Minnesota State Colleges & Universities (Minnesota State)

Enterprise Systems Control Assessment

of Top 5 Security Domains

Prepared for the Board of Trustees

October 31, 2022

Table of Contents

Introduction

Minnesota State Colleges and Universities (Minnesota State) has developed a control framework that is unique to Minnesota State and references elements of internationally recognized frameworks including: New Zealand Information Security framework, Center for Internet Security (CIS) Critical Security Controls and the NIST Cybersecurity framework. This control framework was adopted as a methodology to assist with the assessment of information security risk within the System Office and the 37 colleges and universities. The framework allows Minnesota State to measure key components of the organization's security posture.

Using this framework the Minnesota State System Office Security Team had previously conducted self-assessments to determine compliance with the framework. Last year, the Board requested that an independent 3rd party perform an audit on how closely the system office complies with the Top 5 Security Framework.

Five security domains have been identified as being critical for reducing IT operational risk within the system office and the colleges and universities that make up the Minnesota State system. Each domain has a range of activities that range from minimal effort being made in the area, to high effort expended on activities in the domain.

The goal of this security plan is to define a baseline for each domain and the measurable activities that can be performed during the next fiscal year to show progress in each area. It is critical to understand that the activities in each domain are additive and continuous. Movement along the scale by definition means additional and continuous workload in order to remain vigilant in reducing risk. The ultimate goal is to take each activity and make it part of basic operations.

Control Maturity (Measurement)

Within each of the Top 5 Security Domains, criteria was established by Minnesota State to measure the maturity of controls against the framework including level of effort as described below.

Effort	Description
Minimal (Starting)	Describes the minimal controls that must be implemented to demonstrate commitment by management
Moderate (Improving)	Describes additional controls that must be implemented to illustrate improvement from the baseline controls required under the Minimal Effort category
High (Advancing)	Describes controls that are in addition to those under the Minimal and Moderate Effort categories

Scope

In response to that request, CliftonLarsonAllen LLP (CLA) was engaged to assess controls in meeting the key components of the framework including the following:

- Data Classification and Inventory
- Vulnerability Management
- Controlled Use of Administrative Privileges
- Application Security
- Secure Network Engineering

Approach

In conducting each assessment, CLA used the following approach to reach a conclusion:

1. Reviewed existing policy statements and procedures applicable to the assessment.
2. Met with appropriate Minnesota State personnel applicable to the assessment to obtain a baseline understanding of the controls implemented.
3. Requested documentation as evidence of control(s) being implemented as applicable to the assessment.
4. Reviewed the documentation provided to determine if the evidence illustrated compliance with the key components of the Top 5 Security Domains.
5. Prepared a report summarizing CLA conclusions in preparation for presentation to the Board of Trustees.

Conclusion

CLA concluded that the control framework adopted by Minnesota State mirrors several internationally recognized frameworks and is appropriate for higher education to identify and reduce risk. In addition, the framework supports policy statements approved by the Board of Trustees.

The summary results of each of the Top 5 assessments are identified as follows:

Minimal Effort (Starting)	Moderate Effort (Improving)	High Effort (Advancing)
Data Classification and Inventory		
Identify/assign "Data Owners" – Note: The data owner typically is not the IT department Create an inventory of systems under IT's control or management (Note: ISRS is part of the system office's inventory)	Identify systems and applications where 'Highly Restricted' data resides	Identify systems and applications where 'Restricted' and 'Low' data resides
Conclusion		
Meets Criteria	**Meets Criteria**	**Meets Criteria**

Minimal Effort (Starting)	Moderate Effort (Improving)	High Effort (Advancing)
Vulnerability Management		
Assign devices to appropriate device scanning groups based on the asset's value. Value is determined by the confidentiality and integrity requirements of the data stored, processed or transferred by the device	Implement credentialed scanning on all managed devices	Develop patching and remediation plan and process using a risk-based approach. Plan includes a prioritized top-down patching approach that addresses higher risk resources first (e.g. Internet facing systems, CAP server and PCI networks) and critical patches (e.g. zero-day exploits) as highest priority Monitor progress using reports and metrics
Conclusion		
Meets Criteria for Data Center	**Meets Criteria for Data Center**	**Meets Criteria for Data Center**
Meets Criteria for Workstations	**Partially Meets Criteria for Workstations**	**Partially Meets Criteria for Workstations**

