Introducing the New Campus Partnerships Program

We are fortunate to have the final member of the IT Services leadership team join us this month. In another article of this newsletter, you will find information about Robert Howard, the new Senior Director for Support Services and Campus Partnerships. One of Robert’s charges will be to establish a new Campus Partnership program at Miami. This will be a new service offering to provide end-user and departmental support for technology in a different way from the current Miami model. The scope of services will eventually include end user desktop support, server hosting and management, non-enterprise level application development and other services based on future demand. All services requested for the benefit of a single individual, department, school, college or similar unit will be channeled through the Campus Partnership program. This will facilitate the development of clearly understood service requirements and associated costs.

There are several types of organizations or individuals who will benefit from the Partnership program. One set of beneficiaries will be departments who want to acquire a fraction of a full time equivalent support person. Also, departments or schools who wish to add incremental support beyond their current technology staff positions may find this to be an attractive offering. Many units will find the partnership program to be a positive way to contract for specialized services that their existing technology support staff may consider outside of their core mission, yet still essential. Some units that are currently struggling with retaining and managing technical support staff may also be able to benefit from the program. All services provided by the Campus Partnership program will be provided based on a negotiated Service Level Agreement, or contract, between the Partnership program and the benefiting units. IT Services will be the first major unit to commit to the Partnerships program and will be placing its desktop support needs under service level agreement.

At Robert’s most recent appointment at the University of Georgia, several significant benefits accrued to the institution through the implementation of this Partnership program:

1. Departments, schools and colleges were able to acquire top quality technical support staff at a lower cost.
2. The university achieved a significant cost savings in its technology support budget.
3. Smaller units were able to acquire the same quality of support as larger units.
4. Depth of coverage and continuity of support was provided much more effectively, allowing units to have local staff take leave without being concerned about coverage, as well as have coverage when a staff person leaves employment.
5. IT support staff in departments, schools and colleges were able to concentrate more on core mission activities, leaving routine technical support to the Partnership program.
6. Distributed technical support staff saw a more robust individual career path develop, providing a clear path for career advancement without having to leave the university. Researchers were able to contract for partial FTE support of their proposed research projects, thereby allowing them to focus on core research and not technical aspects of the project.
7. Non-technical administrators were freed from the hassles of having to hire, supervise and evaluate specialized technical staff.
8. Technology support staff persons were more likely to find that their salaries were set on skill levels, and not based on the department for which they worked.

Between now and January, I shall be introducing Robert Howard to administrators, faculty and staff to allow him to explain more of the details of this program. If you are in the process of developing a technology support strategy for your unit, or are otherwise interested in an appointment to hear this explanation, please contact me at 529-8338 or chrisjr@muohio.edu.

J. Reid Christenberry
Vice President for Information Technology
306 Hoyt Hall
Miami University
Oxford, OH 45056
E-mail: vp-it@muohio.edu.
IT Strategic Planning Update: Current IT Initiatives Supporting “First in 2009” Goals

Several tactical projects were identified as a result of the university’s IT Strategic Planning Study completed in May 2004. The study involved all four Miami campuses and is meant to provide a plan of action for the next several years, in conjunction with ongoing reviews to determine emerging and changed needs. Listed below are some of the tactical projects and their status as they align with the First in 2009 goals.

Given that this is the first year of our strategic plan implementation, several of the projects involve studies that provide recommendations on support models and needs.

First in 2009 Goal 2: Strengthening the academic support for existing faculty

1. **Research Support Model Project.** This project will recommend a model for IT support of faculty research, both computational research as well as support for a broader range of research activities. Funding has been identified for staff resources; staff will be hired once the needs are fully identified. Faculty, staff and student focus groups are underway to determine campus needs.

2. **Classroom/Open Access Labs Project.** Seventy-one classrooms have been upgraded with new technology since Spring 2004, with approximately twenty-five planned to be upgraded this academic year. Under development is a strategy and implementation plan to provide technology-rich physical and virtual classrooms and open-access computing labs for teaching and learning that are consistent across the university while also reflecting the programmatic needs of the individual disciplines.

   Four focus groups have been formed to make recommendations to the project core team regarding faculty support, classroom technology levels, software management, and classrooms of the future. All recommendations are currently scheduled to be submitted to the core team by January 11, 2005.

