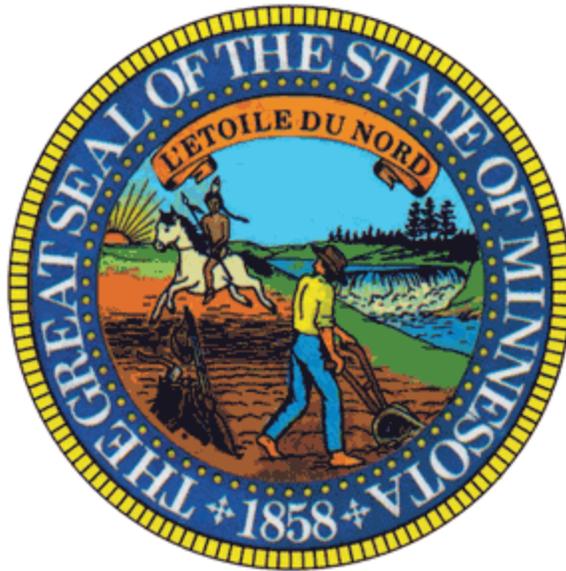


State of Minnesota



Enterprise Security Program Policy

Office of Enterprise Technology

Enterprise Security Office Policy

Version 1.00

Approval:

Gopal Khanna	(Signature on file with the ESO)	06/22/2009
State Chief Information Officer	Signature	Approval Date



Table of Contents

POLICY STATEMENT	3
REASON FOR THE PROGRAM	3
RELATED INFORMATION	3
FORMS AND INSTRUCTIONS	3
APPLICABILITY AND EXCLUSIONS	4
ROLES & RESPONSIBILITIES	5
STATE CHIEF INFORMATION OFFICER	5
STATE CHIEF INFORMATION SECURITY OFFICER	5
INFORMATION SECURITY COUNCIL (ISC)	5
GOVERNMENT ENTITY	5
PROGRAM FRAMEWORK	6
PROGRAM COMPLIANCE	7
ENTERPRISE SECURITY GOVERNANCE	7
POLICY APPROVAL PROCESS	8
STANDARDS APPROVAL PROCESS	9
POLICY AND STANDARDS EXCEPTION PROCESS	10
HISTORY & OWNERSHIP	11
REVISION HISTORY – RECORD ADDITIONS AS MAJOR RELEASES, EDITS/CORRECTIONS AS MINOR	11
REVIEW HISTORY – PERIODIC REVIEWS TO ENSURE COMPLIANCE WITH PROGRAM	11
APPROVAL HISTORY – RECORD OF APPROVAL PHASES	11
OWNERSHIP – CURRENT OWNERS OF THE DOCUMENT	11



Enterprise Security Office Policy

Policy Statement

In order to achieve the statutory requirements in Minnesota Statutes Chapter 16E ([Office of Enterprise Technology](#)) for cyber security, the State of Minnesota will have a comprehensive information security program (the Enterprise Security Program) to protect information assets and comply with regulatory requirements.

Reason for the Program

It is important for all impacted stakeholders to understand the authority for the Enterprise Security Program, its scope, and key roles and responsibilities. Under Minnesota Statutes, Chapter 16E, the State Chief Information Officer (CIO) has the authority and responsibility to define cyber security policies, standards, and guidelines for the executive branch. The State CIO also has authority to install and administer security systems.

In order to implement the Enterprise Security Program and determine appropriate security systems, the State CIO delegates all security-related responsibilities to the State Chief Information Security Officer (CISO). Through the Information Security Council, government entities will have an opportunity to participate in the design and implementation of the policies, standards, and security systems.

Related Information

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

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

Enterprise Security Program Applicability Standard

Enterprise Security Strategic Plan

Enterprise Architecture Program

This policy supersedes the Enterprise Security Program Charter Policy

This policy supersedes the Enterprise Security Compliance Policy

This policy supersedes the Information Security Council Creation Policy

Forms and Instructions

Enterprise Policy/Standard Exception Request form

Terms in *italics* can be found in the Enterprise Security Glossary document.



Enterprise Security Office Policy

Applicability and Exclusions

These policies are applicable to all *government entities* in the Executive Branch of state government. It is also offered as guidance to other *government entities* outside the Executive Branch.

Government entities in the Executive Branch include all the heads, elected or appointed, of any entity established by statute or constitution, and all of the employees within those entities. A comprehensive list of government entities will be maintained by the State CISO in the Enterprise Security Program Applicability Standard.

