

State of Minnesota



Office of Enterprise Technology

Enterprise Security Operational Control Policies

Enterprise Security Office Policy

Version 1.00

Approval:

Gopal Khanna

State Chief Information Officer

Signature

Approval Date



Table of Contents

1.0 OPERATIONAL CONTROLS	3
OP01 – PERSONNEL SECURITY POLICY	3
OP02 – SYSTEM SUPPORT POLICY	3
OP03 – PHYSICAL & ENVIRONMENTAL PROTECTION POLICY	3
OP04 – SECURITY INCIDENT MANAGEMENT POLICY	3
OP05 – AWARENESS & TRAINING POLICY	3
OP06 – CONFIGURATION MANAGEMENT POLICY	3
OP07 – CONTINUATION OF OPERATIONS PLANNING POLICY	3
OP08 – INFORMATION HANDLING POLICY	3
2.0 ROLES & RESPONSIBILITIES	4
2.1 OFFICE OF ENTERPRISE TECHNOLOGY (OET)	4
2.2 GOVERNMENT ENTITY	4
3.0 RELATED INFORMATION	4
3.1 REASON FOR POLICIES	4
3.2 APPLICABILITY AND EXCLUSIONS	4
3.3 REFERENCES	4
3.4 FORMS AND INSTRUCTIONS	5
3.5 COMPLIANCE	5
5.0 HISTORY & OWNERSHIP	6
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



1.0 Operational Controls

Operational Control policies address process based security controls implemented and executed by people. These controls rely on management controls to identify the appropriate processes or actions, and often rely on the technical controls for enforcement.

OP01 – Personnel Security Policy

Government entities must integrate security roles and responsibilities into position descriptions. Job responsibilities and duties must be the basis for determining the necessary level of vetting for the position and the authorization of access to both physical and logical resources. Access authorization must be managed by defined processes.

OP02 – System Support Policy

Government entities must integrate security requirements into processes that address user and system support, information backup, storage media control, system documentation, and change control.

OP03 – Physical & Environmental Protection Policy

Government entities must define the physical and environmental controls to protect the organization's information assets.

OP04 – Security Incident Management Policy

Government entities 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

OP05 – Awareness & Training Policy

Government entities must have an ongoing security awareness and education program, designed to educate users on how to address threats to government operations and data.

OP06 – Configuration Management Policy

Government entities must maintain a set of security configuration standards for all supported platforms and services.

OP07 – Continuation of Operations Planning Policy

Government entities must have a Continuity of Operations Plan (COOP) that is tested and maintained.

OP08 – Information Handling Policy

Government entities must maintain information handling practices that integrate defined security controls for each stage of the information's lifecycle.



Enterprise Security Office Policy

2.0 Roles & Responsibilities

2.1 Office of Enterprise Technology (OET)

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

2.2 Government Entity

1. Integrate operational security requirements into established business processes
2. Maintain and document the necessary processes to address the security requirements of these policies
3. Report on operational security risks as necessary

3.0 Related Information

3.1 Reason for Policies

These policies are necessary to support the management of information risks in daily operations. They help people within the organization understand their day to day security responsibilities and the threats that could impact the State's services, public health and safety, regulatory requirements, and government data.

These policies have an inherent reporting requirement that is necessary to support a consolidated enterprise risk profile of the Executive Branch. The analysis of operational controls can be used to identify operational risks, trends, areas of improvement, and changes. This will help identify emerging and recurring risks, and ways to mitigate new risks that ensure information assets are protected in a manner that is cost-effective and reduces the risk of unauthorized information disclosure, modification, or destruction, whether accidental or intentional.

Implementing consistent operational controls across the Executive branch will help the State comply with current and future legislation to ensure long term diligence in protecting the confidentiality, integrity and availability of State data.

3.2 Applicability and Exclusions

This policy is applicable to all government entities identified within 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.

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 Office Policy

Enterprise Security Management Control Policies (draft)
Enterprise Security Operational Control Policies
Enterprise Security Glossary of Terms
[Enterprise Security Operational Control Standards \(under development\)](#)

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 Office Policy

5.0 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	Enterprise Security Office Approval	07/08/2009
ISC	Information Security Council Approval	09/02/2009
CIO	All CIO Team Approval	
CTAB	Commissioners' Technology Advisory Board Approval	

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