3. **Blackboard Enhancement Project.** The project will result in a long-term plan for continuous improvements to Blackboard and an implementation plan to run all three components of Blackboard (learning system, content system and portal). A faculty online survey will be conducted soon. The new components (the content system and portal) are currently loaded on the IT Services Blackboard development server for investigation by interested faculty and Blackboard support staff.

4. **Client Advocacy Role in IT Services.** John Vaughn has been named IT Services’ Client Advocate. When an individual or department finds that normal channels of service or support are not satisfactorily resolving a situation, John serves as an “ombudsperson” to take the problem in hand. He can be reached at 529-1379 or vaughnjh@muohio.edu.

First in 2009 Goal 6: Enhancing campus facilities, buildings and systems

1. **On-campus Wireless Deployment.** In accordance with the IT Strategic Plan, the initial wireless deployment goal has been completed. Now, all residence and dining hall buildings within the Oxford campus can accommodate wireless network access. Over the next several months, this wireless deployment initiative will encompass the Hamilton, Middletown, and Luxembourg regional campuses, plus all academic and administrative buildings on the Oxford campus. It is anticipated that all wireless deployment activities will be completed during the early Fall 2005 semester.

2. **IT Policy, Planning and Governance.** The Hamilton Campus has formed a Core Team of students, faculty and staff to develop an IT Strategic Plan for the campus. Focus group sessions were held the week of November 8. The goal is to publish an IT Strategic Plan for the Hamilton Campus that is aligned with university goals, Hamilton Campus goals, and the university’s IT Strategic Plan.

   Another goal of the project is to develop a governance structure to advise the Vice President for Information Technology on initiatives, priorities, and policy. The initial effort is to form a team to recommend a Resource Portfolio Management process to replace the previous Resource Allocation Model. The Vice Presidents and Executive Directors of the regional campuses are forming a working team to develop the model.

3. **Technology Funding Model.** A proposal to recommend a student technology fee will be developed for presentation to the Board of Trustees at an upcoming meeting. The goal is to implement the technology funding model in FY06.
4. **Banner Lifecycle/Governance.** The goal of this project is to develop and implement a university-wide plan for the effective and efficient use of Banner, including immediate system enhancements, the evaluation of current Banner modifications, and the ongoing governance, service and support of all university-wide administrative systems. A project kick-off meeting and critical issues session was held November 5 with key clients to identify issues that need to be addressed in the project. Also, the group discussed what the scope and responsibilities would be for an on-going governance group. Several system enhancements were endorsed and will be worked on immediately; they are (1) Bannerweb for Employees, (2) Online purchase requisitioning, (3) Document imaging pilots in the Registrar’s office, University Advancement, Human Resources, and Payroll, and (4) implementation of the web browser-based access to Banner, rather than having a Banner client required on every desktop at Miami. Other efforts will involve working with client offices to help exploit unused and/or unimplemented modules of Banner and an examination of business practices to better adapt them to today’s business environment.

5. **Decision Support System Pilot Project.** The project team will develop a plan to create and manage responsive and secure systems that allow access to administrative information and facilitates informed university decisions. The Core Team has been investigating decision support models at other universities. Two critical issues sessions and the project kick-off meeting were held in mid October. The near-term deliverables for this project are to define the scope, deliverables, and a budget model for what a decision support system at Miami University would entail. If the core team feels enough definition has been done, and resources are available in the late Spring, a pilot project will be started.

6. **Network Access Management System.** This project is to provide a system to supervise network traffic and provide authentication and quarantine services to infected computers in residence halls. The collection of services to be delivered by this project has been branded “Network Protection Services”. The network infrastructure has been upgraded and new equipment needed to provide these services has been implemented. Additionally, the ability to identify computers demonstrating nefarious behavior and quarantine them has been implemented in the residence halls. The project team is currently focusing on developing solutions for network authentication and enforcement of a defined minimum standard (e.g., virus protection and windows updates) in order to obtain network access.

7. **Disaster Recovery Project.** The Information Technology Services Disaster Recovery Project is in the process of refining a draft scope document and finalizing project organization. A pre-project core team has met and committed to improving information technology disaster readiness for instructional, research and business services. This work is being done in concert with campus wide planning performed by the university’s Continuous Operations Planning group.