Agency heads, Chief Information Officers, agency security leaders, and their designees that are part of the Executive branch who are responsible for the management of and reporting on agency security controls must be aware of this policy.

Policy requirements are applicable to any arrangement with third parties that handle, store, or transfer *government data*.

Exclusions to this program include all entities that are not part of the Executive Branch, as defined by the Enterprise Security Program Applicability Standard.



Roles & Responsibilities

State Chief Information Officer

- Provide final approval of all enterprise security policies and standards
- Approve exceptions to enterprise security policies and standards
- Delegate the statutory responsibility for the protection of information assets to the State Chief Information Security Officer

State Chief Information Security Officer

- Serve as Chair of the Information Security Council
- Develop and manage the enterprise security strategic plan
- Develop and enforce baseline information security policies and standards to protect the State of Minnesota's information assets
- Ensure that baseline security policies and standards follow enterprise governance processes
- Oversee the installation and administration of enterprise security systems
- Report on the fiscal requirements and implications of maintaining the Enterprise Security Program.
- Provide assistance to government entities on implementation and compliance with the security objectives of the Enterprise Security Program
- Maintain a list of government entities that must comply with the Enterprise Security Program
- Review and provide recommendation for exceptions to enterprise security policies and standards

Information Security Council (ISC)

- Assist with the development, review, and approval of enterprise security policies and standards
- Assist with prioritizing security initiatives in support of the enterprise security strategic plan
- Review and provide recommendation for exceptions to enterprise security policies and standards
- Monitor enterprise security policies, procedures, and standards for continued applicability and appropriateness

Government Entity

- Participate in the ISC as resources permit
- Comply with enterprise security policies and standards
- Communicate enterprise security policies and standards to impacted employees, contractors, and third parties
- Develop and maintain additional policies and standards to address entity specific regulatory requirements or other needs
- Install and administer government entity security systems



