TECHNOLOGY ACCOUNTS MANAGEMENT 1.80

DEFINITIONS:
♦ EVMS et al. includes
  ▪ Eastern Virginia Medical School (EVMS)
  ▪ Eastern Virginia Medical School Health Services (EVMSHS)
  ▪ Eastern Virginia Medical School Pediatric Faculty Associates (EVMSPFA)

♦ ITMT refers to the appropriate member of the Information Technology Management Team comprised of the management representatives of:
  ▪ The EVMSHS Data Processing Department
  ▪ The EVMS Business and Financial Information Systems Center
  ▪ The EVMS Network Information Center
  ▪ The EVMS Data Base Center
  ▪ The EVMS Communications Department
  ▪ The EVMS Library Services.

POLICY:

The Medical School creates and maintains various levels of network accounts and connection privileges for the benefit of its faculty, staff, and students. Operational cost, network security, and data security requirements dictate that specific policies govern the administration of such accounts. This document establishes criteria for creating, maintaining, and deleting all levels of technology accounts and the associated levels of services.

PROCEDURES:

ACCOUNT CREATION OR MODIFICATION

Network and Email Accounts:
• All levels of network and email accounts and their attendant privileges will be issued only when the required documentation has been received and the creation authorized by a member of the ITMT.
TECHNOLOGY ACCOUNTS MANAGEMENT 1.80

- Modifications related to access to existing network or email accounts will only be made after a documented request is received by the account holder or the responsible departmental leadership. Personal presentation of an EVMS ID Badge will be accepted. Example: password changes.
- Modifications related to privilege extension or suspension to existing network or email accounts will only be made after a documented request is received by the responsible departmental leadership. Additional approvals may be required if the extension of privileges is to an area not under the control of the requestor. Examples: drive maps to different servers, drive maps to different directories, access privileges to directories owned by others, access to other’s email accounts.

Application Accounts:
- Application accounts are administered by security officers charged with the maintenance of user privileges and management procedures related to the application. Examples are:

<table>
<thead>
<tr>
<th>Application</th>
<th>Security Officer Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time &amp; Attendance</td>
<td>Financial Services/BFIS</td>
</tr>
<tr>
<td>Monarch</td>
<td>BFIS</td>
</tr>
<tr>
<td>OneSource</td>
<td>Financial Services/BFIS</td>
</tr>
<tr>
<td>Library Access</td>
<td>Brickell Library</td>
</tr>
<tr>
<td>IDX or EMR</td>
<td>Health Services Data Center</td>
</tr>
<tr>
<td>Blackboard</td>
<td>Network Information Center</td>
</tr>
<tr>
<td>Oracle</td>
<td>Database Center</td>
</tr>
</tbody>
</table>

- Application accounts and their attendant privileges will be issued only when the required documentation has been received and the creation authorized by the application security officer in the responsible area. Required documentation may differ between applications; the security officer will provide specifics on request.
- Modifications to access or privileges related to specific applications must be made by the appropriate security officer and will only be completed upon receipt of the required documentation. Required documentation may differ between applications; the security officer will provide specifics on request.
TECHNOLOGY ACCOUNTS MANAGEMENT 1.80

FULL NETWORK SERVICES
Permanent full network services accounts may be provided to Board of Visitor approved full-time unpaid faculty (PEDS/VA), or community faculty assigned permanent EVMS space, employees (staff/residents/faculty), matriculated students, tenants and affiliated agencies for access to on-campus file storage and print services. Requests for such accounts must come from the responsible departmental leadership for faculty and staff or the Vice President for Administration and Finance for tenants and agencies. Student accounts are created at the request of Student Affairs, Health Professions Program Managers, or the department of Graduate Medical Education. Such accounts normally include personal folder storage on a campus network file server. Validation of personnel status may be requested as follows: employees to Human Resources, students to Registrar or Health Professions, residents to Graduate Medical Education, and faculty to Faculty Affairs.

Temporary full network services accounts may be established for contractors at the request of the responsible departmental leadership if the request stipulates that access to network services is necessary for the contracted work to be completed. These accounts will require an expiration date for setup. The request must also include confirmation that a confidentiality statement and a HIPAA Business Associates Agreement have been completed.

