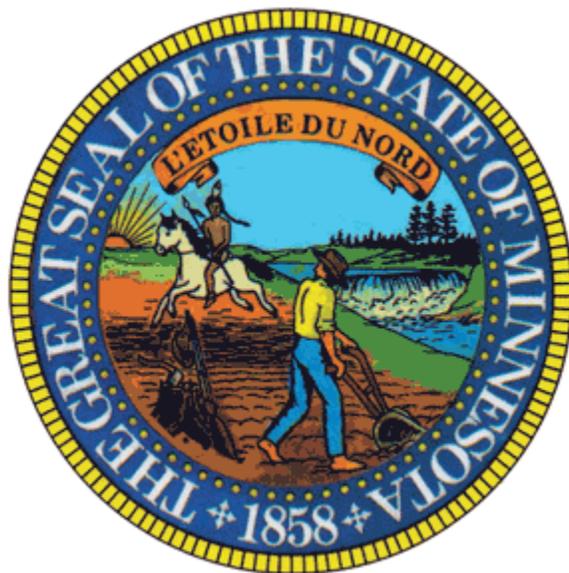


# State of Minnesota



## Enterprise Information Security Incident Management Standard

Office of Enterprise Technology

Enterprise Security Office Standard

Version 1.00

State CIO Standard Approval:

**Gopal Khanna**

<Signature on file with the ESO>

12/23/2009

State Chief Information Officer

Signature

Approval Date



# Enterprise Security Office Standard

## Table of Contents

<b>1.0 STANDARD STATEMENT</b> .....	<b>3</b>
1.1 RESOURCE REQUIREMENT .....	3
1.2 STATE CISO NOTIFICATION REQUIREMENT .....	3
1.3 ESCALATION REQUIREMENTS .....	3
1.4 REPORTING REQUIREMENTS .....	3
<b>2.0 ROLES &amp; RESPONSIBILITIES</b> .....	<b>4</b>
2.1 OFFICE OF ENTERPRISE TECHNOLOGY (OET) - ENTERPRISE SECURITY OFFICE (ESO) .....	4
2.2 GOVERNMENT ENTITY .....	4
<b>3.0 RELATED INFORMATION</b> .....	<b>5</b>
3.1 REASON FOR THE STANDARD .....	5
3.2 APPLICABILITY AND EXCLUSIONS .....	5
3.3 REGULATORY, POLICY, STANDARDS, & GUIDELINE REFERENCES .....	5
3.4 FORMS, TEMPLATES, AND PROCEDURES .....	5
3.5 COMPLIANCE .....	5
<b>HISTORY &amp; OWNERSHIP</b> .....	<b>6</b>
REVISION HISTORY – RECORD ADDITIONS AS MAJOR RELEASES, EDITS/CORRECTIONS AS MINOR .....	6
REVIEW HISTORY – PERIODIC REVIEWS TO ENSURE COMPLIANCE WITH PROGRAM .....	6
APPROVAL HISTORY – RECORD OF APPROVAL PHASES .....	6
OWNERSHIP – CURRENT OWNERS OF THE DOCUMENT .....	6



## Enterprise Security Office Standard

### 1.0 Standard Statement

In order to minimize the impact of security incidents on the Executive branch and comply with the Enterprise Information Security Incident Management Policy the minimum control requirements for the identification and reporting of security incidents affecting information assets must be implemented.

#### 1.1 Resource Requirement

Government entities must make resources available to respond to security incidents

#### 1.2 State CISO Notification Requirement

The State CISO must be immediately notified when there is a security incident that has the potential of requiring broad public disclosure or garner the news media's attention.

#### 1.3 Escalation Requirements

Unless otherwise prohibited by law, Government entities must escalate security incidents (FORM-MN-ISIRT Incident Reporting Sheet) to the Enterprise Security Office within 24 hours of validating the incident has one or more of the following characteristics:

- The incident has the potential of impacting another government entity or originated from another government entity
- The incident has the potential of impacting an enterprise system (MNet, Enterprise Email, etc.)
- The incident requires public disclosure above a threshold that would garner media attention
- The incident requires notification to the Office of the Governor, Minnesota Management and Budget, Office of Legislative Auditor, law enforcement, or a federal agency
- Incident notification originated from a third party

#### 1.4 Reporting Requirements

Government entities must be able to provide to the Enterprise Security Office the following security incidents reports:

- Full Incident Reports related to security incidents affecting the Executive branch
- Executive Summary Incident Reports (FORM-Security Incident Executive Summary for the CISO) related to security incidents affecting government entity specific, mission critical information assets
- Aggregated Security Incident Data Reports (FORM-MN-ISIRT-Monthly Report) for any operational security event & incident data collected (e.g., Malware, isolated incidents, etc.)