Enterprise Security Office Policy

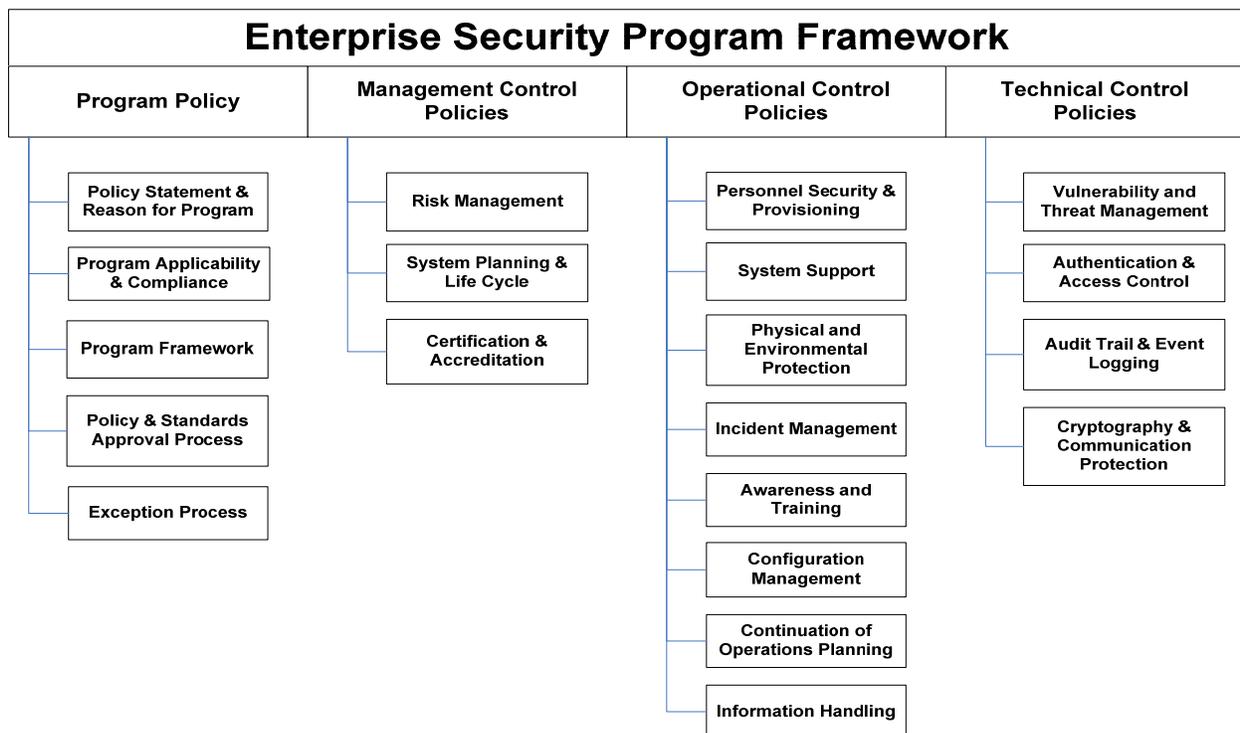
Program Framework

The Enterprise Security Program uses the 800 series of publications by the National Institute of Standards and Technology's (NIST) as a framework. The NIST 800 series has been adapted to accommodate the unique model of Minnesota's government

The program is divided into four components that contain high level policies. Each program area may be supported by one or more Enterprise Security Standards. These standards will be documented separately, but governed by this program and the processes defined in this document.

- **Program Policy** – Identifies the overall purpose, scope, and governance requirements of the security program as a whole.
- **Management Control Policies** – Contains the policies necessary to address risk throughout the life cycle of the State's information assets. The identification, tracking, and reporting of risk is essential for any organization's leadership to make appropriate financial and operational decisions on risk mitigation.
- **Operational Control Policies** – Contains the policies that define a class of security controls implemented and executed by people. These controls support the management controls with processes or actions required to reduce identified risks and often rely on the technical controls.
- **Technical Control Policies** – Contains the policies that define a class of security controls executed or used by systems. They can be automated controls that facilitate the detection of security violations or technologies used by systems to enforce operational security requirements.

Figure 1: Map to the overall set of policies contained within the program documentation





Enterprise Security Office Policy

Program Compliance

The executive branch of Minnesota State Government must monitor and report on compliance to the enterprise security policies and standards, collectively known as the Enterprise Security Program and applicable federal, state, and regulatory requirements.

The Enterprise Security Office (ESO) will assess and monitor the program compliance across the government entities of the Executive branch. The ESO will do this through the following activities:

- Develop and maintain an Enterprise security *audit* plan.
- Monitor for violations of enterprise policies and standards.
- Conduct *audits* and *assessments* of Executive branch entities' information security business objectives, controls, processes, and procedures are effectively applied and maintained, and perform as expected.
- Identify and report on Key Performance Indicators (KPI) for compliance reporting.
- Communicate the *audit* plan to the Governor's Office.
- Present *audit* schedule to other necessary bodies.
- Evaluate this policy and related standard for effectiveness.
- When necessary, coordinate the security assessments, evaluations, and audits activities by third-parties, Office of the Legislator Auditor (OLA), and regulatory agencies.
- Work with agencies to identify compliance gaps and potential mitigating controls, and manage the exceptions process and assist with formal risk acceptance.
- Report on Enterprise Security Program compliance status to the Governor's Office, State CIO, and other bodies as necessary.

Government entities of the Executive branch will assess, monitor, and report on their own compliance to the program and other regulatory requirements. Government entities will do this through the following activities:

- Align resources for and in cooperation with Enterprise Security Office (ESO) compliance assessments.
- Notify the ESO of third party, OLA, and Federal regulatory assessments, evaluations, and audits of information systems.
- Provide the ESO a detailed copy of all results from any third party, OLA, and Federal regulatory assessment, evaluations, and audits of information systems.
- Report remediation efforts to the ESO and take corrective action as required in a timely fashion.
- Assess and report on security compliance status to Enterprise Security Office (ESO).

Enterprise Security Governance

Each policy within the program must fall under one of the three control areas (Management, Operational, or Technical) within the program framework. Each standard within the program must support the Program Policy, or one (or more) of the policies within the three policy control areas of the program framework.

Periodic review of the policies and standards for applicability and appropriateness will be conducted at least once every two years.

The following processes must be used to create, change, periodically review, and approve enterprise security policies and standards.

