CAIR IT Manual

Table of Contents

IT Support

Support Requests

Except where noted with highlighting this manual is identical to the SFMRC IT Manual v.1.5. You should assume that "SFMRC" can be replaced by "CAIR" unless otherwise indicated.

IT requests can be sent via email to perry.radau1@ucalgary.ca. Some requests will be delegated to the Seaman Family MR Center (SFMRC) IT.

Person	Email	Desk Phone	Primary Area of Support
Mark Winder	mark.winder@ucalgary.ca	42824 (944-2824)	SFMRC, any IT escalation
Victor Tse	victor.tse@ucalgary.ca	41919 (944-1919)	SFMRC
Perry Radau	perry.radau1@ucalgary.ca	55436 (955-5436)	ACH

Work is done on a best-effort basis – new higher priority tasks may come in and delay your items. We attempt to meet the following service levels, but these are guidelines only:

Urgency	Target Timeline
Urgent	Immediate Attention
High	48 hours
Medium	1 week
Low	Longer than 1 week

Some support requests must be passed on to the AHS IT or U of C IT (UC IT) groups. This generally results in delays beyond our target service levels.

We may reprioritize items at any time (particularly if there are reasonable workarounds or if items are languishing at the bottom of the priority list).

Priorities can be negotiated with any IT member. If you are not satisfied with the results, conflicts can be escalated to the IT Coordinator.

Operating Hours

Core hours are between 9:00 AM and 4:00 PM weekdays. But generally someone will be on-hand from 9:00 AM – 5:00 PM weekdays.

After Hours Emergencies

If you truly encounter an IT emergency in the evening, weekend, or holiday you can call Mark Winder on his cell at 403-919-9617.

Partner IT Groups

SFRMC IT group cannot help with some issues (for example, with your AHS computer or your U of C email). In these cases we will direct you to contact the AHS or the UCIT groups directly.

If you are having difficulties getting results from another IT organization we can help you converse with their support groups, but you may have to initiate the support call.

AHS IT: 403-310-3111 servicedesk.cal@ahs.ca
http://insite.albertahealthservices.ca/6562.asp

U of C IT (UCIT): 403-220-5555 itsupport@ucalgary.ca
https://ucalgary.service-now.com/it

Contact AHS IT if:

- the computer is owned by AHS (Windows computer with tag).
- it's a network issue (Ethernet port requires activation).

Contact UCIT if:

- issue with UCID password or email address.
- issue with software from the U of C software distribution (e.g. Matlab)

Resources

The technology infrastructure that you use is jointly owned and operated by AHS, the U of C, and Principal Investigators (PIs). The SFRMC IT group primarily maintains it.

As such, there is a complicated set of policies that we need to conform to depending on the resource and where it is located. As a general rule:

Resources managed by the SFMRC IT will conform to the most restrictive of AHS, U of C, and SFRMC policies when appropriate. In this way we will meet everyone's guidelines and benefit from a good relationship with our partners.

If there is a discrepancy between AHS and U of C policy we will favour AHS.

There are cases where, in our unique context, policies do not make sense or are not practical to apply. The SFMRC IT staff is happy to explain conflicting policies. Some of these cases are documented here.

Acceptable Use of IT Resources

The University and AHS both have "Acceptable Use of Information Assets" Policies.

http://www.ucalgary.ca/policies/files/policies/Acceptable%20Use%20of%20Information%20Assets%20Policy.pdf

https://extranet.ahsnet.ca/teams/policydocuments/1/clp-ahs-pol-it-acceptable-use.pdf

To broadly summarize, IT Resources you access should only be used for authorized purposes in support of authorized business-related activities. Using IT Resources for personal business or for personal gain or to do something illegal is not permitted.

Additionally, you can't use or alter IT Resources in a way that will negatively impact or interfere with other Users' ability to do their work. Hacking, whether for good or evil, is not allowed.

Computers

Most computers at the center are Macs, but we do provide limited support (on a case-by-case basis) of Linux and Windows systems as well. Computers are owned and assigned in an arrangement with the PI/Group and the SFMRC.

