ADMINISTRATIVE ACCOUNT REVIEW PROCESS:
BIOMEDICAL SYSTEMS AND DEVICES ON MEDICAL DEVICE NETWORKS

1. Purpose

1.1.1   The primary purpose of this procedure is to ensure that regular review of all administrative accounts for systems and devices on the medical device networks are authorized and up-to-date. Administrators, due to the nature of their roles, have elevated privileges to make changes to a system. These privileges include tasks such as installing software, changing system settings, and installing system updates.

1.1.2   Protection of administrative accounts is important to ensuring system integrity. This process is therefore important to ensure that accounts only have the minimum privileges necessary to perform the functions needed and only be used when required.

2. Definitions

Acronym or Word	Definition
ADUC	Activity Directory User and Computer, a Microsoft product
VPP	These organizations are collectively referred to as VPP: Vancouver Coastal Health (VCH), Providence Health Care (PHC), and the B.C. Provincial Health Services Authority (PHSA)
FHA	Fraser Health Authorities
BME	Biomedical Engineering
PU	Power User
SA	Secondary account with no profile
LMBME	Lower Mainland Biomedical Engineering
FMO	Facility Management Office

3. Scope

3.1   Included:

3.1.1   Networkable assets for which LMBME has the responsibility to maintain their records are in scope. This is typically in the form of, but not all inclusive of scheduled maintenance, work orders, alerts and incidents

3.2   Excluded:

3.2.1   All assets supported by IMITS including non-clinical PCs, Laptops, printers, servers, etc.

4. Procedure

4.1   VPP User Groups

The user groups, description, group owner, and frequency of reviews of user groups will first be documented below for the VPP BME team. Next, the steps to perform key procedures to review, add, and remove members as well as to request new users will be documented for VPP BME.

4.2   List of VPP User Account Lists, Descriptions, and Update Frequency

Root User Group Name	Description	Group Owner	Frequency to Update
VPP_BME_PU	This group policy grants non-administrative power user privileges to BME resources that require access the ADUC tool.	VPP_BME Manage	Bi-annual
VPP_BME_Admin	These group policies grants local administrative access to the PC's in the Biomed department, or any clinical computer that has this group added for local admin. This level of access is often needed for troubleshooting issues or installing updates to software that our department manages. It is granted specifically to the SU user accounts for users.	VPP_BME Manage	Bi-annual
VPP_BME Manage	This group policy grants privileges to modify, add, and remove users from the VPP_BME_PU and VPP_BME_Admin user groups.	VPP_BME Manage	Bi-annual
VPP_BME Group Managers	This group policy grants privileges to modify, add, and remove users from all users groups within VPP_BME.	VPP_BME Group Managers	Bi-annual

4.2.1   Navigate to the VPP User Groups

This procedure will need to be completed at minimum biannually by a member of the VPP_BME Manage user group in order to access the ADUC tool and view the user groups for VPP BME. The next step 4.2.2 will be completed immediately following these steps.

A job aid has been created with screenshots to walk through each step listed. See the "Supporting Documents" section of this document.

Step Number	Description
1	Login to https://seth.healthbc.org/logon/LogonPoint/tmindex.html with your personal username, password and domains.
2	Click on "**Active Directory Users and Computers**" from the list of "All Apps" once logged in.

3	Select **Admin**. Next, click on "**Action**" on the top left.
4	Use the "**Find User, Contacts, and Groups**" action from the first drop down. In the second dropdown beside it titled "In", select "**vch.ca**".
5	Type "**vpp_bme**" in the field titled "**Name**" and then click **Find Now** on the right-hand side.
6	After clicking find now, a list of all user account groups will be displayed.

4.2.2　Review, Add or Delete Users from VPP User Group

This procedure will need to be completed at minimum biannually by a member of the VPP_BME Manage user group to review and update user privileges.

Below are the steps required to review, add or delete users from a user groups. A job aid has been created with screenshots to walk through each step listed. See the "Supporting Documents" section of this document.

