SYSTEMS SECURITY POLICY

Comentado [CR1]: @Mike Sparling another one needing your expertise and thumbs up.

PURPOSE

This document describes MHS security features that govern how users and processes communicate and interact with systems and resources. The objective of implementing access controls is to ensure that authorized users and processes can access information and resources, while unauthorized users and processes are prevented from access to the same. The purpose of this policy is to implement secure practices from initiation through destruction.

GOALS AND OBJECTIVES

- To require the identification of the person or system seeking access to secured information, information systems, or devices.
- To state the access control authorization principles of the organization.
- To ensure that access is granted only to authorized users and processes, and to provide users the minimum access required to perform a given role effectively.
- To logically group network assets, resources, and applications to apply security controls.
- To define the requirements for the secure design, configuration, management, administration, and oversight of border devices.
- To assign responsibility and set the requirements for remote access connections to the internal network.
- To assign responsibility and set the requirements for teleworking.
- To ensure that there is a means to prevent and/or detect attempts to gain access to information resources by unauthorized entities.
- To assign responsibility for key management and cryptographic standards.

SYSTEM SECURITY POLICY INDEX

1. Authentication Policy
2. Access Control Authorization
3. Network Segmentation
4. Border Device Security
5. Remote Access
6. Teleworking Policy
7. User Access Control and Authorization
8. Administrative and Privileged Accounts
9. Monitoring System Access and Use
10. Key Management

POLICY

1. Authentication Policy

1.1 Access to and use of information technology systems require an individual to uniquely identify and authenticate him/herself to the resource.

1.2 Multi-user or shared accounts are allowed only when there is a documented and justified reason that has been approved by the IT Operations Department.

1.3 The IT Operations Department is responsible for managing an annual user account audit of network accounts, local application accounts, and web application accounts.

1.4 Data classification, regulatory requirements, the impact of unauthorized access, and the likelihood of a threat being exercised must all be considered when deciding upon the level of authentication required. The IT Operations Department will make this determination in conjunction with the information system owner.

1.5 Operating systems and applications will at a minimum be configured to require single-factor complex password authentication.

1.5.1 Password complexity will be defined in the company password standard.

1.5.2 The password standard will be published, distributed, and included in the acceptable use agreement.

1.5.3 The inability to technically enforce this standard does not negate the requirement.

1.6 Web applications that transmit, store, or process “protected” or “confidential”, information must at a minimum be configured to require single-factor complex password authentication.

1.6.1 Passwords and PINs must be unique to the application.

1.6.2 Whenever feasible, multi-factor authentication must be implemented.

1.6.3 The inability to technically enforce this standard does not negate the requirement.

1.7 Exceptions to this policy must be approved by the IT Operations Department.

1.8 All passwords must be encrypted during transmission and storage. Applications that do not conform to this requirement may not be used.

1.9 Any mechanism used for storing passwords must be approved by the IT Operations department.

1.10 If any authentication mechanism has been compromised or is suspected of being compromised, users must immediately contact the IT Operations Department and follow the instructions given.

2. Access Control Authorization

2.1 Default access privileges will be set to “deny all.”

2.2 Access to information and information systems must be limited to personnel and processes with a need-to-know to effectively fulfill their duties.

2.3 Access permissions must be based on the minimum required to perform a job or program function.

2.4 Information and information system owners are responsible for determining access rights and permissions.

2.5 The IT Operations Department is responsible for enforcing an authorization process.

2.6 Permissions must not be granted until the authorization process is complete.

3. Network Segmentation

3.1 The network infrastructure shall be segregated into distinct segments according to security requirements and service functions.

3.2 The IT Operations Department is responsible for conducting annual Network Segment Risk Assessments. The results of the assessment will be provided to the CTO.

3.3 Complete documentation of the network topology and architecture will be maintained by the IT Operations Department including an up-to-date network diagram showing all internal (wired and wireless) connections, external connections, and endpoints, including the Internet.