Minimal Effort (Starting)	Moderate Effort (Improving)	High Effort (Advancing)
Controlled Use of Administrative Privileges		
Identify job responsibilities that require administrative access to specific systems (including desktop/laptop PCs) Assign access as appropriate	Conduct periodic review of access using established review schedule	Administrative access is granted based on Minnesota State methods that align with "industry accepted practices"
Conclusion		
Meets Criteria	**Meets Criteria**	**Meets Criteria**

Minimal Effort (Starting)	Moderate Effort (Improving)	High Effort (Advancing)
Application Security		
Application security training for internal development staff Create comprehensive inventory of applications with appropriate data classification assigned	Establish software development life-cycle that includes security touch-points for internally developed applications Establish process to assess 3rd party applications for appropriate security controls and practices	Implement scanning and/or peer review of code for internally developed applications, identifying and remediating vulnerabilities Implement process to assess 3rdparty applications for appropriate security controls and practices Plan for and retire applications that are no longer supportable
Conclusion		
Partially Meets Criteria	**Meets Criteria**	**Meets Criteria**

Minimal Effort (Starting)	Moderate Effort (Improving)	High Effort (Advancing)
Secure Network Engineering		
Develop a comprehensive network diagram for all campus network, server and end-point infrastructure	After classifying data as Highly Restricted, Restricted or Low, and the criticality of the data to the business or academic functions, identify where the data is stored and/or transmitted Identify the perimeters between the various network segments based on data classification level and business/academic functional needs	Implement network security access controls/policies between different data classification levels commensurate with the data's classification and the business or academic needs Validate controls/policies exist between segments of different trust levels Implement appropriate secure remote access methods (e.g. multi-factor, VPN, etc.) to data based on data classification level and criticality to business or academic needs
Conclusion		
Meets Criteria	**Partially Meets Criteria**	**Meets Criteria**

Detailed Results

Data Classification and Inventory

Description and Purpose

The classification of data is one of the first fundamental steps for the protection of confidential data and leads to an appropriate and consistent set of security controls for each data source - not too many controls, not too few. Logically, to classify data, the organization must first have a comprehensive inventory of their applications and data sets.

Data classification also requires the prerequisite step of developing an inventory that includes: the systems and data sources that are managed by IT, the classification of the data on those systems, and the data owner.

Once data has been classified, the system on which it is transferred or resides is known, and the owner identified, appropriate security controls and practices can be implemented to protect the data commensurate with its level of classification.

Objectives

- Identification/assignment of data owners – i.e. the individual or department with ultimate authority and accountability for the data
- Inventory and identification of the systems and data sources under IT's control or management
- Classification of data - e.g. 'Highly Restricted', 'Restricted' or 'Low.'

Data Classification and Inventory Plan Activities

(Conducting activities and implementing controls identified in this plan should be addressed from Minimal to High

DATA CLASSIFICATION AND INVENTORY		
Minimal Effort (Starting)	**Moderate Effort (Improving)**	**High Effort (Advancing)**
Identify/assign "Data Owners" – Note: The data owner typically is not the IT department Create an inventory of systems under IT's control or management (Note: ISRS is part of the system office's inventory)	Identify systems and applications where 'Highly Restricted' data resides	Identify systems and applications where 'Restricted' and 'Low' data resides
Supporting Documentation		
List of system office data owners – title, name and the data for which he or she is the owner Documented inventory of the college or university's systems, applications or data repositories	Documented list of Highly Restricted data and where that data resides	Documented list of Restricted and Low data and where that data resides
Thresholds to meet Requirements		
List of owners includes "C" level and appropriate managers in all functional areas on campus including owners for student data, advancement (e.g. Foundation, booster clubs, etc.) employee data, finance, IT and institution program data (e.g. IR and institution owned intellectual property)	90% or greater of all systems/applications containing Highly Restricted data are listed on the inventory	90% or greater of all systems/applications containing Restricted or Low data listed on the inventory
Observations		
Minnesota State generated a Data Classification Document, illustrating the classification (Highly Restricted, Restricted and Low) for Non-ISRS Systems, ISRS Systems, and ISRS Data Objects. The document includes data owners	Minnesota State generated a Data Classification Document, illustrating the classification (Highly Restricted, Restricted and Low) for Non-ISRS Systems, ISRS Systems, and ISRS Data Objects. The document includes data owners	Minnesota State generated a Data Classification Document, illustrating the classification (Highly Restricted, Restricted and Low) for Non-ISRS Systems, ISRS Systems, and ISRS Data Objects. The document includes data owners
Recommendations		
Data Classification document is complete – no recommendations	Data Classification document is complete – no recommendations	Create change control process for data inventory/classification
Conclusions		
Meets Criteria	**Meets Criteria**	**Meets Criteria**
Management Response		
Not Required	Not Required	Not Required

Vulnerability Management

Description and Purpose

Vulnerability Management is a cyclical practice of identifying, classifying, remediating and mitigating vulnerabilities in software, especially in operating systems. Minnesota State has made a significant investment in a vulnerability management system that can be utilized to reduce risk to each institution.