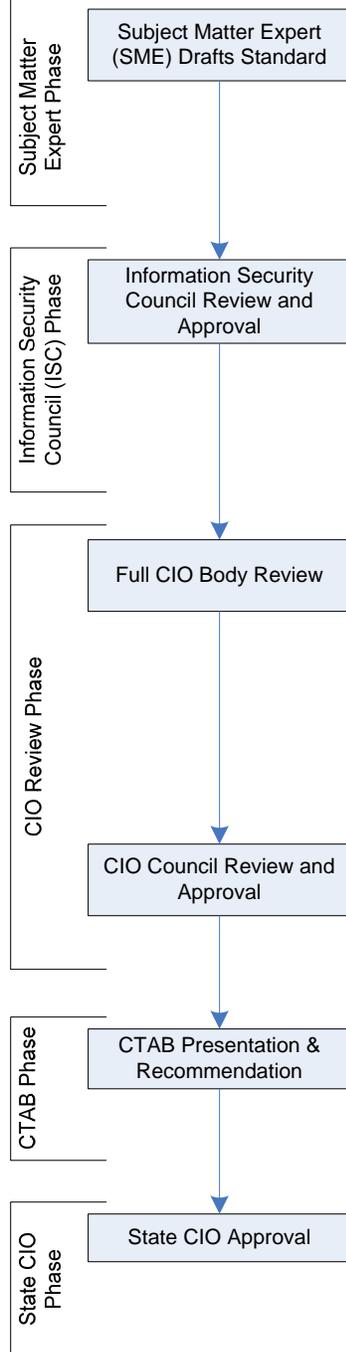


Enterprise Security Office Policy

Policy Approval Process

To add an enterprise security policy to the program or revise the Program Policy, the following process must be used to draft/revise, review, and approve the policy.

Process Flow:



Process Steps:

1. Initial draft and vetting of policy by Subject Matter Expert (SME):
 - a. Policy owner and SME working group draft the policy
 - b. Initial draft is presented to the program management team for feedback
 - c. State CISO approves policy to move onto the ISC review phase
2. Vetting of policy by the Information Security Council (ISC):
 - a. Draft policy is presented to the ISC at next scheduled meeting
 - b. ISC members have at least 30 days to review policy and provide documented feedback to Enterprise Security
 - c. Enterprise Security consolidates feedback and updates draft
 - d. Present updated draft to ISC for approval to move on to the CIO review phase
3. Full CIO body review and feedback:
 - a. Enterprise Security presents draft to the full CIO body
 - b. Full CIO body members have at least three weeks to review
 - c. CIO body members provides documented feedback to Enterprise Security
 - d. Enterprise Security consolidates feedback and updates document
4. CIO Advisory Council review and approval:
 - a. Enterprise Security presents consolidated feedback and updated document to CIO Advisory Council
 - b. CIO Advisory Council approval to move on to the CTAB phase
5. Commissioners Technology Advisory Board (CTAB) review and recommendation:
 - a. Enterprise Security presents policy to CTAB
 - b. CTAB recommends approval of policy
6. State CIO Approval:
 - a. Enterprise Security presents final draft to State CIO
 - b. State CIO Signs final policy
 - c. Enterprise Security files signed copy, announces approval, and posts approval policy

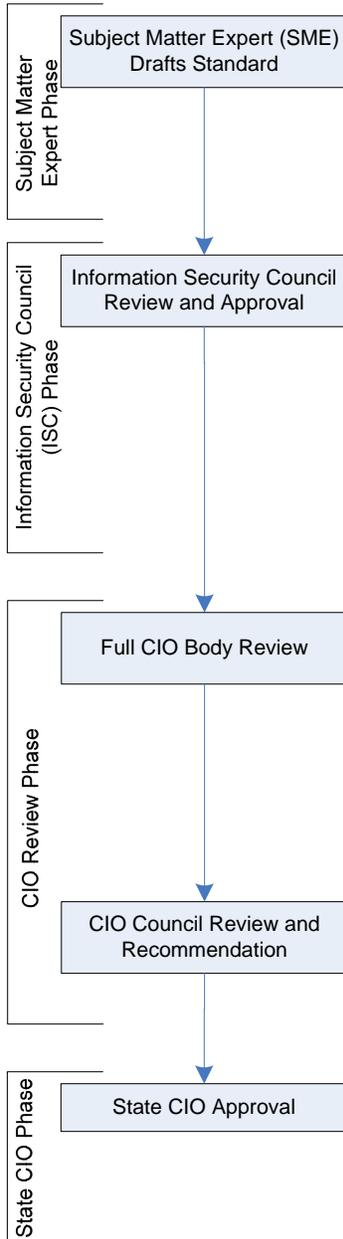


Enterprise Security Office Policy

Standards Approval Process

To add an enterprise security standard to the program or revise an existing standard, the following process must be used to draft/revise, review, and approve the standard.