4. Border Device Security

4.1 Border security access control devices shall be implemented and securely maintained to restrict access between networks that are trusted to varying degrees.

4.2 If any situation renders the Internet-facing border security devices inoperable, Internet service must be disabled.

4.3 The IT Operations Department is responsible for designing, maintaining, and managing border security access control devices.

4.3.1. At the discretion of the CTO, this function or part may be outsourced to a Managed Security Service Provider (MSSP).

4.3.2. Oversight of internal or MSSP border security device administrators is assigned to the IT Operations Department.

4.4 The IT Operations Department is responsible for approving border security access control architecture, configuration, and rule-sets.

4.5 The default policy for handling inbound and outbound traffic should be to deny all.

4.5.1 The types of network traffic that must always be denied without exception will be documented in the border device security standards.

4.5.2 Rule-sets must be as specific and simple as possible. Rule-set documentation will include the business justification for allowed traffic.

4.5.3 All configuration and rule-set changes are subject to the organizational change management process.

4.5.4 All rule-set modifications must be approved by the IT Operations Department.

4.6 All border security access control devices must be physically located in a controlled environment, with access limited to authorized personnel.

4.7 To support recovery after failure or natural disaster, the border security device configuration, policy, and rules must be backed up or replicated on a scheduled basis as well as before and after every configuration change.

4.8 Border devices must be configured to log successful and failed activity as well as configuration changes.

4.8.1 Border device logs must be reviewed and documented daily by the IT Operations Department.

4.9 Configuration and rule-set reviews must be conducted annually.

4.9.1 The review is to be conducted by an external independent entity.

4.9.2 The selection of the vendor is the responsibility of the Audit Committee.

4.9.3 Testing results are to be submitted to the CTO.

4.10 External penetration testing must at a minimum be performed semi-annually.

4.10.1 The testing is to be conducted by an external independent entity.

4.10.2 The selection of the vendor is the responsibility of the Audit Committee.

4.10.3 Testing results are to be submitted to the CTO.

5. Remote Access

5.1 The IT Operations Department is responsible for approving remote access connections and security controls.

5.2 The IT Operations department is responsible for managing and monitoring remote access connection.

5.3 Remote access connections must use 128-bit or greater encryption to protect data in transit (that is, VPN, SSL, SSH).

5.4 Multifactor authentication must be used for remote access.

5.4.1 Whenever technically feasible, one factor shall be “out-of-band.”

5.5 Remote equipment must be company-owned and configured the following company workstation security standards.

5.6 Business partners and vendors wishing to obtain approval for remote access to computing resources must have access approved by the CTO. Their company sponsor is required to provide a valid business reason for the remote access to be authorized.

5.7 Employees, business partners, and vendors approved for remote access must be presented with and sign a Remote Access Agreement that acknowledges their responsibilities before being granted access.

5.8 Remote access devices must be configured to log successful and failed activity as well as configuration changes.

5.8.1 Remote access logs must be reviewed and documented by the IT Operations Department.

5.9 Remote access user lists must be reviewed quarterly by Human Resources.

5.9.1 The result of the review must be reported to the IT Operations Department.

5.10 External penetration testing must at a minimum be performed semi-annually.

5.10.1 The testing is to be conducted by an external independent entity

5.10.2 The selection of the vendor is the responsibility of the Audit Committee.

5.10.3 Testing results are to be submitted to the CTO.

6. Teleworking Policy

6.1 MHS employees have an option for teleworking using MHS managed cloud based systems and/or equipment. The teleworking schedule must be requested in writing by the employee and/or Management and authorized by Human Resources.

6.2 Human Resources is responsible for notifying the IT Operations Department when a user is granted or denied teleworking privileges.

6.3 Teleworking equipment including connectivity devices must be company-owned and configured following company security standards.

6.4 The IT Operations Department is responsible for managing, maintaining, and monitoring the configuration of and the connection to the teleworking location.