---

**New Senior Director of Support Services and Campus Partnerships**

The Office of the Vice President for Information Technology is pleased to announce that, effective November 1, 2004, Mr. Robert Howard has joined Miami’s staff as the Senior Director for Support Services and Campus Partnerships. He joins us from the University of Georgia, where he served as Director of Campus IT Partnerships. Robert was very successful in establishing a strong campus partnership program there. Over 6 years, his unit grew from a staff of two to a staff of over 50 supporting a wide variety of units and providing multiple services to that campus of 35,000 students and 2,200 faculty. Each unit supported was provided negotiated service level agreements specifying the specific deliverables and quality measures.

Robert holds a bachelor’s degree in Cell Biology and Microbiology with a minor in Biochemistry from the University of Georgia. He has served as a speaker on the role of insourcing as a solution to many problems associated with highly decentralized campuses at Educause national and regional conferences and has had the model recognized at the finalist level for several regional best practices competitions.

Robert’s focus areas will be implementing and integrating a successful campus partnership program at Miami within the existing support structures to enhance the quality of end user and departmental technology support, to reduce the total cost of ownership for planning, deploying, and supporting technology at Miami University, and to provide expanded career opportunities for IT staff.
Peer-to-Peer File Sharing Ban and Future Options

In Spring 2004, worms and viruses dramatically increased their use of the same ports that were used by Peer-to-Peer (P2P) file sharing applications. The activity of these worms produced enormous amounts of network traffic, putting the campus network at risk. Miami, and many other institutions, blocked these ports to eliminate network disruptions.

In late September, IT Services lifted a few of the bans to determine if the virus traffic on these ports had subsided. In the 30 days that the bans were partially lifted, two things became clear:

- the ports used for these applications are very active with both P2P traffic and virus traffic.
- copyright infringement groups are very active as well. Miami University received more than 350 copyright infringement notices in the 30 days that the ban was partially lifted. IT Services is in the process of notifying many students that they must remove copyrighted songs and movies from their computers or face possible legal action from the copyright owner. The amount of staff time that this activity is consuming is very large and the risk to Miami students is high.

Peer-to-Peer traffic is once again banned, as legal options for providing music are discussed and explored. A student survey has been posted on myMiami; student input on the value of digital music offerings is being sought to determine if the cost of such services is justified.

Updates to this issue will be posted on the Miami Knowledge Base.

Spam Scoring Enables “Filtering” of Junk E-mail

On Monday, November 8th, a spam scoring system was put into place on Miami’s incoming e-mail servers. End users will now have the option of configuring their desktop e-mail client (for example, Outlook or Eudora) to filter e-mail identified as spam so it is not delivered to their inbox.

What is Spam Scoring?

Each message is reviewed, using multiple tests, to determine if it is spam. Messages that appear to be spam receive a spam score that is placed in an “X-Spam-Score message header”. If the X-Spam Score is at one or above, a score along with asterisks will be present (see example below). If the X-Spam Score is below one then only the words “X-Scanned-By: MIMEDefang 2.42” will be present.

Example of an X Spam Score Header:

X-Sender: samplejq@po.muohio.edu
Date: Tue, 26 Oct 2004 09:20:31 -0400
To: samplejq@muohio.edu
From: John Sample samplejq@muohio.edu
Subject: Test Junk Mail message
X-Spam-Score: (****) 4.021
X-Scanned-By: MIMEDefang 2.45

Testing to date has shown that any e-mail flagged with a score of one or above is very likely to be spam. Please note that spam scores are assigned by the system and cannot be altered.

Will Spam e-mail be delivered to me?

Spam scoring is being implemented in “tag and pass” mode. This means that you will receive ALL messages addressed to you, regardless of spam score. You make the decision as to whether and how you wish to manage e-mail flagged as spam. This approach prevents the mishandling of messages incorrectly identified as spam and leaves the control of what happens to spam messages to you.
How do I use the Spam score to manage spam?

To manage spam messages, you will need to create a filter in your e-mail software based on the X-Spam-Score header. The filter can be configured to move messages to a different mailbox (strongly recommended) or to delete messages. For more information on how to set up a filter in your e-mail application, please refer to the Knowledge Base cases on creating Spam e-mail filters.