Effective vulnerability management has been a proven practice and a key component in securing information assets. Scanning provides a report of system vulnerabilities that can be addressed to remediate risk in operating systems and software. Patching and/or upgrades remediates those vulnerabilities. Vulnerability Management is supported through Board Policy 5.23, Security and Privacy of Information Resources, and Operating Instruction 5.23.1.6, Vulnerability Scanning and 5.23.1.5, Security Patch Management.

Objectives

- Identification of all vulnerabilities through credentialed scanning
- Scanning of all appropriate/managed devices
- Timely, efficient remediation process in place – i.e. patching & updates
- Reporting and metrics tracking effectiveness of above objectives

Vulnerability Management Plan Activities

(Conducting activities and implementing controls identified in this plan should be addressed from Minimal to High)

VULNERABILITY MANAGEMENT		
Minimal Effort (Starting)	**Moderate Effort (Improving)**	**High Effort (Advancing)**
Assign devices to appropriate device scanning groups based on the asset's value. Value is determined by the confidentiality and integrity requirements of the data stored, processed or transferred by the device	Implement credentialed scanning on all managed devices	Develop patching and remediation plan and process using a risk-based approach. Plan includes a prioritized top-down patching approach that addresses higher risk resources first (e.g. Internet facing systems, CAP server and PCI networks) and critical patches (e.g. zero-day exploits) as highest priority Monitor progress using reports and metrics
Supporting Documentation		
Document inventory of devices and endpoints subject to scanning. Assign to appropriate scanning groups based on asset value	Document evidence of credential scans – e.g. reports from system office	Report results of vulnerability scanning activities, including identified vulnerabilities Document patch management plan and/or schedule summarizing the systems and applications subject to patching or updates, including frequency of patching

VULNERABILITY MANAGEMENT		
Thresholds to meet Requirements		
Devices are contained in the appropriate asset group Campus provides attestation that the list of devices is accurate and complete	90% of all managed devices are scanned using credentials However, Minnesota State has determined that a 5% variance is acceptable due to the timing of the scans and limitation(s) of the tool	95% of hosts have a host risk value less than 1000 However, Minnesota State has determined that a 5% variance is acceptable due to the timing of the scans and limitation(s) of the tool
Observations		
Minnesota State Colleges and Universities (Minnesota State) demonstrated that devices are assigned to groups based on the asset value which takes into account classification of data stored or processed by the device and the exposure of that device to public networks	Minnesota State demonstrated that in-scope devices were scanned using both credentialed and non-credentialed methods to ensure vulnerabilities were identified and communicated to the system managers for remediation in a timely manner In the sample provided, Minnesota State was able to demonstrate a success rate for scanning systems that was within the 5% tolerance	Minnesota State demonstrated that a patching and remediation plan was developed that uses a risk-based approach. Risk scores for each detected vulnerability were calculated using a formula that takes into consideration the value of the asset, the length of time the vulnerability has been unpatched since detection, and common vulnerability scoring criteria System managers are responsible to apply patches during the first available maintenance window after the patches have been tested In the sample provided, Minnesota State was able to demonstrate a success rate (a score of 1000 or less) for Infrastructure that was within the 5% tolerance However, only 67% of workstations scanned had a score of 1000 or less which was not within the 5% tolerance
Recommendations		
No significant recommendations	Minnesota State should continue to refine processes to ensure that more than 90% of all managed devices are scanned using credentials	Minnesota state should continue to improve its capabilities to identify the locations of Highly Restricted and Restricted data sets, use consistent identifiers for information assets in the various systems used to monitor and track the inventory to ensure the results are accurate, reportable, and auditable, reconciling to a single master record

