University of Alberta
Faculty of Medicine & Dentistry
Med Account Usage Policy

<table>
<thead>
<tr>
<th>Office of Accountability:</th>
<th>Office of the Dean</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office of Administrative Responsibility:</td>
<td>Chief Operating Officer, FoMD</td>
</tr>
<tr>
<td>Approver:</td>
<td>Faculty Administration Committee</td>
</tr>
<tr>
<td>Scope:</td>
<td>Compliance with this policy extends to all members of the Faculty community (faculty academics, support staff, trainees, etc)</td>
</tr>
<tr>
<td>Effective Date:</td>
<td>March 2015</td>
</tr>
</tbody>
</table>

Overview
The Faculty of Medicine & Dentistry (FoMD) encourages the effective usage of computing resources to support the research, education, clinical care, and administrative missions of the Faculty and University. With a complex network of connected servers and computing devices, it is imperative that such resources are used in an effective, safe, ethical, and lawful manner to protect the information and interest of the University. This policy extends the University’s UAPPOL policy “Information Technology Use and Management” with additional requirements applicable to FoMD.

Policy:
The following defines the expectations and requirements around the creation, usage, and termination of the Faculty’s MED domain account:

Account Creation
- All faculty, staff, and students/learners affiliated with FoMD are entitled to have a MED account created.
- Temporary accounts can be created for non-affiliated FoMD users, must be sponsored by a FoMD organization unit and authorized by the APO or senior department administrator. Temporary accounts must have an end date no longer than one year.
- Any faculty, staff, and students/learners, identified by the University’s PeopleSoft with an “Active” status, will have their associated MED accounts created automatically within one business day if a MED account does not already exist. An email notification will be sent to the supervisor with the account login information. A supervisor can contact the MedIT Service Desk to create MED accounts at any other time prior to this.
- Any security access to IT resources must be authorized by the APO or senior department administrator.

Account Usage
- Account usage must comply with the requirements of the University’s UAPPOL policy “Information Technology Use and Management”.
- All accounts are entitled an allocated amount of network storage assigned by the department or unit based on Faculty’s IT standards.
Each person is responsible for all activities performed under his/her login information, and must exercise care in protecting his account such as the following:
  o Workstation should not be unattended without logging out or locking his/her machine.
  o Passwords should not be written down and displayed in visible areas.
  o Passwords should be changed if known by another person.
Each person should only collect, access, use, and disclose information necessary for the purposes of fulfilling the assigned duties and responsibilities.
The obligation to keep information confidential continues even after the person leaves employment or relationship with the University.
Any potential or actual information breach should be reported to his/her immediate supervisor immediately.
While limited personal use (i.e. not related to the mission of the University) is allowed provided that it complies with the UAPPOL policy above, the Faculty reserves the right for the unit’s APO or senior department administrator and IT staff to access any business information (documents, emails, pictures, folders, links, etc.) within all FoMD systems for the purpose of conducting the business of the University or breach investigations.

## Account Termination
- The APO or department administrator of the terminated faculty, staff, students/learners, must notify MedIT at least one business day so that account access can be revoked appropriately.
- The APO or department administrator of the sponsored temporary account, must notify MedIT at least one business day so that account access can be revoked appropriately.
- Any faculty, staff, and students/learners, identified by the University’s PeopleSoft with an “Inactive” status, will have their associated MED accounts disabled automatically within one business day.

## Account Audit and Usage Violation
- The Faculty may conduct audits of accounts without any notice.
- The Faculty reserves the right to remove account access to anyone that violates this policy.

## DEFINITIONS

<table>
<thead>
<tr>
<th>MED Account</th>
<th>Allows access into FoMD computing network environment, such as network file storage and AHS trusted network (if applicable).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Faculty community</td>
<td>Includes but not limited to individuals of FoMD including academic staff, support staff, trainees (undergraduate students, postgraduate students, post docs, summer students, etc), and volunteers.</td>
</tr>
</tbody>
</table>

## RELATED LINKS

Should a link fail, please contact FoMD MedIT. [▲ TOP]

Information Technology Use and Management Policy (UAPPOL)
Information Technology Security Policy (UAPPOL)
Freedom of Information and Protection of Privacy Act (FOIPP)