IT Services strongly recommends that you create a mailbox named "Spam30" and filter messages to that mailbox. We recommend you periodically check that mailbox to see if any messages have been misidentified as spam. **Please keep in mind that, if you have your e-mail application set up to use IMAP instead of POP, the messages filtered to the Spam30 mailbox will be deleted 30 days after their receipt.**

**myMiami e-mail note:** At the current time, the myMiami e-mail application cannot filter e-mail. Evaluation of myMiami e-mail add-ons will be undertaken, with the hope that a filtering feature can be incorporated in the future.

**Outlook Express note:** Outlook Express cannot filter messages based on a message header. Outlook Express end users should upgrade to the Outlook e-mail application provided as part of the Microsoft Office Suite.

### What is the difference between POP and IMAP?

**POP:** Post Office Protocol (POP) is the most common method of accessing e-mail for faculty and staff at Miami University. If your e-mail application is configured to use POP, messages sent to you are stored on Miami's e-mail server until you connect and retrieve them. When you check your e-mail, your messages are downloaded to your computer and removed from the mail server. If you are using Eudora, you can configure it to leave your messages on Miami's e-mail server after you retrieve them; IT Services recommends you leave message on Miami's e-mail servers for no more than 14 days. With POP, you will need to delete the Spam messages that have been downloaded to your computer manually, after they are filtered to the Spam Mailbox. IT Services recommends that clients who use Eudora as their email application use the POP protocol, as Eudora's handling of IMAP is not optimal at this time.

**IMAP:** If you have your e-mail application configured to use Internet Message Access Protocol (IMAP), your incoming e-mail remains on Miami’s e-mail server until you delete it. You can read and manage your e-mail from different locations. Your In, Out, Sent, and Trash mailboxes, plus any mailboxes you create, are visible to you no matter what computer you use to access your mail account. If you are filtering Spam e-mail, IT Services recommends that you create a mail folder for Spam e-mail named "Spam30". IT Services will delete any message over 30 days old from your Spam30 mail folder. This is a convenient way to further manage spam messages you may receive. IT Services does NOT recommend using IMAP with Eudora, as Eudora's handling of IMAP is not optimal at this time.

---

**Computer Remediation Center Helps with Virus/Spyware-infected Personal Computers**

Students, faculty or staff concerned that viruses have infected their personally-owned computer or that have Internet connection issues due to spyware can call the Support Desk at 513.529.7900 for a quick fix over the phone or a free appointment with the Computer Remediation Center. The Computer Remediation Center is a new extension of the Support Desk that repairs computers infected with viruses or debilitating "spyware."

The Computer Remediation Center was created over the summer of 2004 to respond to the increased number of virus and connectivity issues on the campus network. Computers are brought into the Computer Remediation Center after appointments are scheduled by the Support Desk. While in the shop, technicians install updated virus protection software, catch up with the newest Windows updates and use a myriad of tools to combat spyware - programs that track the user's Internet usage, display popup ads and often cause connectivity problems.
IT Services Print Center is proud to announce a new arrival – a three-ton Xerox iGen3 Digital Production Press

The iGen3 revolutionizes digital production printing. You won’t be able to tell the difference between a full color piece produced on the iGen3 and one printed on an offset press – except by the speed. Now even small quantities can be produced to the highest quality, at a price that will surprise you.

With 600x600 dpi imaging, an 8-bit depth resolution, and patented Xerox dry inks for excellent fine line rendering and accurate color matching, the iGen3 brings the Print Center’s digital printing capabilities firmly into the 21st century.

The iGen3 also expands the sizes and weights of paper that can be used in full-color printing. From as small as 7”x7” to 14”x20” the iGen3 handles paper from 16 lb. bond to 130 lb. cover. And now your choices for accurate reproduction of color images is not limited to smooth, white paper. The iGen3 can produce quality color images on a wide range of paper stocks, including textured papers.

Not only does the iGen3 handle full color printing, but it is also a high-quality black and white printer as well, utilizing 256 gray levels to ensure that even the finest detail reproduces as sharply and cleanly as possible. You can even combine color with black and white to produce custom booklets, programs, brochures, class packets and a variety of other materials.

