to government entity information assets or information systems are informed and aware of their responsibility in protecting state data.

## Compliance

Compliance with this standard is required within 2 years of the approval date of the standard.

## Related Information

### Regulatory, Policy, Standards, & Guideline References

- Minnesota Statutes 2007 Chapter 16E (Office of Enterprise Technology)
- Minnesota Statutes, Chapter 13 (Data Practices Act)
- Minnesota Statutes, [Chapter 43A.21 \(Training Programs\)](#)
- [Admin Procedures #21](#)
- Enterprise Security Operational Control Policies

- NIST Special Publication 800-50 (Building an Information Technology Security Awareness and Training Program)
- NIST Special Publication 800-16 (Information Security Training Requirements: A Role- and Performance-Based Model)

### Forms, Templates, and Procedures

- Enterprise Security Authorization Decision template
- Italicized terms can be found in the Enterprise Security Glossary of Terms.

## History

### *Revision History – record additions as Major releases, edits/corrections as Minor*

Date	Author	Description	Major #	Minor #
05/05/2011	Eric Breece	Initial Release	1	00

### *Review History – periodic reviews to ensure compliance with program*

Date	Reviewer	Description	Compliance
n/a			
n/a			

### *Approval History – record of approval phases*

Phase	Description	Date
SME	Aaron Molenaar, Enterprise Security Office Eric Breece, Enterprise Security Office	07/27/2011
ISC	Information Security Council Approval	11/03/2011
CIO Team	All CIO Team	01/27/2011