CAH Technology Policy Abstract

The College of Arts and Humanities uses a wide array of technological resources to uphold the vision and mission of the college and university. The guidelines presented here are intended to facilitate the use of technology resources while promoting consistency and compliance with college and university regulations. CAH Technology policy addresses conditions related to resources, services, and personnel expertise available for use by CAH faculty and staff. Please read this policy carefully. Particular attention should be paid to the following points:

- The college adheres to all university policies
  - http://www.itr.ucf.edu/policies/policies.asp
- In order to receive the fullest CAH Technology support possible, college units and users must comply with the policy outlined herein. Users requesting administrator rights changes the security, responsibility, and support scopes
- Preservation and maintenance of CAH Technology policy requires the cooperation and effort of CAH Technology staff, college units, and individual users
- CAH support is limited for some hardware and software. See full CAH policy for list
- CAH support is only available on hardware and software that has an administrator account used solely by the Technology Office
- All operating systems and software must have licenses purchased by the appropriate college unit when applicable
- Students' personal identifiable information (Employee/Student ID, ISO number, grades/GPA, See FERPA for complete list) must not be e-mailed or stored on portable hardware. Social Security numbers should not be used at any time
- Personal files on university hardware will not be recovered, restored, or backed up by Technology Support

CAH Technology Office Contacts

- Technology Support: cahtech@ucf.edu or 407-823-2719
  - Supervisor: John Lazar, lazar@ucf.edu or 407-823-0993
- Network and Server Support:
  - Client/Server Analyst: Darryl Tucker, Darryl.Tucker@ucf.edu or 407-823-2478 or cahserver@mail.cah.ucf.edu
- Web, Programming and Communication: cahweb@ucf.edu or 407-823-3450
  - Web Designer: Matthew Dunn, Matthew.Dunn@ucf.edu or 407-823-3450
  - Web Applications Developer Assistant: Michael Powell, Michael.Powell@ucf.edu or 407-823-3450
- Management
  - Assistant Dean: Rudy McDaniel, Ph.D., rudy@ucf.edu or 407-823-3448
  - Manager: Bryce Jackson, Bryce.Jackson@ucf.edu or 407-823-3450

CAH Technology Policy

Rationale for Policy

The College of Arts and Humanities requires considerable technology resources, expertise, and services in order to provide professional support, equipment, communication, and information to staff, faculty, and students. This policy sets standards that are meant to ensure that the college can provide this professional support within realistic, logistical, and fiscal constraints. This policy intends to facilitate and promote consistency of equipment, procedures, and information. The CAH Technology Office is funded by the college to be a technology advocate for the college and to act as a technology liaison within the university; CAH Technology will implement and promote university and college policies.

Terms of Use

The college adheres to all policies in effect by the university, which are designed to comply with federal, state, and local regulations. These policies (see http://www.itr.ucf.edu/policies/policies.asp) relate to computing, networking, and Web sites. The college must ensure these policies and procedures are adhered to by staff, faculty, and students.

Any use of university- or college-funded computing equipment or services must be in accord with university and college policy. Failure to adhere to university and college policies may lead to limited or revoked support from the CAH Technology Office and may result in federal, state, or local prosecution, and/or additional costs. Any user may request administrator privileges; however, the user is fully responsible for complying with university policy and having administrator privileges diminishes the CAH Technology Office's ability to support the user. See Software Support and Requesting Administrator Privileges.

Computing equipment or services purchased through grants and special projects do not immediately fall within the terms of use for college support. In order for support to be given, the grant's principal investigator or project-lead must consult with CAH Technology and include support costs as part of the project.