Customize and personalize your printed pieces using Variable Information Printing. Using your database, the Print Center can place variable text, images and graphics in your materials. Variable information printing increases the response rates for any direct-mail communication, from recruitment to staying in contact with your department’s alumni.

The new Xerox iGen3 brings award-winning technology to your Print Center. Winner of the 2004 InterTech Technology Award as one of the most useful and significant technology advances in graphic communication, the 2004 Gold Ink award and the 2004 IAPHC International Gallery of Superb Printing, the iGen3 is wowing clients and printers around the world. Prepare to be wowed – here at Miami!

For more information about the iGen3 or any Print Center services, contact John Bowser, manager of print services at bowserjh@muohio.edu.
MU Wireless is Now Available in All Residence and Dining Halls

In mid-August, IT Services began rolling out MU Wireless into the dining and residence halls. As of early November, all of the residence halls (except MacCracken where the wiring for the access points is still being installed) are now active and using the service.

MU Wireless is the University’s next generation of wireless access service to connect to Miami’s network (MUnet). Wireless network access provides the advantage of mobility, especially to laptop users. The wired network, however, still provides speed and security advantages. The combination of both the wireless and wired service enhances the online experience.

Please note the following aspects of MU Wireless:

- MU Wireless currently allows only web traffic (http/https traffic). This means that any other services like Eudora, Instant Messaging, FTP, etc. will NOT be available.*
  
  **Note:** myMiami (http://mymiami.muohio.edu) is available for checking e-mail and using netDisk to access your UDS files.

- When you open your web browser, you will be directed to the MU Wireless login page. You will need to log in using your Miami UniqueID and MUnet password in order to receive network service.

- Wireless traffic is very easy to intercept. MU Wireless does not encrypt your wireless network communications. VPN functionality will soon be available to secure your MU Wireless traffic*. 

*Secure access using the Virtual Private Networking (VPN) client will allow you to use the full range of network services. We anticipate VPN will be available within the next few days. Please check for updates at the Miami Knowledge Base (http://kb.muohio.edu).

We want your feedback on your wireless experience in the residence and dining halls - please share your comments using our feedback form.

IT Services will be installing wireless service in academic and administrative areas that do not already have wireless coverage. MU Wireless in these buildings will begin its availability sometime in the spring semester; a schedule for this service in these buildings is being created and will be made available online upon completion. Existing wireless networks in academic and administrative buildings will be transitioning to MU Wireless service (from the current WAM service) later in the school year and into the summer.

New Network Protection Service offered and Network Protection Services Update

The first major component of the Network Protection Services project with visible effects to the university community, the “Quarantine Network”, was implemented in the residence halls in late October.

Computers infected with viruses, worms, or trojans present a threat to the network. If a computer demonstrates such an infection, it is now “quarantined” (unless it poses an extreme threat to the network).

When a computer is quarantined, it is restricted to a Quarantine Alert web site. Services such as e-mail, web browsing, or file sharing will not be accessible. If you are in the residence halls and are having trouble obtaining network service, you should open a web browser to see if the Quarantine Alert web page appears. If it does, your computer has been quarantined and the web page outlines what actions you should be take to fix the problem. In this initial phase, you will be asked to bring your computer to the Support Desk’s Computer Remediation Center to have it serviced by a technician. For the future, IT Services is working to provide instructions and tools for users to fix their own problems if they so choose. As they become available, these instructions and tools will be accessible from the Quarantine Alert web site.

In extreme cases where the network cannot afford to provide any service to the device, the data jack it is attached to will be disabled. In this case, the device will get no network service at all.
Network Protection Services Update

In a previous Tech Talk article, IT Services outlined the plans for the delivery of many services to provide safe (secure, vulnerability and virus-free) network access.