Step Number	Description
1	From the list of VPP user account lists, click on one of the group lists to review. In this job aid, steps for the **VPP_BME_Admin (RL)** group list have been documented as the main admin account. These steps should be performed for each group list below to ensure they are all up-to date. *Note: Only users who are part of the "VPP_BME_Manage (RL)" group have the authority to add an account to the admin list.*
2	Click on the "**Members**" tab to review a list of the users that have administrative account access.
3	A complete list of users that have administrative account access will be displayed.
4	Upon Completion of a Periodic review of administrative accounts, users may need to be removed. To perform this action, select the user from the list and then click **Remove**.
5	Alternatively, if a user needs to have their account permissions elevated and therefore added to the list, click on "**Add**" user. *Note: Only SA accounts should be added within VPP for system security. To request an SA account, see the "Request SA account" subsection.*
6	Enter the name of the user (in the format: "DOMAIN\USER") in the text field. Validate the name and user by next clicking on "**Check Names**".
7	Confirm the user selected is correct. If this looks correct, click "**OK**"
8	The text will have updated upon completing the check names step. Click on **OK** to complete the process to add users.

9	In an existing account requires further elevation in order to manager the list of administrative users, it may be added to the list of VPP_BME_Group_Manage group by any other member of that privilege level.

4.2.3   Request a New User to be Setup for VPP (Not User Group Specific)

This step will be complete on an ad-hoc basis as requested. A job aid has been created with screenshots to walk through each step listed. See the "Supporting Documents" section of this document.

Step Number	Description
1	Only SA user accounts for VPP can be added to the list of administrative users. To request an SA Account, a ticket request must be raised with the IT Help desk. To raise a ticket with the help desk, click on the below link: https://healthbc.service-now.com/sp_phsa_vch_phc/?id=search&spa=1&t=sc&q=sa%20account
2	The supervisor of the user must approve the ticket request when prompted via email. In case of a delay or issue, record the ticket number. In case of a delay (e.g. supervisor illness), forward the ticket number and a spreadsheet of pertinent user accounts to PHSA's Identity Services team.
3	All SA user accounts will have "_SA" listed as their suffix.
4	Once complete, the user will be added to the appropriate group per the service request.

4.2.4   Process for Requesting, Adding, or Removing for FHA Admin Accounts

This step will be complete on an ad-hoc basis as requested. A job aid has been created by FHA that details the steps performed to request, and remove users. See the "Supporting Documents" section of this document.

4.2.5   Process for Reviewing for FHA Admin Accounts

This step will be completed annually by the User Experience and Service Management team at FHA to ensure that the LMBME members of FHA have appropriate access.

Step Number	Description

1	A request is logged in Service Now with a list of current team members that require admin access by an LMBME delegate. The ticket needs to be assigned to "FH-HI-Device Engineering". Note: In case of any issues, contact FHAUXDesktopEng@fraserhealth.ca
2	The list in the ticket is then reviewed by the User Experience and Service Management team. The list provided in the ticket will be analyzed against the list of users listed in the Ivanti tool.
3	User privileges are modified, added or removed based on the list submitted by LMBME per existing FHA procedures. FHA's User Experience and Service Management team has a list of permissions for biomed admin access in working with them. Based on this, a security group in FHA's Invanti tool has been created for LMBME users. Any new machine added to this group will be updated automatically with the relevant permissions. Admin account access for users on the machine are controlled by a security group in Active Directory called "Ivanti users". Note: Refer to FHA's job aid "· Instructions for Elevating Access & Unmanaging workstations" for the steps taken to modify, add, or remove user accounts.
4	The ticket is closed by the User Experience and Service Management team at FHA. This will trigger an email alert to the LMBME delegate that will be saved on the LMBME SharePoint site for traceability by the requestor.

5.   Reference Documents

The below should be reviewed in conjunction with this document:

- Job Aid – Administrative User Accounts for the ADUC Tool
- Instructions for Elevating Access & Unmanaging workstations (For FHA process)

Effective Date:	10-JUN-2021			
First Released:	10-JUN-2021			
Last Revised:				
Last Reviewed:				
Approved By:	LMBME Executive Director			
Owners:	Cybersecurity Team			
Revision History:	Version	Date	Description/ Key Changes	Revised By
	1.0	10-JUN-2021	Reviewed with LMBME directors	Biomed Directors