There are a small number of AHS computers at our sites. If they have an AHS sticker then any hardware issues, software installs, etc. are done through AHS IT.

Personal Computers

You may bring in personal devices but **external equipment is not allowed on the AHS wired network at the Seaman Family MR Centre or Alberta Children's Hospital.** You may connect wirelessly to an AHS network such as healthspot (public) or AHSRestrict (private for those with AHS usernames).

Borrowing and Moving Computers and Accessories

If you need a mouse or keyboard do not take one from a nearby computer. In some cases the accessories are matched to a system and you will be causing harm by taking what is not yours. Even if the intention is to borrow it temporarily.

If you have any problems with accessories (mice, keyboards, etc.) talk to your friendly SFRMC IT person and we'll help you out.

Moving computers by yourself is also not allowed (unless IT is in the loop). We have records of our equipment and where it is located. If it moves around without our knowledge it is difficult to find in our audits.

Taking things home

You need permission from your Manager/PI (who is presumably the equipment owner) and a letter signed by IT approving the transfer (or risk being accosted by security as you exit the hospital). There should be a time frame for returning the equipment.

Equipment Disposal

Even if equipment is broken or has little market value, all the resources you use at the SFMRC are owned by someone (U of C, AHS). As such, you can't throw it out, take it home, or give it away. It's not yours.

Anything with an asset tag (and some things without) are tracked and must be disposed of using an appropriate process. Both AHS and U of C have their own processes for recycling or surplusing equipment, regardless of whether it is operational.

http://www.ucalgary.ca/finance/scm/distribution/material-disposal

http://insite.albertahealthservices.ca/1536.asp

Special care must be taken disposing equipment with built-in storage devices. By policy old hard drives that may have contained health data must be securely erased (ideally by SFMRC IT) or physically destroyed.

Data Storage

The SFMRC provides storage space accessible from AHS locations in the form of file server shares and a research PACS (rPACS). In general, network storage space is backed up to a secondary site (if you want to verify your data backup plan, ask SFRMC IT).

CAIR storage is on the server "grotto" (IP 139.48.221.20). Upon joining CAIR you will be assigned a username and group.

SFMRC storage can be allocated on request, but is a limited resource. Depending on your requirements there may be a financial conversation.

We recommend that network shares be used for valuable data that warrants the built-in backup and long-term availability. We recommend using the storage in your workstation and/or an external NAS or DAS device (eg. Synology, Promise) for storing intermediate/processed files. Particularly if these files are not required again or can be easily regenerated.

Users at a location in the University will have the opportunity to purchase storage directly from UC IT (Compellent storage).

If your whole team is physically located within AHS you may also request a network share from AHS IT (via a Network Access Request).

Storage (mobile)

AHS requires that all of their mobile devices, including phones, laptops, and portable storage devices be encrypted. At the SFRMC we do not have personally identifiable

health data, so this is not a requirement. However, it would be embarrassing to have to report that data has gone missing so we recommend:

1. Don't put data on mobile storage (portable drives, USB) unless absolutely required.
2. Encrypt it if possible (SFRMC IT can help).
3. Remove the data when you are done.
4. Don't leave portable storage in plain sight when not in use.
5. Don't take portable storage off-site unless necessary.

Software

Although the AHS does not allow you to install software on their computers, we are more permissive on CAIR computers provided that:

1. You have a legal license. Your research group is responsible for the cost unless other arrangements have been made.
2. The software comes from a reputable source for a reputable purpose.
3. The software does not introduce known security risks.
4. You understand CAIR IT may not be able to support your use of the software.

We can also make recommendations on software packages given your requirements.

Anti-virus

The policies of SFMRC and CAIR require that every lab computer has anti-virus installed. This is a minimum standard to maintain computer hygiene and not adversely affect the entire network. Currently the standard anti-virus software is Kaspersky or ESET. If you find that this software is causing performance issues, you should seek help from IT to resolve the issue rather than disabling it.