The following services have been recently deployed or are currently in development:

<table>
<thead>
<tr>
<th>Network Protection Service</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Develop an Intrusion Detection System.</strong></td>
<td><strong>Newly implemented</strong></td>
</tr>
<tr>
<td>Information from a variety of sources, including the IPAs described above, is gathered in a single location for identifying the computers that pose a threat to the network or to others connected to it.</td>
<td></td>
</tr>
<tr>
<td><strong>Establish a Quarantine Network.</strong></td>
<td><strong>Newly implemented</strong></td>
</tr>
<tr>
<td>ResNet computers that have been identified by our Intrusion Detection System as a threat are placed in a special network where a web page will provide instructions for obtaining assistance, and, ultimately, tools for users to self-remEDIATE their computers.</td>
<td></td>
</tr>
<tr>
<td><strong>Require Network Login.</strong></td>
<td><strong>In Development</strong></td>
</tr>
<tr>
<td>Users who wish to obtain network service will be required to sign in first. This process will be established first with the residence hall network before it is brought to the rest of campus.</td>
<td></td>
</tr>
<tr>
<td><strong>Require Computer Registration.</strong></td>
<td><strong>In Development</strong></td>
</tr>
<tr>
<td>Users will be required to register any devices – computers, gaming devices, hand-held computers -- they wish to use on the network.</td>
<td></td>
</tr>
<tr>
<td><strong>Enforce Minimum Standards for Access.</strong></td>
<td><strong>In Development</strong></td>
</tr>
<tr>
<td>Devices will be required to meet certain defined standards before access to the network is permitted. For example, a Windows computer may be required to have a set of patches installed and have up-to-date virus protection.</td>
<td></td>
</tr>
</tbody>
</table>

Next steps focus on clarifying network access privileges:

- The project team is currently conducting requirements analysis for the three closely related services identified as “in development”: Network Login, Computer Registration, and Minimum Standards Enforcement.
- The project team is working to establish the needs of the university community in regards to these three components. We hope that by identifying the needs of a very diverse user community (from the residence halls to special purpose research facilities) early on that we will be able to build on the network protection services in a beneficial fashion.

IT Services appreciates your patience as we continue to explore these new technologies designed to provide a safer network. Please contact the IT Services Support Desk with questions or concerns: supportdesk@muohio.edu.
Miami Information Environment (MInE) Upgrade

MInE, the Miami Information Environment, will be upgraded with a new software release over the weekend of January 15 – 17, 2005.

The new version sports new, more attractive colors, some new icons, and the replacement of tabbed pages with a pull-down menu. The main functions of MInE will remain intact, and MInE users still will navigate through folders and generate and view the reports that they use now. To simplify the MInE interface, report scheduling, which is used only by a small number of people, will be disabled by default; it can be enabled easily for those who need it.

Although the changes are small for MInE users, “under the hood” is an entirely new architecture that simplifies administration, improves control of access to reports and sensitive information, and allows tuning for better performance.

A preview system running the new version of MInE is available at https://webdev.admin.muohio.edu/Brio/browse/Main. We encourage all MInE users to take a look. In addition, IT Services will offer a brief instructor-led overview of the changes in the new version in early January. Faculty and staff who wish to attend should register in advance in TRAIN.

If you have questions about the new version of MInE, please contact Support Desk at 529-7900.

Virus Scanning of Universal Disk Space (UDS)

On November 2, IT Services performed a virus scan of Universal Disk Space (also known as netDisk, UDS, or the M Drive) to identify files containing viruses. Clients with infected files were sent an email explaining the problem and detailing the list of infected files found on his/her space. The email informed clients of the next steps to be taken with the files and how to obtain assistance.

On November 11, IT Services ran another scan to clean the infected files. Files that could not be cleaned were deleted. This scan took place after a backup of the servers was completed; the backup provides the ability to salvage any files that have been removed, in the unlikely case that a virus-infected file will be needed by its owner.

Each semester IT Services will repeat this process of scanning to identify virus infected files; notifying the individual; then conducting a second scan to clean or delete the infected files. Please note: IT Services does not read files on your Universal Disk Space, the scan simply matches the fingerprint of the file to that of known viruses.

For more information, please refer to the Knowledge Base case 87894 on “Virus Removal From Universal Disk Space”.

Results of the 11/2/04 UDS Virus Scan

The scan found 995 infected files in 179 user accounts.

Top viruses:

- W32/Nimda.eml: 372
- W97M/Melissa.a@MM: 170
- W32/SirCam@MM: 80
- W32/FunLove.gen: 57
- VBS/LoveLetter@MM: 37
- W32/Nimda.gen@MM: 31
- W32/Magistr.b@MM: 23
- W32/BleBla.b@MM: 21
- W97M/Marker.gen: 19
- W32/Netsky.j@MM: 19
- W32/Bagle.af@MM: 18
- W32/Bagle.z@MM: 17
- W32/Bagle.ai@MM: 13

What should I do if you find that I have a virus in my UDS space?