VULNERABILITY MANAGEMENT		
Conclusions		
Meets Criteria for Data Center	**Meets Criteria for Data Center**	**Meets Criteria for Data Center** 100% of the hosts scanned scored less than 1000
Meets Criteria for Workstations	**Partially Meets Criteria for Workstations** 80% of workstations were scanned which is not within the 5% tolerance.	**Partially Meets Criteria for Workstations** 67% of the workstations scanned scored less than 1000
Management Response		
Not Required	Management agrees with the finding. Due to the increase in teleworking remotely, scanning a device has required the remote user to manually initiate a connection to Minnesota State's network. Two (2) projects are currently in progress to alleviate the manual process, ensuring devices are automatically attached and scanned.	Management agrees with the finding. Due to the increase in teleworking remotely, scanning a device has required the remote user to manually initiate a connection to Minnesota State's network. Two (2) projects are currently in progress to alleviate the manual process, ensuring devices are automatically attached, scanned and patched.

Controlled Use of Administrative Privileges

Description

System administration access and privileges must be controlled in a manner that only allows the administrator to conduct the activities needed to complete assigned tasks. Controlling access requires a formal process that includes the granting of access rights, or revoking access when no longer needed. Administrators' access and privileges need to be reviewed by management on a scheduled, recurring basis. Authentication strength requirements (i.e. password, multi-factor, etc.) should be commensurate with the level of data and/or system configuration protection requirements. Administrator's activities should be monitored and logged.

Limiting administrative access and privileges based on only the requirements needed to conduct assigned activities mitigates the risk of unauthorized individuals accessing Highly Restricted or Restricted data, or the ability to conduct tasks for which they are not authorized. Limiting access and privileges also reduces the risk of corrupting data or system configurations through malicious intent or by accident. Applying appropriate authentication strength, recurring reviews of account access privileges and changing passwords on a recurring basis, reduces the possibility of a compromise of the administrator's credentials. Logging administrative transactions and activities produces an audit trail that can be utilized for troubleshooting issues or to identify unauthorized or malicious actions.

Objectives

- Administrative access and privileges are limited to only those required for job responsibilities or to complete a task
- Access and privileges are reviewed on a recurring basis to identify any excess access or privileges and/or to remove access if it is no longer required
- The strength or method of authentication is appropriate for the administrative task or activity
- Audit trails are created through logging to assist in trouble-shooting problems or issues, or to identify unauthorized or inappropriate actions

Controlled Use of Administrative Privileges Plan Activities

(Conducting activities and implementing controls identified in this plan should be addressed from Minimal to High)

CONTROLLED USE OF ADMINISTRATIVE PRIVILEGES		
Minimal Effort (Starting)	**Moderate Effort (Improving)**	**High Effort (Advancing)**
Identify job responsibilities that require administrative access to specific systems (including desktop/laptop PCs) Assign access as appropriate	Conduct periodic review of access using established review schedule	Administrative access is granted based on Minnesota State methods that align with "industry accepted practices"
Supporting Documentation		
List of all campus roles/positions that require admin privileges Document inventory of all active user accounts with administrator rights, including user account name and data accessed/rights	Document administrator accounts that have been removed for those individuals that do not require admin privileges, including last date of review	Document technologies/processes used to grant admin access
Thresholds to meet Requirements		
Identification and documentation of all roles/positions that require admin privileges	Documented review of admin accounts and access rights have been reviewed within the past 12 months, including admin accounts that have been removed	Validate that administrative access is granted based on Minnesota State methods that align with "industry accepted practices"
Observations		
Minnesota State defined administrative access roles for user workstations (local admin), desktop support, network admin, and cloud-based services For each of these roles, Minnesota State provided a list of users with administrative rights For Local Workstation Admin, Minnesota State a list of users who have been granted an exception for this access For Desktop Support, Network Admin and Cloud Admin, Minnesota State provided job descriptions illustrating the need for administrative access in order to perform the job responsibilities CLA reviewed roles and access rights, compared with job descriptions to validate that access was appropriate to the role	For workstations with Local Administrator privileges granted by exception, a review was performed annually, but not formally documented For Network/Cloud administrative privileges, review was performed periodically, but not formally documented	The Maximum Effort criteria and Threshold are only related to Local Admin access (exception process for workstation users). For this role, the process is well documented, evidence of the exception request and approval was found in tickets For System Admin roles (desktop support, network admin, cloud admin), the process is not documented, although Cherwell tickets were found to be used for onboarding/off boarding/ changes to administrative access