Definitions

- *CAH Active Directory Account ,CAH Account, User Account* – a membership that securely stores contact information, privileges, user name and password, organizational hierarchy, and other information in a centralized database. An account is needed to access network resources such as printers, file shares, and other directory services. Accounts may not be shared by multiple people
- *CAH Active Directory Domain, CAH Domain* – the group of workstations, servers, and other networked resources that are logically connected under one name and share a centralized directory database. The domain name is "cah.ucf.edu." All hosts or networked resources contain a domain name with "cah.ucf.edu"
- *CAH Administrator Account* – a special account or group that has elevated privileges that allow access and control to hardware and software configuration as well as file permissions; an administrator account is required on all hardware receiving support. See Hardware Support
- *College Units* – any official department, program, office, institute, laboratory, or center under the College of Arts and Humanities. Official college units are designated by an E&G budget unit (for example, 23012001). See Supported Units and Areas Appendix

- *Computing Consumables* – recurring-use items included but not limited to toner or ink cartridges, paper, transparencies, batteries, pressurized air cans, DVDs, CDs or other disposable items that are not considered hardware
- *DDC* – Dean, director, or chair including associate and assistant deans, directors and chairs
- *Domain Name* – a domain name is a series of characters that provides a label for a given network resource other than the actual IP address. Each domain name provides a direct link to the address of a particular resource (for example, sirius.cah.ucf.edu)
- *Hardware* – computing equipment including but not limited to workstations, monitors, keyboards, mice, uninterruptible power supplies, hard drives (external or internal), disc drives(external or internal), USB Flash drives, speakers, servers, network switches, network cables, USB cables, FireWire cables, mobile phones, copiers, scanners and many other devices and components. See Hardware Support
- *Image* – a pre-packaged configuration (stored on media) for hardware including operating system, updates, and standard supported software that allows for efficient setup of new hardware or resetting of old hardware
- *IP Address* – an internet protocol address is a numerical identification that is assigned to some network resources such as workstations, servers, copiers and printers
- *IT Liaison* – individual selected by the chair/director of the individual's respective college unit, or other permissible project to serve as the primary point of contact for CAH technology related issues. IT Liaisons must be a full-time faculty or staff member
- *Lab Manager* – individual selected by the chair/director of the individual's respective college unit to oversee a computer lab or select group of workstations. Lab Manager must be a full-time faculty or staff member
- *Network* – the system of communication between hardware using cabling, Wi-Fi, and IP addresses. The university has internal (Intranet) and external (Internet) components to its network; many server services and workstations depend on its functionality, efficiency and security
- *Server* – a computer running 24-hour services such as Web site hosting, file shares, approved research activities, Active Directory Account login authentication, and other related services
- *Software* – programs, applications and operating systems that can be run with various hardware, which also may require purchased licenses. See Software Support
- *Support* – generally considered troubleshooting, configuring, designing, programming, securing, setting up software and/or hardware to properly function; support does not include instruction on specific features or functions of software or performing tasks that are the responsibility of the end user
- *End-User, User* – a person who is or will be operating or performing tasks with software on a workstation or networked resource. Each user must have an Active Directory Account to login into a workstation or server
- *UCF e-mail address* – an e-mail address within the "ucf.edu" (Exchange or Knightsmail)
- *Workstation* –a laptop or desktop computer, with one operating system installed, used for day-to-day operations by a user to perform job-related duties; a laptop or desktop computer running two operating systems would be considered two workstations

Requesting Administrator Privileges

Any individual can request administrator privileges. Requesting administrator privileges should be employed for extenuating circumstances when an individual needs computing autonomy within university constraints. Any individual with administrator privileges agrees to take full responsibility for all the assigned workstations and the CAH Technology Office agrees to provide continued support when possible. The individual is responsible for complying with any university technology policy.

Prior to requesting administrator privileges, an individual should confer with a CAH Technology Office staff member, the individual's DDC, and the CAH Dean's Office designee to identify and discuss the individual's needs. Requests are not automatically approved.

Any individual requesting administrator privileges must have the approval of the individual's DDC and CAH Dean's Office designee. An agreement must be established and the procedures must be followed on the Request for Administrator Rights Form (see http://technology.cah.ucf.edu/ for Request for Administrator Rights Form). By agreeing, the DDC shall identify and assign the individual a workstation or workstations, which the individual's user account will have local administrator rights applied.

