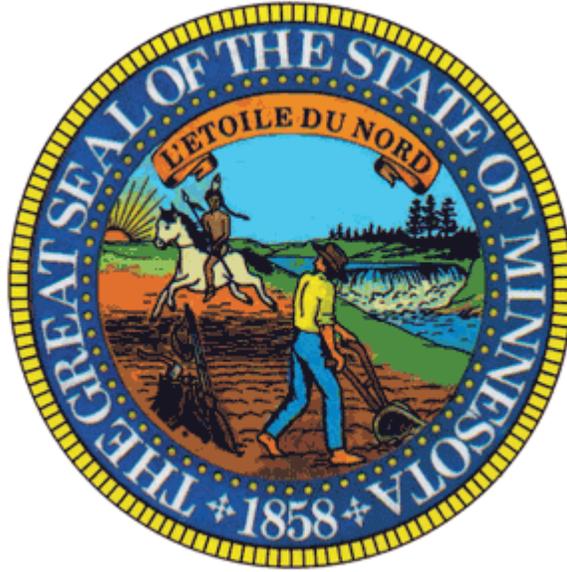


State of Minnesota



Office of Enterprise Technology

Enterprise Security Management Control Policies

Enterprise Security Office Policy

Version 1.00

Approval:

Gopal Khanna	<Signature on file with ESO>	03/24/2010
State Chief Information Officer	Signature	Approval Date



Table of Contents

MANAGEMENT CONTROLS	3
MC01 – RISK MANAGEMENT POLICY	3
MC02 – SECURITY PLANNING AND LIFE CYCLE POLICY	3
MC03 – SECURITY AUTHORIZATION POLICY.....	3
REASON FOR POLICIES	3
COMPLIANCE	3
RELATED INFORMATION	3
FORMS AND INSTRUCTIONS	3
APPLICABILITY AND EXCLUSIONS	4
ROLES & RESPONSIBILITIES	4
OFFICE OF ENTERPRISE TECHNOLOGY – ENTERPRISE SECURITY OFFICE	4
OFFICE OF ENTERPRISE TECHNOLOGY – ENTERPRISE TECHNOLOGY SERVICES.....	4
GOVERNMENT ENTITY	4
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



Management Controls

The Management Control policies are the foundation for an information security risk management program. The management of risk is an integral part of doing business and must be treated as a management function, not as a technical function. This requires policies that are owned, supported, and practiced by management to address risks to an organization's information assets.

MC01 – Risk Management Policy

All government entities must identify and assess the risks to information assets and manage the potential impact on organizational operations, systems, and individuals.

MC02 – Security Planning and Life Cycle Policy

Government entities must have a process to document and address security risks to information assets throughout the asset's life cycle. The process must determine appropriate, cost-effective safeguards and countermeasures for both the development and acquisition of systems.

MC03 – Security Authorization Policy

Government entities must certify that controls appropriately mitigate security risks and residual risk is accepted by a level of management that has the authority to accept residual risk on behalf of the organization.

Reason for Policies

These policies are necessary to define risk management requirements that will help organization leaders with making reasonable and appropriate risk management decisions. Proper identification, mitigation and management of security risks will reduce the likelihood of a threat having an impact on the State's services, public health and safety, or government data.

These policies will also help ensure that security risks are properly managed during the initiation, development or acquisition, implementation, operation and maintenance, and disposition phases of life cycle planning.

These policies have an inherit reporting requirement that is necessary to create a consolidated enterprise risk profile of the Executive Branch. The consolidated report of a defined set of metrics will be used to identify trends, areas needing improvement, changes with controls, emerging/recurring risks, and to help identify appropriate funding necessary to mitigate new risks.

Compliance

Compliance to this policy is required within 24 months from approval date of related standards

Related Information

[Minnesota Statutes 16E](#) Office of Enterprise Technology
[Minnesota Statute 13](#) Data Practices

Forms and Instructions

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



Enterprise Security Office Policy

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 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.

Roles & Responsibilities

Office of Enterprise Technology – Enterprise Security Office

1. Maintain this document and related standards, guidelines, and processes
2. Maintain an enterprise information security risk management program
3. Collect and create a consolidated risk profile of the Executive branch

Office of Enterprise Technology – Enterprise Technology Services

1. Fulfill the Government Entity roles and responsibilities for the Office of Enterprise Technology

Government Entity

1. Implement and manage an information security risk management program
2. Report on risk management activities as necessary



Enterprise Security Office Policy

History & Ownership

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

Date	Author	Description	Major #	Minor #
03/24/2010	Eric Breece	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	Enterprise Security Office Approval	02/03/2009
ISC	Information Security Council Approval	02/10/2010
CIOC	CIO Council Approval	03/18/2010

Ownership – current owners of the document

	Owner	Division	Department
Primary	Chris Buse	Enterprise Security Office (ESO)	Planning & Preventive Controls
Secondary	Eric Breece	Enterprise Security Office (ESO)	Planning & Preventive Controls