## Enterprise Security Office Standard

### 2.0 Roles & Responsibilities

#### 2.1 Office of Enterprise Technology (OET) - Enterprise Security Office (ESO)

- Maintain this document
- Maintain corresponding standards, templates, and guideline documents
- Collect aggregate security incident metrics for the purpose of security reporting
- Notify Executive Branch government entities of security incidents that have a potential *threat* beyond the originating entity or require immediate mitigating actions
- Notify Department of Homeland Security of cyber security *threat* level changes through the Multi-State Information Sharing and Analysis Center (MS-ISAC)
- Create and maintain authorization agreements with *government entities* so that specific named Enterprise Security Office (ESO) staff may work with protected agency data during investigations. Such agreements may be for the term of the investigation or for a longer period
- Maintain the enterprise security incident management procedures to manage enterprise level security incidents and to assist in responding to *security incidents* affecting multiple agencies
- Provide security incident response assistance to other *government entities* as needed
- Coordinate notifications of Enterprise Security Incidents to the Office of the Governor, Office of Legislative Auditor, and other entities as necessary

#### 2.2 Government Entity

- Maintain government entity-specific security incident management procedures that address the recording and prioritization of security events, and the identification, prioritization, classification, and investigation of security incidents (see Enterprise Information Security Incident Management Guideline).
- Assign values to information systems based on data classification, data sensitivity, impact to state services, and threat to health or safety (see Appendix A)
- Notify Enterprise Security Office of active security incidents
- Provide security incident management assistance as necessary
- Agency Chief Information Security Officer (CISO)/equivalent (or designee) shall collect and provide to the Enterprise Security Office aggregate reporting security incident metrics
- Provide to the State CISO executive summaries of security incidents
- Enter into Agreements with the Enterprise Security Office so that specific named ESO staff may work with the government entity's data during investigations
- Ensure that third party contracts are in compliance with this standard
- Provide ESO access to all necessary data to complete an enterprise security incident investigation
- Fulfill responsibilities for breach notification in accordance with regulatory and statutory requirements



## Enterprise Security Office Standard

### 3.0 Related Information

#### 3.1 Reason for the Standard

Incident management processes are essential to help reduce the overall reputational and regulatory risks posed by breaches in security. The proper management of security incidents must also be done to ensure the integrity of any security breach investigation.

Government entity and enterprise procedures for the management and reporting of information security incidents must have a consistent approach across the Executive branch to ensure the proper identification and reporting of security incidents. The requirements defined in this standard are designed to identify and report on security events and incidents across the Executive branch.

#### 3.2 Applicability and Exclusions

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

Agency Heads, Responsible Authorities, Chief Information Officers, Chief Information Security Officers, Data Practices Compliance Officials, and their designees who are responsible for responding to, management of, and reporting on security incidents must be aware of this standard

This requirements of this standard must be incorporated into agreements with third parties to ensure proper notification of information security incidents and their impact on state information assets.

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

Minnesota Statutes 2007 Chapter 16E (Office of Enterprise Technology)  
Minnesota Statutes, Chapter 13 (Data Practices Act)  
Minnesota Statutes, section 13.055 (State Agencies; Disclosure of Breach in Security)

Enterprise Information Security Incident Management Policy  
Enterprise Information Security Incident Management Guideline  
Enterprise Security Program Applicability Standard

#### 3.4 Forms, Templates, and Procedures

FORM-MN-ISIRT Incident Reporting Sheet  
FORM-MN-ISIRT-Monthly Report  
FORM-Security Incident Executive Summary for the CISO  
SAMPLE-Security Incident Executive Summary for the CISO  
*Italicized* terms can be found in the Enterprise Security Glossary of Terms

#### 3.5 Compliance

Compliance with this standard is required within 1 year of the approval date of the standard.



## Enterprise Security Office Standard

### History & Ownership

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

Date	Author	Description	Major #	Minor #
12/23/2009	David Appleby	Initial Release	1	00

Review History – periodic reviews to ensure compliance with program

Date	Reviewer	Description	Compliance

Approval History – record of approval phases

Phase	Description	Date
SME	Steve Busarow MSRS Marc Klein Department of Public Safety Brian Matheson Minnesota Pollution Control Agency Patrick Pueringer MN DEED Scott Phalen City of Saint Paul Eric Christensen Minnesota Department of Health Debbie Leithauser MN DoLI Bruce Showel Minnesota Department of Revenue Melinda Mattox Hennepin County John Israel Enterprise Security Office Terry Seiple Enterprise Security Office Catherine Scott IPAD John Ladwig MNSCU David Appleby Enterprise Security Office Eric Breece Enterprise Security Office	10/02/2008
ISC	Information Security Council Approval	11/04/2009
CIOC	CIO Council Approval	12/17/2009

Ownership – current owners of the document

	Owner	Division	Department
Primary	Rick Ensenbach	Enterprise Security Office (ESO)	Enterprise Security Governance
Secondary	Eric Breece	Enterprise Security Office (ESO)	Enterprise Security Governance