Network Access

Most of our users are sitting in a hospital facility with network services provided by AHS. It is recommended to use the wired (Ethernet) network for best performance. If the occasion requires wireless, use the private wireless network AHSRestrict with username and password from AHS (e.g. <FirstnameLastname> for username). This private network has access to the servers and printers, but the public network (healthspot) does not.

Computers that are plugged into the wall are given IP addresses automatically via a protocol called DHCP. If you will routinely use a DICOM client like Horos, a request can be made to AHS IT for a static (reserved) IP. Otherwise your PACS connectivity may fail when the DHCP protocol assigns you a new IP.

You must not assign your own static IP! Although, if you are clever you could get it to work, you may also be colliding with the legitimate IP owner causing network issues for both of you!

The only wireless access available at most AHS sites is through AHS. To connect you will require an AHS ID. If you do not have one, the only wireless connectivity option for you is healthspot.

Some clever folks have figured out that they can use their Mac workstations as a wireless access point. Although this does allow you to connect your devices to the AHS network wirelessly, it also potentially allows the public to do the same. This is a security risk, even if you've setup a password, and is not allowed by AHS policy.

If you are still tempted, AHS IT limits each network jack to 3 "devices" – of which your computer is one, as are VM's on your computer, as are devices you allow to connect wirelessly. If you exceed 3 devices your network access may work sporadically. For the same reason you can't connect your own switch or hub. If you are short on ports you should discuss your challenges with SFMRC IT.

If you are sitting at a University location (eg. Health Brain Aging Lab) you will have access to the University wireless (if you have a University ID). Any networking requests for static IP's or port activation at University locations are done through UC IT.

Hacking

Hacking is not permitted on AHS network, U of C network, or from the SFMRC. If you require the install of software that may have utility in hacking you must get written permission from the SFRMC IT and notify the Centre's Scientific Director, even if the intended use of the software is good.

Intrusion Prevention Systems (IPS) monitor our networks. They will quickly pinpoint a workstation that is generating non-standard traffic. If you are about to do something you know is not allowed, just don't do it.

Don't try and guess other people's passwords. If you are in a situation where you need to guess, please enlist the help of the SFMRC IT group.

Don't access data you are not specifically consented to access. If you don't have explicit permission, you must ask. If you don't know who to ask, someone from the SFRMC IT group can help you find the proper contacts (but it is your responsibility to ask).

Physical Access

If the public has unsupervised access to our workstations then our data and personal belongings are not secure. It is every person's responsibility to make sure doors are closed and/or locked when appropriate.

Thieves may follow you into the center or other research area (which is also called tailgating). If it is someone you don't know, it is not rude to ask them who they are and what their business is. If their answer or actions are suspicious don't hesitate to call security.

Unattended computers should be screen locked and require a password after 10 minutes of inactivity.

Backups

It is your responsibility to backup your data properly. Most Macs have an external hard drive for Time Machine backups. You can request one from your PI.

Network shares are generally backed up, but if you have valuable data and have any concerns about backups please verify with the SFRMC IT group.

If you have a network home folder, it is backed up. If you have a local home folder you should discuss backup options with someone from the SFRMC IT group. Some workstations have a network or local instance of TimeMachine available. Other workstations may require a Chronosync backup to a network share.

If you have local home folders, even if you do not have an automated backup solution you should consider copying valuable files to a network share or external media on a frequent basis.

Cloud Backups

There are many cloud backup solutions (eg. iCloud, One Drive, etc). You should not store health care data in cloud solutions, even if it is not personally identifiable.

If you do use a cloud backup service or cloud storage for other data types you should use a service that encrypts the data and/or you should personally encrypt the data before uploading it. A service that stores your data in Canada is preferable to a service that stores your data in another country (eg. United States). Data should be removed as soon as it is no longer needed.

Onboarding

As new members are hired, the P.I. will ideally give SFMRC IT two weeks notice to set them up, but any notice is better than no notice.

