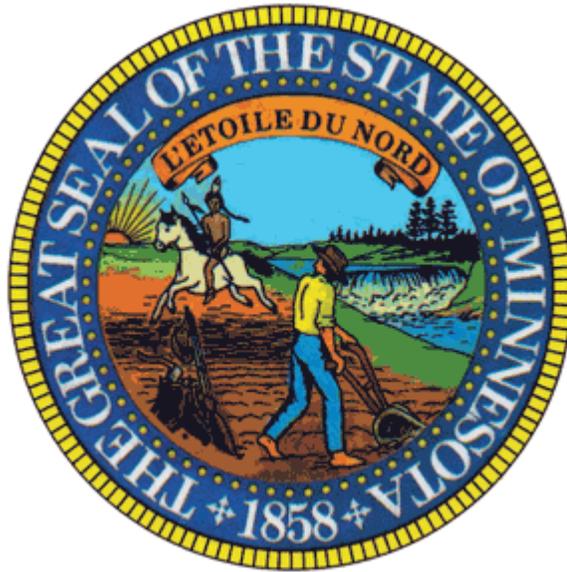


State of Minnesota



Office of Enterprise Technology

Enterprise Security Technical Control Policies

Enterprise Security Office Policy

Version 1.00

Approval:

Gopal Khanna	<Signature on File with ESO>	12/23/2009
State Chief Information Officer	Signature	Approval Date



Enterprise Security Technical Control Policies

Table of Contents

1.0 TECHNICAL CONTROLS.....	3
TC01 – VULNERABILITY AND THREAT MANAGEMENT POLICY.....	3
TC02 – AUTHENTICATION AND ACCESS CONTROL POLICY.....	3
TC03 – AUDIT TRAIL AND EVENT LOGGING POLICY.....	3
TC04 – CRYPTOGRAPHY AND COMMUNICATION PROTECTION POLICY.....	3
2.0 ROLES & RESPONSIBILITIES.....	3
2.1 OFFICE OF ENTERPRISE TECHNOLOGY (OET).....	3
2.3 GOVERNMENT ENTITY.....	3
3.0 RELATED INFORMATION.....	3
3.1 REASON FOR POLICIES.....	3
3.2 APPLICABILITY AND EXCLUSIONS.....	4
3.3 REFERENCES.....	4
3.4 FORMS AND INSTRUCTIONS.....	4
3.5 COMPLIANCE.....	4
5.0 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 Technical Control Policies

1.0 Technical Controls

The Technical Control policies identify a class of security controls executed or used by systems. They can be automated controls that facilitate the detection or prevention of security violations, or technologies used by systems to support operational security requirements

TC01 – Vulnerability and Threat Management Policy

Government entities must manage their exposure to security vulnerabilities to the State's information assets.

TC02 – Authentication and Access Control Policy

Government entities must use authentication and access controls to ensure users, systems, applications, and networks have appropriate access to only the resources necessary to perform their function.

TC03 – Audit Trail and Event Logging Policy

Government entities must log system events of critical information assets for the purposes of security monitoring, investigation, and compliance activities.

TC04 – Cryptography and Communication Protection Policy

Government entities must use appropriate cryptographic controls to ensure the protection of data and communications.

2.0 Roles & Responsibilities

2.1 Office of Enterprise Technology (OET)

1. Maintain this document and related standards, guidelines, and processes
2. Maintain enterprise tools and solutions to support these policies
3. Monitor and report on enterprise compliance to these policies
4. Fulfill the Government Entity role and responsibilities for OET

2.3 Government Entity

1. Implement and manage entity specific tools and solutions to comply with these policies
2. Report on compliance to these policies to OET
3. Document processes that support technical security controls

3.0 Related Information

3.1 Reason for Policies

As the State becomes more and more dependent on technology to effectively deliver services, these technologies become more complex and larger targets for malicious individuals. The increased complexity and ever expanding exposure to vulnerabilities increases the risk that something will go wrong and result in the compromise of a State system. A compromise could be something simple with limited ramifications to something more catastrophic. The range could be from something limited (as a person not having access to the information needed to perform their job) to legal ramifications (as a violation of basic regulatory requirements) to the more catastrophic with an impact on the health and safety of the public.



Enterprise Security Technical Control Policies

In order to help protect the State's systems, additional technologies are used to protect these information assets. They are designed to prevent a breach in security and provide with a number of benefits:

- Better situational awareness of events affecting the State's systems
- Controlling who or what has access to sensitive information
- Limiting what someone can do with the data they have access to
- Ensuring the integrity of State data
- Provide the capability to proactively respond to emerging threats
- Traceability to help determine what caused a security incident to occur

The implementation of any security technology requires significant consideration for the operational implications and must align with the overall management of security within the Executive branch. Therefore these policies are necessary to identify the appropriate usage of these security technologies and support the objectives of the Operational Control Policies. They are also key to understanding and monitoring the protection of the State's the information assets.

3.2 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.

3.3 References

[Minnesota Statutes 16E](#) Office of Enterprise Technology
[Minnesota Statute 13](#) Data Practices
Enterprise Security Program Policy
Enterprise Security Applicability Standard
Enterprise Security Management Control Policies (draft)
Enterprise Security Operational Control Policies
Enterprise Security Glossary of Terms

3.4 Forms and Instructions

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

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

3.5 Compliance

Compliance to these policies is required within 24 months from approval date of the supporting standards.



Enterprise Security Technical Control Policies

5.0 History & Ownership

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

Date	Author	Description	Major #	Minor #
12/23/2009	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	07/08/2009
ISC	Information Security Council Approval	09/02/2009
CIO	All CIO Team Approval	12/17/2009
CTAB	Commissioners' Technology Advisory Board Approval	N/A

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