CONTROLLED USE OF ADMINISTRATIVE PRIVILEGES		
Recommendations		
Although job descriptions were provided for Desktop/Network/Cloud admin users, administrative roles were not specifically identified and had to be inferred from the narrative Recommend improving job descriptions to specifically note the access that is required for the role	Document annual review process of local admin exceptions, and document when the actual reviews occur, what actions (if any) were taken Document periodic review process for network and cloud administrative users, and formalize evidence of occurrence	Implementation of administrative privileges is performed using Cherwell tickets. The process for local admin exceptions is well documented, but Minnesota State should formally document the process for desktop support/network/cloud admin privileges requests
Conclusions		
Meets Criteria	**Meets Criteria**	**Meets Criteria**
Management Response		
Not Required	Not Required	Not Required

Application Security

Description

Application security is the implementation of proven processes and practices in software to secure confidential data from unauthorized access and modification. This includes measures taken through the application lifecycle to prevent gaps in the code itself or the underlying system through flaws in the design, development, deployment, upgrade or maintenance of the application.

An effective application security program that includes appropriate security practices result in code and applications that are resistant to malicious attacks throughout the lifecycle of the application.

Objectives

- Development skills that include secure coding practices
- Third-party vendors and applications have been evaluated for appropriate security controls and practices
- Validate that applications are secure and resistant to malicious attacks
- Code is appropriately managed and maintained throughout its life cycle
- Accurate inventory and data classification of internally developed and 3rd party applications

Application Security Plan Activities

(Conducting activities and implementing controls identified in this plan should be addressed from Minimal to High)

APPLICATION SECURITY		
Minimal Effort (Starting)	**Moderate Effort (Improving)**	**High Effort (Advancing)**
Application security training for internal development staff Create comprehensive inventory of applications with appropriate data classification assigned	Establish software development life-cycle that includes security touch-points for internally developed applications Establish process to assess 3rd party applications for appropriate security controls and practices	Implement scanning and/or peer review of code for internally developed applications, identifying and remediating vulnerabilities. Implement process to assess 3rd party applications for appropriate security controls and practices. Plan for, and retire applications that are no longer supportable
Supporting Documentation		
Document showing all application security training, including curriculum that has been provided to application developers and supporting development staff Document inventory of in-house and 3rd party developed applications that are implemented or utilized by the campus	Documented Software Development Life Cycle (SDLC) for internally developed applications, validating that security controls are implemented. Documented 3rd party application security assessment process.	Document in-house and 3rd party application developed code scanning results – include findings and remediation. List of retired applications.
Thresholds to meet Requirements		
At least 75% of internal application developers have had security training within the past 2 years Inventory of all applications with attestation that it is at least 90% complete	SDLC for internally developed applications includes code scanning and/or peer review Documented security assessment for 3rd party developed applications	Documented results of internal and 3rd party developed application assessments, including remediation or mitigation of critical security vulnerabilities List of retired applications and/or plan for retirement of all unsupportable applications
Observations		
Based on interviews and documentation provided, Minnesota State development team members do not formally attend security training, nor is security training currently incorporated into employees "Independent Development Plan (IDP)" Minnesota State provided an inventory of applications, which included scope (external, internal), business risk, and data classification. However, the list was manually generated and maintained	Minnesota State has created a "Secure Software Development Plan" document, which is an excellent step in moving toward secure coding. However, a formal SDLC document does not exist, so incorporating the security touchpoints into the SDLC is more ad hoc and not documented Minnesota State has created a vendor security assessment tool for 3rd party applications, which is used and documented	Minnesota State provided evidence of all external facing applications containing highly confidential data being scanned (scope of this assessment) Evidence or process to retire applications was not observed

APPLICATION SECURITY		
Recommendations		
Continue to maintain and build on the inventory of applications, and find tools to make the process more automated. Incorporate formal Security Code training into all developers training programs, include in budget, and perform annually. Consider adding an in-house resource with specific knowledge on secure coding practices and have the individual lead secure coding practice training and implementation.	Create a documented, overarching SDLC for all software development, which integrates with the "Secure Software Development Plan" touchpoints Formally incorporate and document the security touchpoints (secure code reviews, scanning) as part of the SDLC Automate the SDLC and secure coding process so that all changes to all applications include those security touchpoints	Scanning process could be more formalized to clearly show when scans happen, the results of the scans, remediation steps taken, rescans performed Develop and implement process to determine software life cycle and retire applications
Conclusion		
Partially Meets Criteria Minnesota State has not formalized a secure coding practices training program for developers.	**Meets Criteria**	**Meets Criteria**
Management Response		
Management agrees with the finding. Management has implemented formal processes that require scanning of all developed software, and vulnerabilities remediated to an acceptable risk level prior to implementing into production. Most developers have completed baseline training. Management will identify gaps in training and ensure training is completed.	Not Required	Not Required