Assigned workstations must retain a CAH Administrator account.

Violation of policy may result in mandatory revoking of the involved individual's administrator privileges. Violation incidents require the individual, the DDC, a Dean's office representative, a CAH Technology Office representative, and possible university representatives to review the details of the incident and determine the course of action.

The CAH Technology Office shall maintain the Request for Administrator Rights Form and the CAH Dean's Office shall retain the record copy.

Responsible Parties

Technology Office

The CAH Technology Office will implement and promote university and college policies as effectively as possible. The office shall create and maintain guidelines, policies, practices and procedures to facilitate compliance with all policies for all users and college hardware. The Technology Office shall continuously review all Technology Office policies and publish amendments on a quarterly basis starting the first of the fiscal year. The Technology Office will notify college units of any changes to college technology services in the case of severe weather conditions (see http://technology.cah.ucf.edu/). The office consists of four teams: technology support; network and server support; Web, programming and communication; and research. These teams have specific responsibilities and duties. See CAH Technology Office Staff.

Technology Support

Technology Support shall support college-appropriated hardware and software related to workstations and end-user systems including most network troubleshooting (only up to a wall jack) and provide cost-effective hardware and software solutions to college units. Technology Support shall provide setup services and file migration services for users and hardware.

Network and Server Support

Network and Server Support shall manage server maintenance and configuration, network planning and maintenance, security practices, account and security group administration and security monitoring as well as act as security liaison for the college within the university.

Web, Programming and Communication

Web and communication shall manage websites, Web-based software, secure programming practices, Web server maintenance and configuration, publications and communication practices, and database programming and administration. The Web policy details further responsibilities (http://www.cah.ucf.edu/files/Web_policy.pdf).

Research

Research shall manage consultations with faculty and staff for potential and ongoing projects or grants, creating customized software or configurations and conducting college-level research in regards to technology implementation. The team shall provide initial consultations with the potential project principal investigator. Any further support must be included in the project budget and participating technology staff will be credited as a Co-PI when warranted.

College Units

IT Liaison

Every official college unit and official college affiliated website must have an IT Liaison. Department chairs and directors shall oversee the IT Liaison. The IT Liaison will work in conjunction with the CAH Technology Office and will serve as the primary point of contact for all technology related issues and requests within the unit or website.

The IT liaison must work in conjunction with Technology Support to surplus hardware. The liaison must also maintain and request accounts and account access levels as well as notify the CAH Technology Office when a user is no longer employed or a new user is hired. IT liaisons must report issues with multi-user hardware. IT liaisons have additional responsibilities identified in the CAH Web policy. The IT liaison must maintain communication with the liaison's DDC regarding CAH Technology procedures, policies and practices (see http://technology.cah.ucf.edu/).

Lab Manager

Every supported lab within the college must have a designated Lab Manager. In order for a lab to be supported by the CAH Technology Office, specific criteria and conditions must be formally agreed upon by the college unit that supports the lab and the CAH Technology Office (see Supported Units and Areas Appendix for current list of supported areas). The Lab Manager will have a special account with elevated privileges to perform managerial duties within the lab. Any configuration changes to lab workstations from either the lab manager or the Technology Support team must communicated between the lab manager and the Technology Support team. The Lab Manager will work in conjunction with Technology Support team to ensure that computers adhere to university and college policies. The Lab Manager may be responsible for security updates as well as non-standard or additional software installations and configurations for the specific needs of the lab (see Supported Software Appendix).

Accounts and Access

Any account requests for access or deprovisioning of access must be completed at the college unit level except when otherwise noted. Account requests include CAH Active Directory, CAH Manager, UCF e-mail, PeopleSoft, PARIS, RDS, ARGIS, or other university or college account systems.

Software Licenses

The college unit must maintain all software license records for software it purchases. See Software Support and Supported Software Appendix.

