Computing Access Control and Management Policy

PURPOSE
The purpose of this policy is to establish standards for the administration of computing accounts that provide access to Massachusetts Maritime Academy’s (MMA) information technology resources and data. This policy establishes standards for issuing and managing computing accounts in order to protect MMA’s information technology resources and data from unauthorized access and use.

SCOPE
This policy applies to all MMA staff members, faculty and contractors who access MMA’s information technology resources.

POLICY
Computing accounts that access information technology resources and data at MMA require prudent oversight. The following security precautions should be part of account management:

Issuing Accounts and Access

- All access to MMA applications, systems and technology infrastructure must be authorized and approved. Any access not explicitly authorized and approved will not be granted and is forbidden.

- System access control is to be achieved via user accounts that are unique to each individual user to ensure user accountability.

- Access to specific applications, systems, and technology infrastructure shall only be granted to staff members with a legitimate business need. The level of access granted and privileges assigned to a user shall be limited to the minimum access required to perform their assigned job duties. This ensures that the standard security principle of “least required access” is utilized when granting access.

- A user account for new staff members, temporary staff members and guests will only be setup based on the Helpdesk’s receipt of written authorization from either the new user’s manager or a representative from Human Resources.

- For temporary staff members and guests, an expiration date must be entered on each user account they utilize, whenever possible. This will ensure that these accounts are disabled as soon as the temporary staff member or guest has completed their assignment.

- The use of generic and shared user accounts is allowed on rare occasion where it makes business sense. The associated access of these accounts must be highly restricted and they must be approved by the Vice President, Technology and Library Services prior to being created. The use of anonymous user accounts will not be allowed under any circumstance.
Computing Access Control and Management Policy

- When users create passwords for their accounts, the passwords must be a minimum of 8 characters, be complex and should not be shared or written down. Passwords must adhere to the standards set forth in MMA’s Password Policy.

- Access for all computing accounts must be configured through a centralized point of authentication, such as Active Directory or LDAP.

Managing Accounts and Access

- Changes to existing user access will require the Helpdesk’s receipt of written authorization from the user’s manager or a representative from Human Resources requesting the change.

- Managers must notify the Helpdesk when staff members are transferred or reassigned. This will prompt a review of access and adjustments will be made to remove unneeded access.

- Managers must notify the Helpdesk when staff members will be on a temporary leave. The staff member’s computing access will be disabled until they return to work.

- Managers must notify the Helpdesk when staff members have left the Academy. User access should be revoked upon termination of any staff member’s employment. To help identify staff members who have left the Academy where no notice was given to the Helpdesk, a monthly search for accounts inactive for 90 days or more will be done. The managers of these accounts will be contacted to determine if the staff member is still with the Academy and appropriate action will be taken regarding the user access.

- User accounts should be locked after 5 failed login attempts, whenever possible. Once locked out, the user account will remain locked for a period of 30 minutes, unless manually unlocked.

- When leaving a workstation, a staff member is expected to properly log out of all applications and networks. Inactive workstations will be logged off automatically after 20 minutes. Resumption of access will require the user’s password.

- The sharing of user accounts by staff members is strictly prohibited. Staff members must take precautions to keep their user accounts secure and refrain from writing them down.

Monitoring Accounts and Access

- For critical systems, an audit of system accounts must be completed twice per calendar year. This will be done to ensure that disabled accounts are removed, accounts inactive
Computing Access Control and Management Policy

for more than 90 days are removed and accounts for staff members no longer employed
are removed. Any exceptions made during this process must be documented.

Administrative Level Access
- The allocation of privileged system access must be restricted and controlled. The
  granting of privileged access should be limited to the smallest number of personnel
  possible to prevent the loss of confidentiality.
- Personnel who have administrative system access must use other less powerful
  accounts for performing non-administrative tasks.
- Activities performed as an administrator or super-user must be logged, whenever it is
  feasible to do so.

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.

RESPONSIBILITY
Under the direction of the Vice President of Technology and Library Services, TLS Directors
are responsible for coordinating and establishing procedures and practices which are necessary
for compliance with this policy.

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

REFERENCES

<table>
<thead>
<tr>
<th>Framework SANS Top 20 Controls</th>
<th>Regulations and Requirements PCI DSS - MA 201 - HIPAA</th>
<th>Supporting Standards and Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSC 12-8, 16-1 – 16-7, 16-9 – 16-12</td>
<td></td>
<td>Staff Onboarding Procedure</td>
</tr>
</tbody>
</table>

REVISION HISTORY
This section contains comments on any revisions that were made to this document and the date
they were made.
<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>1/12/2016</td>
<td>Compass ITC</td>
<td>Initial Draft</td>
</tr>
<tr>
<td>2.0</td>
<td>2/5/2016</td>
<td>Anne Marie Fallon</td>
<td>Additions made to policy</td>
</tr>
<tr>
<td>2.1</td>
<td>5/13/2020</td>
<td>Anne Marie Fallon</td>
<td>Made edits to policy.</td>
</tr>
</tbody>
</table>