Secure Network Engineering

Description

Secure network engineering involves applying perimeter network controls to segment data based on its classification and criticality to the business and/or academic functions. Based on the classification and criticality, data must be grouped with similar type data which results in 'segregation groups.' Appropriate security network controls must be applied at the perimeters of segregation groups. Secure network engineering also includes establishing secure access methods for both wired and wireless connections, and remote access for teleworkers.

Properly implemented network controls permit access to data and Information Technology Resources to only those individuals with a legitimate need-to-know. Limiting user access based on need-to-know basis through the implementation of network controls and secure access methods assists in the protection of data confidentiality, data integrity and system availability.

Objectives

- Network controls are implemented at perimeters between different classifications of data (i.e. Highly Restricted, Restricted, Low) that only allow access to data and services based on legitimate business needs
- Users, information systems, data and services are appropriately segregated
- Secure methods of access to data via wired, wireless or remote access connections

Secure Network Engineering Plan Activities

(Conducting activities and implementing controls identified in this plan should be addressed from Minimal to High)

SECURE NETWORK ENGINEERING ASSESSMENT		
Minimal Effort (Starting)	**Moderate Effort (Improving)**	**High Effort (Advancing)**
Develop a comprehensive network diagram for all campus network, server and end-point infrastructure	After classifying data as Highly Restricted, Restricted or Low, and the criticality of the data to the business or academic functions, identify where the data is stored and/or transmitted Identify the perimeters between the various network segments based on data classification level and business/academic functional needs	Implement network security access controls/policies between different data classification levels commensurate with the data's classification and the business or academic needs Validate controls/policies exist between segments of different trust levels Implement appropriate secure remote access methods (e.g. multi-factor, VPN, etc.) to data based on data classification level and criticality to business or academic needs
Supporting Documentation		
Comprehensive network diagram that includes points of remote access to data	Current network diagram identifying where Highly Restricted, Restricted and Low data is stored, processed or transmitted	Identify and document the network controls implemented between Highly Restricted, Restricted and Low data that prevent or limit unauthorized access – i.e. Access Control Lists (ACLs), firewall policies, Virtual Private Network (VPN), etc. Documented process for provisioning and de-provisioning remote access users. Remote access configuration documentation Current list of users and/or 3rd party vendors with remote access
Thresholds to meet Requirements		
Current network diagram exists	Current network diagram exists that identifies where all Highly Restricted, Restricted and Low data is stored, processed or transmitted	List of ACLs, firewall and VPN configurations, etc., that enforce access control Documentation exists for provisioning and de-provisioning remote access users Remote access configuration settings ensure that users are only allowed access to network resources that are required for their business or academic need Current list of users and/or 3rd party vendors with remote access is accurate and approved by appropriate parties

SECURE NETWORK ENGINEERING ASSESSMENT		
Observations		
Minnesota State has developed network diagrams and documentation that identify the perimeters between segregated groups	Minnesota State has developed documentation that details which network segments may contain different classifications of data However, the current network diagram does not specifically identify where all Highly Restricted, Restricted and Low data is stored, processed or transmitted	Minnesota State has developed processes to manage ACLs, firewall and VPN configurations that enforce access control However, the documentation of those ACLs and configurations is not readily accessible or in terms of the present configuration or a configuration baseline
Recommendations		
No significant recommendations for this area	Minnesota State should continue to improve network documentation to ensure the locations where Highly Restricted, Restricted and Low classified data is stored, processed or transmitted are clearly identified	Minnesota State should continue to improve network documentation to include documentation of current ACLs, the reason the ACL is needed, and the approval for the addition or change to the ACL Minnesota State should also work to improve the documentation of processes for adding remote access
Conclusion		
Meets Criteria	**Partially Meets Criteria** Minnesota State had not identified the physical locations where Highly Restricted, Restricted and Low classified data resides	**Meets Criteria**
Management Response		
Not Required	Management agrees with the finding and accepts the risk. Minnesota State has implemented strong controls that limit access to sensitive data based on 'need-to-know' and a person's job responsibilities. The controls mitigate unauthorized access and the need to physically identify where classified data resides.	Not Required