

Procedure 1410.23  
Issued: March 12, 2001  
Effective Date: March 15, 2001

**SUBJECT:** State of Michigan Security Matrix

**APPLICATION:** All Executive agencies and other non-executive-branch entities using the Lansing-Metropolitan-Area-Network (LMAN) or the State of Michigan - Wide Area Network (SOM-WAN).

**PURPOSE:** To standardize a frame of reference and a means for presentation and representation of the security risks and mitigating technologies associated with each type of connection to the State of Michigan's data networks. This framework provides an informational reference point for security policies and standards to internal security decision-makers and application developers. The matrix provides a correlation from security risk checklists to related technologies for mitigating agency and enterprise security risks in an overall hierarchical and correlated security context for SOM information systems. It also provides a context for relating the relevance and value of new security technologies

**CONTACT AGENCY:** Department of Information Technology (DIT)  
Office of Strategic Policy

**TELEPHONE:** 517/373-7326

**FAX:** 517/335-2355

**SUMMARY:** This procedure establishes a connection type and technology matrix categorized and labeled as a consistent model for communicating the enterprise and agency security framework. The matrix is intended as a guideline to facilitate the recognition of security risks and in the planning, managing, mitigating, and implementation effort of applying information technology security counter-measures and initiatives at the agency and enterprise level to reduce risks to tolerable levels.

**APPLICABLE FORMS:** None.

**PROCEDURE:**

**General Information:**

The objectives of this standard are to:

Standardize a framework for mitigation of agency and enterprise security risk;

Establish a reference profile for related security policies and standards; and

Provide a method to examine the relevance of new security technologies in a standard context.

Benefits expected:

Facilitate consistent communication of access security technology and associated risk.

Provide a common method for describing and connecting interrelated security technologies.

Describe security solution interactions and dependencies in a consistent manner.

Assist in associating connection types with available technologies and State of Michigan standards, policies, and procedures.

Provide the ability to view and analyze data across multiple dimensions of the security technologies while maintaining an appropriate contextual setting.

Provide a mechanism for improved collaboration of security risks and a baseline for risk analysis or security risk analysis checklists.

Improved communication within the State of Michigan information technology community.

Ability to rapidly assess the impact of recommended or required changes to security processes, procedures, policy, designs, or implementations.

Increase the visibility and clarity of standards and procedures related to system security.

Facilitate substantive documentation of the security framework in a repeatable way.

Provide the ability for a large audience to understand the issues through consistent illustrative presentation.

Applicability:

Conditions of Application:

This information standard is applicable to any host, client, or server connections or nodes provided access on any of the State of Michigan's data networks including LMAN and SOM-WAN. The standard applies to internal networks or Intranets used solely for inter or intra-agency connectivity and Internet and extra-net connections.

Implementation considerations: Vendors selected to provide access security technology goods and services to agencies or the enterprise should become familiar with this matrix and use its features in the documentation and/or communication of proposed changes or improvements to information security.

Procedures:

The security matrix is available upon request.

Procedure 1410.23

Procedure Update: 06-16-02

Its labeled tabs include the following six identified high-level security categories:

- A. Identification - confidence of who is connecting;
- B. Authentication - confident of source device;
- C. Authorization - granting of access rights;
- D. Access Control - user, device, or protocol profile and allowed connections and routes;
- E. Administration - security management procedures; and
- F. Auditing - intrusion detection, monitoring, and reporting.

1. Each security category is further divided into technology modules, and subsequently by technology element where appropriate. Each row grouping and cell is labeled and numbered to provide a way to reference appropriate related technologies.
2. The numbered connection types are listed on the top horizontal axis to form columns, and are numbered 1 to 58 for reference. The information as shown at each intersecting cell in the matrix reveals part of the State of Michigan's defensive strategy and is to be considered and treated as confidential protected information.
3. The security matrix document is to be considered a constant work in progress. The current version should be requested when making security decisions for internal or externally available connections.
4. A note on how to use the matrix. Enter the matrix from the horizontal column headings based on the type of connection you are evaluating. Proceeding down in the column selected will provide guidance on security considerations. Moving from an intersecting cell to the left on each tab will provide information on what technologies are potentially involved. Information at the intersection of the column and row provides the number of relevant security standard(s) or procedure(s) that have germane applicability to that connection type. If an intersection is blank, follow the row to the column labeled Policy/Standard highlighted in red, right next to the Detailed Technical Element Column to determine if a security policy or standard is listed as associated.

Maintenance:

DMB: Acquisition Services shall not approve any acquisition or purchase request without confirmation from the Department of Information Technology, Office of Strategic Policy that such request is in compliance with the standard.

Operational  
Units (OU):

All new or existing network connections within State agencies must use this informational standard when concerned with determining security needs. Agencies should review the security risks for new or existing connections across the data networks by using this standard as a checking point or framework. Determining how much security is enough and then implementing appropriate steps to reduce risk to acceptable levels mitigates security risk. As each application and connection is considered this matrix provides an overall context and often a specific recommendations by way of the numbered standards included. It is the agencies' security administrators and developers responsibility to be familiar with the standards and technologies available for reduction of security risks.

Any and all projects, consulting requests, equipment and software acquisition requests, or ITB's relating to security matrix components will be subject to review for compliance with this standard.

DIT: The Office of Strategic Policy will review this standard on a continuing basis and make recommendations for changes. An appropriate group of staff, representing a wide-range of state operational units, will review and possibly revise these standards and guidelines as often as needed.

Exceptions from this standard for reasons other than those outlined above will be made through the exception handling process described in the Exception Process Template.

\*\*\*