

State of Minnesota



Enterprise Information Security Incident Management Policy

Office of Enterprise Technology

Enterprise Security Office Policy

Version 1.00

State CIO Policy Approval:

Gopal Khanna

<Signature on File with Enterprise Security Office>

October 2nd, 2008

State Chief Information Officer	Signature	Approval Date
---------------------------------	-----------	---------------



Enterprise Security Office Policy

Table of Contents

POLICY STATEMENT	2
REASON FOR POLICY	2
APPLICABILITY AND EXCLUSIONS	2
RELATED INFORMATION	2
COMPLIANCE	2
FORMS AND INSTRUCTIONS	2
ROLES & RESPONSIBILITIES	3
OFFICE OF ENTERPRISE TECHNOLOGY – ENTERPRISE SECURITY OFFICE DIVISION	3
OFFICE OF ENTERPRISE TECHNOLOGY – ENTERPRISE TECHNOLOGY SERVICES DIVISION	3
GOVERNMENT ENTITY	3
GLOSSARY	4
E.....	4
G	4
I.....	4
L.....	4
R.....	4
S.....	4
T.....	4
V	5
HISTORY & OWNERSHIP	5
REVISION HISTORY – RECORD ADDITIONS AS MAJOR RELEASES, EDITS/CORRECTIONS AS MINOR.....	5
REVIEW HISTORY – PERIODIC REVIEWS TO ENSURE COMPLIANCE WITH PROGRAM	5
APPROVAL HISTORY – RECORD OF APPROVAL PHASES	5
OWNERSHIP – CURRENT OWNERS OF THE DOCUMENT	5



Enterprise Security Office Policy

Policy Statement

All government entities of the Executive Branch of state government must manage information *security incidents*. Security incident management must contain the following:

- Recording of *security events*
- Prioritization of *security events*
- Identification and prioritization of *security incidents*
- Classification of *security incidents*
- Investigation of *security incidents*
- Reporting of *security incidents*

Reason for Policy

Adopting an enterprise approach to security incident management will help the state identify and respond to security incidents in a more timely and effective manner. It will also help clarify expectations and promote a consistent approach in responding to information security incidents. In addition, it will provide a better understanding of the security posture across the Executive Branch through metrics based reporting of security incidents.

Applicability and Exclusions

This policy is applicable to all *government entities* in the Executive Branch of state government that manage systems that handle, store, or transfer *government data*. It is also offered as guidance to other *government entities* outside the Executive Branch.

Agency Head, Chief Information Officer, and Chief Information Security Officers, Data Practices Compliance Officials, and their designees who are responsible for the management of and reporting on agency security controls must be aware of this policy.

Any third party contracted by a government entity to handle/process, transmit, store, or dispose of Government data or handle electronic media on behalf of the State.

Related Information

Minnesota Statutes 2007 Chapter 16E ([Office of Enterprise Technology](#))

Minnesota Statutes 2007 Chapter 13 ([Data Practices Act](#))

Information Security Incident Management Standard

Information Asset Valuation Standard

Compliance

Compliance with this policy is required within two years (24 months) from approval date.

Forms and Instructions

Forms and instructions related to the recording, prioritizing, classifying and reporting of *security events* and *security incidents* are included in the Information Security Incident Management Standard.

Terms in *italics* can be found in the glossary section of this document.

Requests for changes and additions to this document may be submitted to the Enterprise Security Office for consideration. All submissions must include the specific change and a detailed reason for the change.



Enterprise Security Office Policy

Roles & Responsibilities

Office of Enterprise Technology – Enterprise Security Office Division

1. Maintain this document
2. Maintain corresponding standards documents and reporting requirements for incident management
3. Maintain a set of procedures and templates for consistent incident response process implementation
4. Collect and provide aggregate reporting on security incident metrics
5. Notify other Executive Branch government entities of security incidents that are a potential *threat* to the entire Executive Branch or require immediate mitigating actions
6. Notify Department of Homeland Security of cyber security *threat* level changes through the Multi-state Information Sharing and Analysis Center (MS-ISAC)

Office of Enterprise Technology – Enterprise Technology Services Division

1. Fulfill the Government Entity roles and responsibilities for the Office of Enterprise Technology
2. Maintain the enterprise security incident management procedures to manage enterprise level security incidents and cross agency security incidents
3. Provide security incident assistance to other government entities as necessary

Government Entity

1. Maintain entity-specific security incident management procedures in accordance with the enterprise security policies, standards, and other applicable regulatory or legal requirements
2. Provide security incident metrics in accordance with enterprise security standards
3. Notify Enterprise Security Office of active security incidents that pose a *risk* to the enterprise in accordance with enterprise security standards
4. Assign values to information systems based on data classification, impact to state services, and threat to health or safety
5. Provide security incident management assistance as necessary
6. Ensure that third party contracts are in compliance with this policy



Glossary

E

Event:

An identifiable occurrence of activity that has significance for a system and typically represents some outcome.

G

Government Data:

All data collected, created, received, maintained or disseminated by any government entity regardless of its physical form, storage media or conditions of use.

Government Entity:

Any office, department, division, bureau, board, commission, authority, district, or agency in Minnesota state government.

I

Incident:

Any event which is not part of a standard operation that requires an action or a response.

L

Likelihood:

Determining the probability of a future event or circumstance based on the measure of past events or current state. Making an(a) inference, assumption, or distinction about the quality or complexity of future events or patterns based on the qualitative measure of past events.

R

Risk:

The *likelihood* of a *threat* exploiting a *vulnerability* and the resulting impact.

S

Security Event:

A notification of logged or reported *event(s)* that is/are suspected to be a *security incident*, but has not been validated.

Security Incident:

A security event that has been validated to be a violation of policy, has had an adverse effect on government data or the delivery of state services, or is a *threat* to health and safety.

T

Threat:



Enterprise Security Office Policy

A natural, human, or environmental source with the intent or opportunity to trigger the exploitation of a *vulnerability*.

V

Vulnerability:

A flaw or weakness in a process, design, implementation, control, system, or organization that could be triggered or intentionally exploited, resulting in a *security incident* or breach.

History & Ownership

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

Date	Author	Description	Major #	Minor #
10/02/2008	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	INT
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	02/06/2008	
ISC	Information Security Council Approval	03/20/2008	
CIOC	CIO Council Review	06/19/2008	
CAB	Commissioners' Advisory Board Review	09/11/2008	

Ownership – current owners of the document

	Owner	Division	Department
Primary	Deb Stafford	Enterprise Security Office (ESO)	Investigative & Corrective Controls
Secondary	David Appleby	Enterprise Security Office (ESO)	Investigative & Corrective Controls