There are excellent on-boarding checklists for the U of C here:

http://www.ucalgary.ca/hr/onboarding-checklist-new-hires

A new employee can request a U of C email address as soon as they have a UCID. In addition, to setup a new member for SMFRC resources you need to provide:

1. User's full name (correct spelling)
2. Start date
3. Current contact info (if possible, in case IT has questions)
4. User's manager/PI
5. Where the user will be sitting (ask the PI)
6. What computer equipment he/she will be allocated (based on a negotiation between the SMFRC and the PI of available resources)
7. Local or Network home folders (pick local if he/she doesn't move between computers)
8. Phones at the Centre are managed by AHS and should already be active, but SFMRC IT can submit tickets for password resets, etc. if required.
9. Email is arranged through U of C (http://www.ucalgary.ca/hr/just-joined)
10. The software the user will need (U of C software licenses will be requested with the User's U of C ID).
11. The data the user will need access to (see data access policy).
12. AHS access card (physical access – arranged through Glenda)

It would be prudent for new staff and trainees to book a few minutes of SFMRC IT time to go over their setup and ensure they have everything they need to be productive. At some point in the future there may be a mandatory IT orientation.

Offboarding

The PI must notify SFMRC IT when User's last day is. The user will be unable to log in after their last day unless SMFRC IT is notified of a different last day of access.

The PI must ensure the user has returned his/her access cards, keys, FOBs, etc. to the appropriate people.

Users with local home folders will have their home folder archived to a central storage location on their last day of access. This local data may be removed from the workstation after the last day of access (after it is archived) to prepare the workstation for a new user.

Users with network home folders will have their home folder moved to a central storage location.

If the user has data/results in their home folder that other users will need, it is the PI's responsibility to ensure it is copied/moved to the new recipients. If the user has data/results outside their home folder it is particularly important that the PI be aware of this and make archival or access arrangements with SMFRC IT.

User Accounts and home folder contents will be stored for a minimum of 3 months after their last day. If the data stored in the user's account requires longer retention the PI must make appropriate arrangements with SFMRC IT.

We will archive data for 3 years. After this period, it is the PI's responsibility to arrange a suitable archive location.

User Accounts

User accounts are required for authentication (to prove who you are) and authorization (to manage what you can access).

In general, the AHS and UC IT departments will not allow someone from SFMRC IT to manage accounts on your behalf. If you have account/password issues on a U of C or AHS account it is up to you to submit the request, although we can assist in any support conversations.

Each user is responsible for the actions performed with their user account. **Personal accounts should never be shared.** If you require an account for group access, for example to access a research application or data, talk to SFRMC IT.

As you are responsible for actions taken with your account, unattended workstations should have a screen saver with a password lock (recommended 10 minutes or less) to prevent someone from using your workstation with your credentials while you are away. On a Mac choose these settings:

```
System Preferences / Desktop & Screensaver / Start After 10minutes.
System Preferences / Security & Privacy / Require password 5 sec after
sleep or screen saver begins.
```

Tip! Pressing Control-Shift-Eject on a Mac will lock the system immediately.

Passwords

Passwords are one of those challenging areas where we have to find a balance between security and convenience. You will likely have many passwords to manage - for mail, file shares, databases, web sites, etc.

AHS and U of C both have password policies that you have to follow to access their systems.

http://www.ucalgary.ca/it/services/it-account

http://insite.albertahealthservices.ca/4237.asp

These URL's also contain links to sites where you can reset your AHS and U of C passwords. To reset an SFMRC password just talk to someone in the SFMRC IT group.

The Seaman Centre also has a password policy for the systems we manage. It is not as strict as AHS and U of C, but we do require:

1. Choose a secure password. A longer password is better than a complicated one. You may want to use a passphrase instead of a single word. We will not force you to choose letters/numbers/symbols, but for your part do not pick a password that is easy to guess.
2. Your passphrase should be easy to remember. You may write it down or use a password program (e.g. 1Password). But do not attach it to your computer or anywhere it can easily be found.
3. DO NOT SHARE YOUR PASSWORD. You are responsible for everything that happens with your credentials. Do not give your password out. If you need an account that many people can access, talk to someone in SFMRC IT.
4. Unlike the AHS and U of C we will not expire your passwords. But if you reuse passwords and one of your passwords is compromised you must change all your passwords here as well.