Purchases

The college unit must purchase all hardware, software, software licenses, computing consumables and un-supported services except where otherwise noted. Technology Support must be consulted prior to any hardware purchase to ensure that the support can be given to the equipment; hardware acquired through surplus is treated as a new purchase (see Hardware Support). Technology Support must be consulted before software purchasing as well to determine license availability, existing license agreements, and other options that may reduce costs (see Software Support). Technology Support must receive all new hardware to setup prior to use to ensure proper licensing. CAH Technology recommends hardware and software listed on the Supported Hardware Appendix and Supported Software Appendix.

Users

Users are responsible for the basic care and condition of the hardware assigned to them including maintaining general cleanliness, monitoring and replacing toner/ink, paper levels, or monitoring battery levels (where applicable). Users must keep the immediate area of the hardware clear for easy access and airflow. In the case of severe weather conditions, CAH Technology recommends users to follow the procedures for securing hardware (see http://technology.cah.ucf.edu/). Users are responsible for ensuring the overall security of hardware and use of software and behaving in a manner consistent with all university and college policies; this includes not sharing account passwords with anyone. Users must also use assigned hardware and software for job-related responsibilities with incidental personal use (see Incidental Personal Use).

Users are encouraged to be present for all hardware and software support. Users must indicate who should be present during a work order and request that individual's presence. A chair, director, or IT liaison may be present or provide permission to perform a work order in the user's absence. Users can report hardware or software issues to the user's IT Liaison or directly to Technology Support. Issues with multi-user hardware must be reported to the user's IT liaison.

FERPA regulations regarding students' rights must not be violated (http://www.registrar.ucf.edu/ferpa/staff/welcome/). Users should also be aware of CAH Technology procedures, policies and practices (see http://technology.cah.ucf.edu/). See UCF's Use of Information Technologies and Resources Policy (http://policies.ucf.edu/documents/4-002UseofInformationTechnologiesandResourcesFINAL.pdf) for additional responsibilities. See UCF's Retention Requirements for Electronic Mail Policy (http://policies.ucf.edu/documents/4-001RetentionRequirementsforElectronicMailFINAL2007.pdf) for additional e-mail retention responsibilities.

Use of Hardware and Software

Users are generally free to utilize hardware and software to perform their job responsibilities. See UCF's Use of Information Technologies and Resources Policy (http://policies.ucf.edu/documents/4-002UseofInformationTechnologiesandResourcesFINAL.pdf) for additional policy on use and misuse.

Use of some hardware requires additional restrictions and precautions on Active Directory Accounts. See Portable Hardware Support and UCF's Security of Mobile Computing, Data Storage, and Communication Devices Policy (http://policies.ucf.edu/documents/4-007SecurityofMobileDevicesFINAL.pdf). Users should not register software including operating systems with personal information or accounts unless approved by the Technology Office.

Incidental Personal Use

Users are generally free to utilize hardware and software for incidental personal use. This use may include storing documents, photographs, music, or movies, however, it must comply with the Use of Information and Technologies and Resources Policy regarding copyright. The use of personally-owned external storage hardware is recommended for personal information and files. Technology Support will not be recover, restore, transfer, or back up files determined to be personal on university hardware. Excessive use of university hardware for personal storage that results in hardware or software malfunction or significant performance degradation is not considered incidental personal use. Procedures and guidelines, including limitations, for personal use of hardware for storage will be maintained by Technology Support. See Terms of Use.

Support

Primary support is offered to faculty and staff users and the university-owned hardware and software required for their job responsibilities. Support is not available for privately owned hardware and software. Support is limited to two workstations per user. Support is also offered to designated classrooms and laboratories (see Supported Units and Areas Appendix). Support is also given through providing procedures and forms for some of the actions and steps outlined within university and college policies.

Hardware and software that does not appear on the Supported Hardware Appendix or Supported Software Appendix may not be capable of support and may incur additional costs for support to the college units. Hardware that does not have a required CAH asset tag assigned will not be supported until the tag is present. Hardware and software purchased or acquired from surplus prior to the effective policy date will receive support, but this support may be limited.