6.5 Remote access will be granted following the Remote Access policy and standards.

6.6 The teleworker is responsible for the physical security of the telecommuting location.

Comentado [HW2]: I think we should update this for COVID. We can simply provide an intro to say all employees have the option for teleworking using equipment and cloud based systems purchased and managed by MHS (o something to that effect). I think the rest of the info stands OK.

6.7 Local storage of information classified as “protected” or “confidential” must be authorized by the IT Operations Department.

6.8 Monitoring the teleworker, teleworking schedule, and productivity is the responsibility of their reporting Manager.

7. User Access Control and Authorization

7.1 Default user access permissions will be set to “deny all” before the appropriation of specific permissions based on role and/or job function.

7.2 Access to company information and systems shall only be authorized for workforce personnel with a need-to-know to perform their job function(s).

7.3. Access shall be restricted to the minimal amount required to carry out the business requirement of the access.

7.4. An authorization process must be maintained. Permissions must not be granted until the authorization process is complete.

7.5. Information owners are responsible for annually reviewing and reauthorizing user access permissions to data classified as “protected” or “confidential.”

7.6. The IT Operations Department is responsible for managing the review and reauthorization process.

7.7. An annual report of completion will be provided to the Audit Committee.

8. Administrative and Privileged Accounts

8.1 Request for assignment of administrator-level accounts or changes to privileged group membership must be submitted to the IT Operations Department and approved by CTO.

8.2 The IT Operations Department is responsible for determining the appropriate use of administrator segregation of duties and dual controls.

8.3. Administrative and privileged user accounts will only be used when performing duties requiring administrative or privileged access.

8.4. All administrative and privileged account holders will have a second user account for performing any function where administrative or privileged access is not required.

8.5. User accounts assigned to contractors, consultants, or service providers who require administrative or privileged access will be enabled according to documented schedule and/or formal request and disabled at all other times.

8.6. Administrative and privileged account activity will be logged daily and reviewed by the IT Operations Department.

8.7. Administrative and privileged account assignments will be reviewed quarterly by the IT Operations Department.

9. Monitoring System Access and Use

9.1 The IT Operations Department and Human Resources are jointly responsible for determining the extent of logging and analysis required for information systems storing, processing, transmitting, or

providing access to information classified as “confidential” or “protected.” However, at a minimum, the following must be logged:

9.1.1 Successful and failed network authentication.

9.1.2 Successful and failed authentication to any application that stores or processes information classified as “protected.”

9.1.3 Network and application administrative or privileged account activity.

9.2 Exceptions to the above list must be authorized by the CTO.

9.3. Access logs must be reviewed and documented daily by the IT Operations Department.

10. Key Management

10.1 The IT Operations Department is responsible for key management including but not limited to algorithm decisions, key length, key security, and resiliency, requesting and maintaining digital certificates, as well as user education.

10.2 The IT Operations Department will publish cryptographic standards.

10.3 The IT Operations Department is responsible for the implementation and operational management of cryptographic technologies.

10.4 Without exception, encryption is required whenever “protected” or “confidential” information is transmitted externally. This includes email and file transfer. The encryption mechanism must be NIST approved.

10.5 Without exception, all portable media that stores or has the potential to store “protected” or “confidential” information must be encrypted. The encryption mechanism must be NIST approved.

10.6 Data at rest must be encrypted regardless of media when required by provincial and/or federal regulation or contractual agreement.

10.7 At all times, passwords and PINs must be stored and transmitted as ciphertext.

Following the above procedures of this policy will ensure MHS’s adherence to industry best practices, its compliance to several regulations, and will ensure safety and security of our systems.

For any questions to this policy, please contact the Privacy Officer via email at **privacyofficer@mhs.com.**

DOCUMENT CHANGE CONTROL

Date	Summary of Amendments	Changes Made by (Title)
May 11, 2020	Initial policy creation	Information Security Specialist
January 12, 2021	Annual Review	