Mailing Lists (Slack)

There is a CAIR Slack group named cair-mri.slack.com. This is used to send messages about docs, journal papers, questions, and also random CAIR messaging. In order not to miss these messages, it is recommended to check Slack at least once per day, or have desktop app version running in the background. To join/unjoin make a request to Glenda. If you need technical help with Slack or would like to setup a new channel, speak to Perry.
Similarly, there is a Slack group named ach3t.slack.com managed by Perry. This is open to all Level 1 and 2 MR trained people, and is used to provide information and discuss current issues with the research 3T. It is highly recommended that it is checked weekly by users of the 3T.

Email Desktop Clients

If you require either U of Calgary or AHS email, you must request from their respective IT departments. If you would like to use a desktop client (e.g. Mail or Outlook) instead of webmail, be aware that

1. University of Calgary mail serves mail with the Exchange /Office 365 account. Using your U of C authentication you should be able to select automatic configuration during account setup with the client.

2. AHS has a security policy that does NOT permit any desktop clients.

Calendars

CAIR uses several different Google calendars to notify of events, schedule rooms, laptops and even the research Paediatric 3T MRI. Please ask Glenda (glenda.maru@albertahealthservices.ca) to add you to the appropriate calendars and explain their usage.

Auditing

Be aware that your actions on the network will likely be monitored. Many of our own systems also have auditing capabilities. This stresses the importance of not sharing your credentials with others.

Compliance to some standards does require all accounts have a form of authentication and be assigned to a single person (or it is difficult to enforce accountability).

Some of our agreements may also allow outside organizations (vendors, Health Canada, etc.) to audit or inspect aspects of our infrastructure and process.

SFMRC IT will review our data collection processes periodically to ensure we are following the conditions of our research agreements. The U of C and AHS have formal policies for Monitoring and Auditing of IT Resources:

http://www.ucalgary.ca/policies/files/policies/Information%20Asset%20Security%20Monitoring%20Policy.pdf

http://insite.albertahealthservices.ca/Files/cpd-pol-approved-monitoring-auditing-it-resources.pdf

Whether AHS or the U of C employs you, government legislation does allow an employer to access your email.

VPN

If you wish to access your computer at the SFMRC or ACH from home (or any remote location) your **only** option is to get an AHS account, AHS keyfob/token generator, and use the AHS VPN. AHS policy blocks the port to remotely access Mac's. The SFRMC IT group can help you configure remote access to run on a port that AHS does allow.

If your computer is at a University location (eg. the HBA lab or on the U of C side of the Foothills) you can use the U of C VPN solution to access it remotely. You would need to download the Forticlient software and install it:

http://www.ucalgary.ca/it/services/virtual-private-network

Note that any issues you have setting up or configuring the VPN would have to be directed to the UCIT Support Desk.

Purchasing

Hardware Requests

The SFRMC IT group does not usually have equipment available to freely give away. Each Principal Investigator (PI) has equipment that the SFRMC IT group manages and configures through Support Requests.

SFMRC IT can give advice and suggestions on technology purchases and obtain quotes.

All purchases will require a department code to charge to and appropriate approvals.

Software Requests

The U of C provides a website for software distribution:

https://iac01.ucalgary.ca/SDSWeb/

The software packages listed are generally provided without purchasing paperwork, although requests typically require your department code (if you don't know yours please ask your supervisor/manager).

Other software can be purchased through the Microstore or direct from vendors. This will require following the U of C purchasing process. The SFMRC IT staff can assist.

Printing

Printers Available

On level 4 there are two printers as visible under System Preferences / Printers & Scanners:
ACHBEHRSH03 – Black & White, Lexmark MX610, should be your **DEFAULT**.
ACHBERHRSH01 – Color, Lexmark C736. Try to use sparingly.