In order to receive support, the hardware and software must also be configured with certain security and naming standards. These configurations include:

- One Administrator account used solely by the Technology Office
- Computer domain name/name
- IP address

A user must correct alterations to the above configuration before hardware or software support can be offered. Violation of policy may result in mandatory revoking of the involved individual's administrator privileges. The hardware must also be located on university property, recognized university space, or be brought to Technology Support unless CAH remote support is available. CAH Web policy explains Web support (see http://www.cah.ucf.edu/files/Web_policy.pdf).

No support is given for moving furniture, providing instruction on software use, registering wireless network devices, retrieving hardware from vehicles, or providing services requiring UCF Facilities Improvements such as installing additional network jacks. Backup services are not offered on classroom, laboratories, and some servers.

Support requests via e-mail, phone, and online work order system are the preferred methods for all hardware and software issues, scheduling moves or presentation setups. Support request response times will reflect the severity of the issue and the current workload. The immediate needs of the college and the severity of the issue dictate the priority of support.

Classroom Support

Designated general assignment and college unit classrooms are supported by the Technology Support team (see Supported Units and Areas Appendix). The CAH Technology Office will retain administrator rights to the computers, and provide users with a general account and password that can be used by anyone in the university. Hardware and software issues can be reported by anyone, and the Technology Support team will determine if other university offices need to be involved.

Lab Support

The CAH Technology Office will retain administrator rights to the computers in the lab and will perform initial setup and configuration. All workstations must conform to the general support policy. Hardware and software issues must be reported by the lab manager or faculty teaching in the lab.

Hardware Support

Hardware support includes but is not limited to installations and troubleshooting. Support may be limited for hardware that is no longer under warranty. Technology Support will verify functionality and/or network connectivity. The college unit must purchase replacement hardware. Technology Support will identify the replacement hardware needed. Hardware support installations include but are not limited to the following: memory, hard drive, mice, keyboards, monitors, video cards, speakers and other supported hardware.
See Supported Hardware Appendix.

Multiple-user hardware issues must be reported by IT liaisons. No support is given to local (non-networked) printers that are concurrently shared between multiple workstations or laptops.

Portable Hardware Support

CAH Technology Support must configure supported laptops. There is no support offered for any portable devices other than laptops. Technology Support will verify the functionality of non-laptop portable hardware that is still under warranty; the IT Liaison may work in conjunction with Technology Support to acquire a replacement.
See Portable Hardware Security.

Software Support

Software support is limited to ensuring the software functions without configuration or permission errors; this does not include instruction on how to use software.

Licenses are required for operating systems and software. Software and operating systems will not be installed without verification of required licenses. The college does not purchase software that requires licenses unless noted on the Supported Software Appendix. The college units are responsible for purchasing and maintaining proof of licenses.

Software support includes but is not limited to the following: operating system failures and errors, software failing to run/open, fatal error messages, password resets, software installations and updates, configurations for functionality such as mapping network resources or correcting monitor resolutions, backup services and other issues. Software support does not include changing personal preferences such as background colors or themes.

Setup Services

New hardware or existing hardware that is being re-assigned will be installed with the newest CAH hardware/software image containing up-to-date versions of the standard software (see Supported Software Appendix) before the hardware is set up for the user in the user's work area. Additional non-standard software requests that qualify under software support can be made at any time. Setup includes installing and configuring the

latest supported e-mail client including an archive location on the hardware. Setup includes file migration services from a user's previous hardware, if applicable and possible.

Updates

Security, critical, and/or service pack operating system updates will be applied to all hardware with supported operating systems on it. Security and critical updates for supported software will also be applied. The Network and Server Support team will verify that there are no adverse operating effects to operating system or software updates prior to installation. Supported software and operating system updates shall be transferred and installed automatically to workstations through the network whenever possible. Some updates may require involvement of the Technology Support team, which may be initiated by the user or the Technology Support team.