AUTHENTICATION SERVICES
Accounts for authentication only may be granted on request for individuals who do not otherwise qualify for full network services account privileges. Such accounts may be used for Blackboard access and Library online resource access. Examples include but are not limited to guest instructors for Blackboard courses, special Blackboard student categories, and community faculty who request access to library resources. Requests for special Blackboard access should come from the associated Blackboard course director. Requests for community faculty access to library resources should be directed to appropriate library staff.

EMAIL ACCOUNTS
EVMS email accounts are granted only to persons who qualify for full network file services. Requests for such accounts must come from the responsible departmental leadership for faculty and staff or the Vice President for Administration and Finance for tenants and agencies. Student accounts are created at the request of Student Affairs, Health Professions Program Managers, or the department of Graduate Medical Education.

Email accounts are not available for community faculty not assigned permanent EVMS space,
volunteer faculty, guest lecturers, volunteer staff, consultants, and non-matriculated students.

Temporary accounts may be established for contractors at the request of the responsible departmental leadership if the request stipulates that access to email is necessary for the contracted work to be completed. These accounts will require an expiration date to be setup.

REMOTE CONNECTIONS
Remote connections to on-campus computer systems with software such as pcAnywhere or VNC require specific written authorization by the responsible senior departmental leadership. Remote connections are not authorized with telephone modems. Remote access requires an encrypted connection via the campus VPN. Remote connections may only be granted to persons who qualify for permanent full network service accounts and contracted technical support.

ACCOUNT TERMINATION
All levels of network and application accounts and their attendant privileges will be terminated when the account holder status changes such that the account creation criterion no longer exists. The responsible departmental leadership may request the termination of account privileges at any time.

FULL NETWORK, EMAIL and APPLICATION ACCOUNTS
Employee Accounts – will be terminated when a notice of termination is received from Human Resources Department.

Non-paid Faculty Accounts – will be terminated when the faculty member no longer occupies permanent EVMS space, the faculty assignment has been terminated or at the request of the responsible departmental leadership.

Student Accounts – will be terminated upon graduation, when the individual is no longer a student in good standing in his or her program or at the request of the responsible departmental leadership. Graduating Medical students may request continuance of email accounts for up to 45 days after graduation to assist in their transition to a residency assignment.

Tenant/Affiliated Accounts – will be terminated when the tenant no longer occupies permanent EVMS space, at the separation of an affiliated agency or at the request of the Vice President for Administration and Finance.
Temporary Accounts – will be terminated on the expiration date indicated in the setup request by the responsible departmental leadership or at the request of the responsible departmental leadership.

**AUTHENTICATION ACCOUNTS (BLACKBOARD and LIBRARY RESOURCE ACCESS)**
These accounts will be terminated when the Blackboard Course activity is completed, when the qualification criteria for library access is no longer met or at the request of the responsible departmental leadership.

**REMOTE ACCESS ACCOUNTS**
Remote access accounts will be terminated when the faculty or employee’s work assignment no longer requires remote access privileges or at the request of the responsible departmental leadership.

**EMPLOYEE TRANSFERS**
This provision is designed to protect confidential departmental information associated with an employee’s former department. Departmental leadership losing an employee due to transfer may request that an employee’s mailbox be retired for a period of time not to exceed 60 days and designate other personnel to have access prior to the mailbox’s termination after that time. If such a request is made, a new set of credentials are to be issued to the employee for use in their new department to access a new mailbox. The credentials for the retired mailbox will be modified and provided to the former department’s designee. No access to the retired mailbox will be allowed by the employee. The former department designee will have full rights to the retired mailbox and may forward email to the employee’s new mailbox manually if desired. The request should occur prior to the physical transfer of the employee to eliminate all possible email conflict, if made after the physical transfer the former department must forward all emails relative to the new department to the new mailbox.

**POLICY VIOLATIONS**
Network or email accounts may be terminated if:
- It is subsequently determined that the account holder does not actually qualify for the particular account which has been created.
- The account holder commits significant infractions of campus information technology policies while utilizing the account.