If setting up for the first time, be sure **not** to select "Airprint" for the "Use" protocol option. Instead you should select the printer model name.

Printer Requests

Requests for printer consumables, such as paper and ink, should be sent as a Support Request to the SFRMC IT group. You are encouraged to give SFRMC IT advanced warning if you see levels are low.

If there is an issue with a printer itself (continually jams or has an error message) a ticket can be submitted directly to AHS IT. Alternatively the SFMRC IT group can be informed who in turn will make a ticket with AHS IT.

Tools

OsiriX / Horos

The latest OsiriX is version 9.0 (at the time of writing). But you should be using the same version as the person who is managing your study/database. For most, this is version 5.9, but you can ask your database administrator if you're not sure.

NOTE: Some versions of OsiriX have incompatible database formats. If you open a database with a new version and the database is updated, ALL readers will have to upgrade their version.

To see your version, go to the OsiriX menu item and pick "About OsiriX". The version is at the bottom right of the dialog. If your version says 32 bit and/or your OsiriX is running an older version than your database admin then please drop myself or Victor (or Perry if you're at the ACH) a note asking if it's possible to upgrade.

At CAIR many of us use Horos to provide the DICOM connectivity and basic tools, and it resembles OsiriX closely in most respects except that it requires no license.

DICOM connectivity to Research PACS for a new computer must be arranged with SFMRC IT.

FSL

FSL is a comprehensive library of analysis tools for FMRI, MRI and DTI brain imaging data developed in Oxford.

FSL can be installed from:

http://fsl.fmrib.ox.ac.uk/fsl/fslwiki/

Bash shell users (which is the standard shell) need to add or create a file in their home folder (cd ~) named .bash_profile that contains:

```
FSLDIR=/usr/local/fsl
. ${FSLDIR}/etc/fslconf/fsl.sh
PATH=${FSLDIR}/bin:${PATH}
export FSLDIR PATH
```

The .bash_profile script should have rwx permissions for the owner, and no permisions for groups and everyone (chmod 700 .bash_profile).

FreeSurfer

FreeSurfer is an open source software suite for processing and analyzing (human) brain MRI images.

http://freesurfer.net

To run it you'll also have to install XQuartz, an X11 implementation for OS X. Instructions for both installations can be found here:

http://freesurfer.net/fswiki/MacOsInstall

Bash shell users (which is the standard shell) need to add or create a file in their home folder (cd ~) named .bash_profile that contains:

```
export FREESURFER_HOME=/Applications/freesurfer
source $FREESURFER_HOME/SetUpFreeSurfer.sh
```

The .bash_profile script should have rwx permissions for the owner, and no permisions for groups and everyone (chmod 700 .bash_profile).

Quantomo

Quantomo was developed in-house and is used for volume measurements. It is not officially maintained or supported.

AnToNIa

Is a Linux based program written by Dr. Nils Folkert. It requires version 3 of a graphics library called libqt, which must be compiled separately on newer Linux versions. See Dr. Folkert for support.

Analysis Servers

Grassi

Grassi is a processing server (Linux) managed by Marc Lebel for processing pipelines that require considerable compute (e.g. FSL, FreeSurfer).
Request login information from Marc Lebel Marc.Lebel@ge.com after approval from your supervisor.

Stanley

Stanley is a Linux computer used to store and process spectroscopy files using LC Model.

a) Usually there is an automatic backup of raw (P-files) from the scanner (This can be sequence dependent and attention network interruption can cause data to be dropped, always verify that your files have been properly transferred as the scanner will overwrite the data)
b) process your data and organize your data carefully.

Request access from Frank MacMaster or Rose Swansburg.

High Performance Computing (super-computers)

If your project required a lot of image processing, you could see with your supervisor to get access to Helix or WestGrid (all are super computers).

Helix: http://hpc.ucalgary.ca/quickstart/helix
Westgrid: https://www.westgrid.ca