Security

Security must be considered at all times to protect personal information from intrusion and unauthorized use. Use of Hardware and Software references UCF's Use of Information Technologies and Resources Policy (http://policies.ucf.edu/documents/4-002UseofInformationTechnologiesandResourcesFINAL.pdf) and UCF's Security of Mobile Computing, Data Storage, and Communication Devices policy (http://policies.ucf.edu/documents/4-007SecurityofMobileDevicesFINAL.pdf), which all contain critical security criteria that must be followed. CAH Technology recommends all users follow UCF's Information Security Office's Security Standards and Guidelines (https://publishing.ucf.edu/sites/itr/cst/Pages/ComputerSecurityStandards.aspx). The college has included additional criteria and emphases as follows.

Antivirus

The college will provided antivirus software and install the software on all supported hardware and software. The antivirus software will be uniform across all hardware and software whenever possible. See Supported Software Appendix.

Portable Hardware Security

Files containing personal identifiable information must not be stored on portable hardware. Personal identifiable information includes but is not limited to social security number, Employee/Student ID, ISO number, residency status, gender, religious preference, race/ethnicity, e-mail address, grades/GPA, student's class schedule, test scores, academic standing, and academic transcripts. It is critical that all users adhere to FERPA regulations (http://www.registrar.ucf.edu/ferpa/staff/welcome/). The university's Security of Mobile Computing, Data Storage, and Communication Devices policy outlines additional responsibilities (see http://policies.ucf.edu/documents/4-007SecurityofMobileDevicesFINAL.pdf)

Account Security

Users must have unique accounts that are not shared by other users. Passwords must be set for every account. Account passwords may not be shared by anyone including the CAH Technology Office. Passwords must have a complexity; they must be at least eight characters in length and contain a letter number, and a symbol. Passwords will expire after 60 days and then must be changed. When a successful password is changed, one day must pass before being able to change the password again. An immediate previously used password cannot be the new password.

Accounts must be disabled immediately upon termination of employment. Accounts will expire and be disabled at the end of a user's contract date for users who are part-time employees, vendors, visiting, or otherwise considered temporary.

CAH Active Directory accounts will be based on a user's NID. A valid UCF e-mail address and contract end date, if applicable, is required.

Network and Server Support shall work with IT Liaisons to coordinate accounts and request information.

Security Groups

Security Groups are used to help define and control security access levels on user accounts. The implementation of groups allows for the greatest efficiency and usability of network resources and security considerations. User accounts may belong to multiple groups or none at all.

Security groups provide access to the college file shares. (see File Shares). While other security groups can be created, the four recommended security groups are:

- *Secure* –for chairs, directors and users assisting in evaluations, personnel records, grievances and other sensitive information
- *Staff* – for users working with administrative tasks such as budget, enrollment, course scheduling, and curriculum
- *Faculty* –for full-time users who do not need access to administrative or highly sensitive information
- *Departmental* – for users requiring only minimal access

The departmental security group for the unit will be given to a user unless otherwise requested by the IT Liaison or chair/director.

Network and Server Support shall work with IT Liaisons to coordinate security groups.