You do not need to do anything. If the file is one that you do not need or want, it will be cleaned or deleted for you as part of this periodic process. If the file is needed, please call the Support Desk at 513-529-7900 and we will assist you.
Electronic Accounts for Miami Retirees and Emeriti

Society of Miami Retirees (SOMR)

A new retirement society has been established for Miami Retirees to remain in close contact with the University and each other. Named the Society of Miami Retirees (SOMR), members will receive a number of services formerly discontinued at retirement.

IT Services will provide electronic accounts, including e-mail, dial-in service, inclusion in the electronic directory as a member of SOMR, and services offered by Network Services Enterprises which include off campus high speed access. In most instances, retiree accounts will be continued without interruption for those enrolling in the Society at the time of their retirement. Those who retired prior to the foundation of this Society, and whose accounts were deleted upon retirement, will have new accounts created for them upon receipt of a request for membership.

For additional information about the SOMR, contact Jan Ames in Advancement Services at 529-4635. The IT Services Support Desk at 529-7900 can provide information and assistance on electronic resources.

Society of Miami Emeriti (SOME)

The Society of Miami Emeriti (SOME) was founded in 1972. Retiring faculty are recommended by their college for inclusion in SOME. This recommendation must be approved by the Board of Trustees. Most University services are retained by the faculty member as a benefit of being inducted in the SOME.

IT Services provides continued electronic accounts to members and spouses of the Society of Miami Emeriti which include e-mail, dial-in service, inclusion in the electronic directory as a member of SOME, and services offered by Network Services Enterprises which include off campus high speed access.

Visit [http://www.miami.muohio.edu/University_Advancement/Emeriti/](http://www.miami.muohio.edu/University_Advancement/Emeriti/) or contact University Advancement at 529-5957 for more information. The IT Services Support Desk at 529-7900 can provide information and assistance on electronic resources.
Blackboard Tip for Instructors–Copying and Moving Course Content

Blackboard, in an effort to ease the integration of content into your site, has introduced the ability to copy/move content items. Now, with the implementation of the Blackboard Learning System version 6.1.5 at Miami, you can move a content item to a new location in your site, copy it to other locations within your site, or even move or copy it to any other site for which you hold the role of Instructor.

Note: Please make sure that you do not have pop-up blocking enabled, as the Course Map - required to choose the destination of copied/moved content - is a pop-up window.

To copy or move content:

1. Navigate to the Control Panel view of your content item.
2. Click the "Copy" button to the right of the content item, illustrated below.
3. Select the location where you wish to copy/move the item.
4. Click "Submit".

Note: If you wish to move the item, select "Yes" for Delete item after copy?.

Please direct any questions or issues with Blackboard to Advanced Learning Technologies at 529-6068.
Password Security

When it comes to managing your password, it should be treated like your toothbrush - don’t share it with anyone and change it periodically. Since we’re on a roll, another comparison would be that of the similarities between passwords and bubble-gum: They are always strongest when fresh, they shouldn’t be shared by a group and if left lying around, they result in a sticky mess.

As you may already know, Miami University’s password policy states that passwords should be changed frequently to enhance computer security, but should never be used longer than 180 days. Passwords should also be at least 6 characters in length and should not duplicate previous passwords to prevent password reuse.

Miami has done a lot towards weaving applications together such that you don’t have to re-login to each system each time you move. Nevertheless, there is still a big responsibility on the user to ensure that their password is properly protected.

Remembering passwords has always been a challenge for me, and I have seen several methods to help with this problem. The best among them is the “first letter of a phrase with case and number fixes”.

Here is how it works: First pick a short phrase you’ll be able to remember. Something like “A Better Day Is Coming Soon”. Now pick off the first letters of each word. ABDICS would be the word you’d use.

To improve the security I would change the letter “I” to the number one, which would give me “abd1cs” Now all you need to remember is the passphrase. (Please note, MUnet passwords must be all lowercase.)

You can find more information on this topic, refer to the Knowledge Base case 18591 on “Choosing a good password” and the Knowledge Base case 1731 on “Mandatory MUnet Password Change”