Server and Computer Configuration Policy

PURPOSE
The purpose of this policy is to define how servers and computers are configured to ensure the protection of confidentiality, integrity and availability of Massachusetts Maritime Academy’s information systems.

The overriding goal of this policy is to reduce operating risk. This policy is intended to:
● Minimize operating system and application vulnerabilities.
● Minimize configuration errors and reduce server and computer outages.
● Reduce undocumented configuration changes that tend to open up security vulnerabilities.
● Facilitate compliance with the regulations and requirements applicable to the Academy.
● Protect data from unauthorized use and/or malicious attack.

SCOPE
This policy applies to all Massachusetts Maritime Academy (MMA) owned and operated servers, desktop and laptop computers. Servers include file and print servers, application servers, and database servers, residing either on-premise or in the cloud.

POLICY
All servers, desktops, and laptops will have configurations that are designed to protect and secure the operating systems and applications. Servers may require modification to baseline configurations in order to support different applications. Configuration modifications will be applied with a focus on the maximum amount of security that will allow applications to function properly.

● All computing resources must be inventoried with a tool which scans the MMA network and automatically inventories these resources. The inventory must include installed patches, applications, event log data, and hardware information. If possible, a cloud-based tool should be used to continue the inventory process when devices are not on the MMA network.
● Documented configuration baselines will be created and maintained for all servers, desktops, and laptops. The master images must be stored on secure servers and any changes to the master images must follow change management policy, as defined in the Change Management Policy.
● Configuration baselines will conform to industry best practices. Many vendors publish baseline configurations, such as Microsoft, and these should be used whenever possible to define the baseline configurations.
Server and Computer Configuration Policy

- Modifications to configuration baselines must be documented with compensating controls that will allow applications to function properly.
- Baseline configurations will be reviewed twice a year to identify any needed changes to enhance the security posture of the organization.
- No server or computer will be placed on the network without appropriate security configurations.
- All unnecessary ports, protocols and services not directly needed to perform the system’s specified function will be disabled.
- All unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web services will be removed from servers and computers, whenever possible.
- SEIM security and vulnerability software will be used to scan servers to stay up-to-date on new and emerging threats which may necessitate changes in server configurations.
- Default usernames and passwords will be changed/disabled on servers and computers prior to connection to the MMA network.
- System configuration management tools, such as Microsoft Group Policy, will be deployed to automatically enforce and redeploy configuration settings at regularly scheduled intervals.
- All servers will be patched with the latest available patches in a timely manner as defined in the Patch Management Policy.

ENFORCEMENT
Any employee found to have violated this policy, intentionally or unintentionally, may be subject to disciplinary action, up to and including termination of employment, per any applicable collective bargaining agreements.

RESPONSIBILITY
This policy is owned by the Vice President, Technology and Library Services, who will coordinate any and all revisions.

REFERENCES

<table>
<thead>
<tr>
<th>Framework</th>
<th>Regulations and Requirements</th>
<th>Supporting Standards and Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Top 20 Controls</td>
<td>PCI DSS - MA 201 - HIPAA</td>
<td></td>
</tr>
</tbody>
</table>
Server and Computer Configuration Policy

CSC 3

REVISION HISTORY

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Issued Date</th>
<th>Changes Made By</th>
<th>Description of Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>5/1/2020</td>
<td>Rob MacGregor</td>
<td>Initial edits and formatting.</td>
</tr>
<tr>
<td>1.1</td>
<td>5/10/2020</td>
<td>Anne Marie Fallon</td>
<td>Additional edits made.</td>
</tr>
<tr>
<td>1.2</td>
<td>5/13/2020</td>
<td>Anne Marie Fallon</td>
<td>Published the policy.</td>
</tr>
</tbody>
</table>