Network

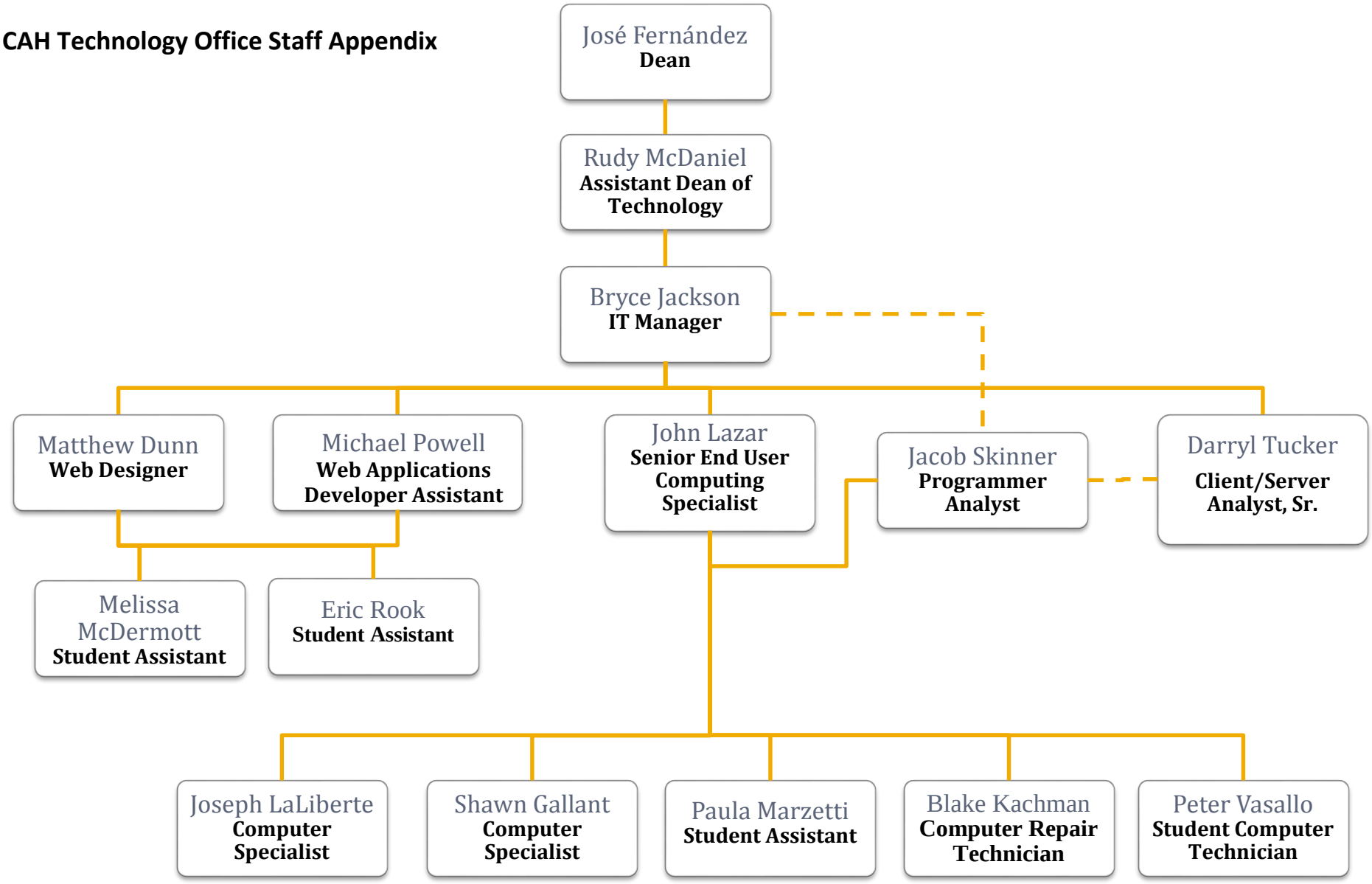
The network provides numerous services and resources. The CAH Technology Office works in conjunction with UCF's Computer Services and Telecommunications Division to ensure the efficiency, security, and reliability of all the aspects of the network. UCF's Use of Information Technologies and Resources Policy (http://policies.ucf.edu/documents/4-002UseofInformationTechnologiesandResourcesFINAL.pdf) and UCF's Server Standards (https://publishing.ucf.edu/sites/itr/cst/Pages/UcfServerStandards.aspx) contain additional information regarding policies put into effect by the CAH Technology Office. Users must be familiar with these official security policies. The college has included additional criteria and emphases on certain university policies.

Technology Support and Network and Server Support will provide support for network issues and services. Network support is limited to general troubleshooting, diagnosing, and configuring of hardware as well as ensuring physical connections to the network jack in a wall. Any network connectivity issues arising beyond a wall jack are the responsibility of UCF Computer Services and Telecommunications. Network connectivity issues must be reported to Technology Support and/or Network and Server Support. The teams shall report the issues to the appropriate university offices.