Process Flow:



Process Steps:

1. Initial draft and vetting of standard by Subject Matter Expert (SME):
 - a. Standard owner and SME working group draft the standard
 - b. Owner presents initial draft to program management team and gathers feedback
 - c. State CISO approves standard to move onto the ISC review phase
2. Vetting of standard by the Information Security Council (ISC):
 - a. Draft standard is presented to the ISC at next scheduled meeting
 - b. ISC members have at least 30 days to review standard with their respective government entity and provide documented feedback to Enterprise Security
 - c. Enterprise Security consolidates feedback and updates draft
 - d. Present updated draft to ISC for approval to move on to the CIO review phase
3. Full CIO body review and feedback:
 - a. Enterprise Security presents draft to the full CIO body
 - b. Full CIO body members have at least three (3) weeks to review
 - c. CIO body members provide documented feedback to Enterprise Security
 - d. Enterprise Security consolidates feedback and updates standard
4. CIO Advisory Council review and approval:
 - a. Enterprise Security presents consolidated feedback and updated standard to CIO Advisory Council
 - b. CIO Advisory Council recommends approval of standard
5. State CIO approval:
 - a. Enterprise Security presents final draft to State CIO for signature
 - b. Enterprise Security files signed copy, announces approval of standard, communicates compliance date, and posts approval policy

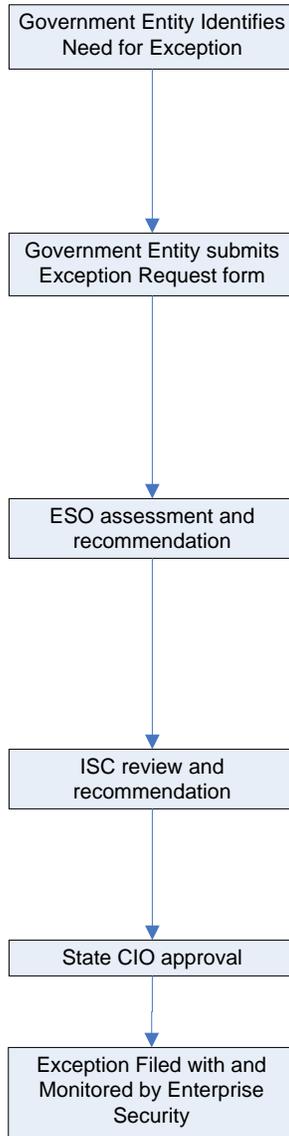


Enterprise Security Office Policy

Policy and Standards Exception Process

If a government entity can not comply with any part of the Enterprise Security Program (policy or standard) they must submit a request for an exception that includes a plan for becoming compliant. The following process is used to submit, review, approve, and track exceptions to the program.

Process Flow:



Process Steps:

1. Government entity requires a policy or standard exception due to compliance gap identified by:
 - a. Internal or external audit
 - b. Resource constraints
 - c. Other mechanism (e.g., exception renewal)
2. Government entity submits an Enterprise Policy/Standard Exception Request form
 - a. Specific Policy and/or Standard requirement
 - b. Business and risk justification
 - c. Proposed mitigation plan
 - d. Signed by the head of the government entity
3. Enterprise Security conducts an assessment of the risk, its potential impact, and makes a recommendation to:
 - a. Approve request as is
 - b. Approve request with additional mitigating controls
 - c. Deny request until acceptable mitigation plan can be developed
4. Information Security Council (ISC) reviews request to:
 - a. Assess impact on individual agency
 - b. Validate Enterprise Security findings
 - c. Approve recommendation
5. State CIO reviews and approves exception for a maximum time period of two years.
6. Exception filing and mitigation monitoring by Enterprise Security:
 - a. Approved exception are filed with Enterprise Security
 - b. Enterprise Security periodically audits progress of mitigation plan and reports status to State CIO
 - c. Enterprise Security notifies State CIO and government entity's head of expiring exceptions



Enterprise Security Office Policy

History & Ownership

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

Date	Author	Description	Major #	Minor #
<TBD>	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	Eric Breece, Rick Ensenbach, Mark Mathison, Clif Meier, ESO Management Team, Chris Buse	09/09/2008
ISC	Information Security Council Approval	11/05/2008
CIOC	CIO Council Approval	05/21/2009
CTAB	Commissioners' Technology Advisory Board Approval	06/11/2009
State CIO	Signing by the State CIO	06/22/2009

Ownership – current owners of the document

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