File Shares

Network file storage will be available to all college units. User accounts, security groups and the college unit will restrict and grant access to the various file shares. File shares will be allocated 50GB for operational and administrative needs. File shares shall be established in cases where multiple users must access the same files from different physical locations. Network and Server Support will back up file shares weekly and keep them for a minimum of 30 days. In the event of hardware failure related to the file shares, files shall be restored from the latest working backup, which may be up to a week old. All supported file shares must be located and administered on CAH Technology servers and hardware. File shares shall be made easily accessible to users through mapping or startup preferences.

CAH Technology Office Staff Appendix



Supported Software Appendix

Standard

Standard software is automatically included with new or re-assigned workstations. Some software may be part of a license agreement with the college or university. The latest versions of the software will be installed (unless known issues exist).

- Adobe: Acrobat Professional[3], Flash Player, Shockwave
- Microsoft: Internet Explorer, Office[1], Media Player
- Apple QuickTime
- MPEG2 (DVD) and other video codecs
- Mozilla Firefox
- Symantec Antivirus or Microsoft Security Essentials[3]
- Sun Microsystems Java
- Roxio CD Burning (Dell - Windows Only)

Additional

Additional software must be requested and may require purchasing a license.

- Adobe Products[2] except Acrobat Reader, Acrobat Professional, Flash Player, Shockwave
- Vectorworks Products[2]
- SyncRO Oxygen[3]
- Object Warehouse RBrowser[2]
- Microsoft: Visioabove[2], Project[2]
- Bare Bones TextWrangler

Operating Systems

Workstations

- Microsoft: Windows XP Professional[1] or Windows 7 Professional[1]
- Apple OSX[2]

Servers

- Microsoft: Windows Server 2008 R2[1]
- Ubuntu Linux 64-bit
- Red Hat Linux

[1] Collgewide license purchased and provided through Campus License Agreement
[2] Requires a purchased license
[3] Collegewide license purchased and provided

Supported Hardware Appendix

Workstations

Desktop

- Dell OptiPlex: 330, 380, 390, 745, 755, 760, 780, 790, 990, 9010, 9020
- Apple: iMac, Mac Pro, Mac mini (Intel based Macs only)

Laptop

- Dell Latitude: E series, 13
- Apple: Macbook Pro, Macbook (Intel based Macs only)

Servers

- Dell PowerEdge: R210, R410, R420, R610, R620, R710, R720

Supported Units and Areas Appendix

All CAH units are supported except WUCF, which has opted to not receive support from technology support team.

Current Rooms

Colbourn Hall

- CNH202 (T&T Laboratory)
- CNH204[4]
- CNH401
- CNH203 (Technical Writing Laboratory)
- CNH207E[4]
- CNH126

Visual Arts Building

- VAB104
- VAB107[4]
- VAB108 (Graphic Design Laboratory)
- VAB109[4]
- VAB111[4]
- VAB113[4]
- VAB146
- VAB213B (Graphic Design Laboratory)
- VAB217[4]
- VAB221 (MLL Laboratory)

Nicholson School of Communication Building

- NSC108[4]
- NSC110[4]
- NSC111[4]
- NSC112[4]
- NSC114[4]
- NSC116[4]
- NSC117[4]
- NSC147[4]

Performing Arts Center

- PACM116
- PACM132
- PACM143
- PACM144
- PACM260
- PACM261
- PACT107
- PACT110
- PACT115
- PACT204 (Vectorworks/CADD Laboratory)
- PACT244 (Lighting Laboratory)
- PACM263

Center for Emerging Media

- CEM105 (SVAD M.F.A. Laboratory)
- CEM203 (CREATE Laboratory)
- CEM305 (SVAD Laboratory)
- CEM306 (SVAD Junior Laboratory)
- CEM307 (SVAD Senior Laboratory)

OTC

- OTC106 (HCI Laboratory)
- OTC107 (A/V Laboratory)
- OTC111 (SVAD Laboratory)
- OTC134 (SVAD Laboratory)

Classroom I

- CL1220[4]

[4] General Assignment Classrooms (OIR supports project bulb replacements at no cost)