FEATURES

TECH TAILGATE

COMPUTING SERVICES: MEETING YOUR NEEDS BEHIND THE SCENES (IT-HELP@CMU.EDU)

WORKDAY AND CMUWORKS SERVICE CENTER GO LIVE!

CAMPUS RESEARCH COMMUNITY TO BENEFIT FROM SPARCS

GOOGLE APPS FOR FACULTY, STAFF AND GRAD STUDENTS

SUPPORTING INDIVIDUALS, WORKGROUPS, AND THE TOOLS THEY NEED

MORE

REVISITING PASSWORD SECURITY

PORTAL AND MYANDREW RETIREMENT

CLUSTERS AND CLASSROOM UPGRADES

ISO CORNER

LEARNING THROUGH LYNDAL.COM

SUPPORT FOR OS X 10.9 MAVERICKS

PERSONALLY IDENTIFIABLE INFORMATION (PII)

GUEST WIRELESS AND EDUROAM

cmu.edu/computing/ AUGUST 2014
CURSOR_ is published twice each year for Carnegie Mellon faculty, staff and students. Content in Cursor may be reprinted without permission; however, credit to the source is requested.

Computing Services Vision
Computing Services will meet the changing needs of Carnegie Mellon by combining the best of industry-standard information technology services, innovative solutions and best practices.

Computing Services Mission
Computing Services enables and advances an information technology environment that supports the research and education missions and the associated administrative functions of Carnegie Mellon.

Carnegie Mellon University
Computing Services

STUDENTS! JOIN US FOR A
TECHNOLOGY TAILGATE
AUGUST 26TH
3:30 - 6:00
UC RANGOS

Join the Computing Services team for discussion, free food, and a chance to win some great prizes including an iPad mini!
Computing Services has been working behind the scenes to improve the way the campus community interacts with our service offerings. From how you work to resolve a problem with the Help Center, to browsing and finding information about a service, we are committed to providing a more streamlined and service oriented user experience.

Computing Services provides IT services that enable and advance Carnegie Mellon’s business objectives: research and artistic creation, teaching and learning, international initiatives, and finance and infrastructure. IT service management (ITSM) is a set of organizational capabilities, processes and practices that focus on the relationship between IT and customers’ business outcomes rather than the underlying technology. With a business-centered view of our services, we can manage people, projects and funding to meet the needs of students, faculty and staff.

Following the trend of many of our higher-ed peers, Computing Services’ service-based approach is founded on a set of standard practices known as the Information Technology Infrastructure Library (ITIL). ITIL was developed to standardize IT practices of government agencies and private contractors.

While this is an ongoing effort, we have made changes to move towards this service-based approach and will continue to do so in the coming years.

**Help Center Email Address Change**

The advisor@andrew.cmu.edu email was recently transitioned to it-help@cmu.edu in order to more appropriately tie our identity and services to our email address. This change is also the first step in standardizing points of contact for Computing Services. The new email address is currently active, however, email will still be accepted through advisor@andrew.cmu.edu as campus adjusts to this transition.

**Servicenow Support and Management Tool**

Earlier this year we replaced Remedy with ServiceNow, an incident, request, knowledge and problem database and tracking tool. In making this switch, we can allow for more transparency and efficiently manage service tickets from one department or individual to another. Self-service applications will eventually be developed through ServiceNow to allow the campus community to initiate and manage their IT requests, where they will also have access to reporting and dashboard capabilities.

**Moving Towards Transparency**

As we make progress, Computing Services will transform our website to be more customer focused; similar to the landing pages we currently provide for staff, students, and faculty. This will include further development and publication of our service catalog, with a consumer-centric view of available services and the level of service that should be expected.

Stay informed of our changes — visit Computing Services News at cmu.edu/computing/news/. 

---

*Cursor*
There is no doubt that you've heard a lot about password security at Carnegie Mellon University — whether through the Information Security Office and Computing Services or through your own department. So, why are we bringing up the topic of password security again?

As the new academic year begin, we remind you to change your Andrew password; select a strong password and set your password reset questions.

In spite of the amount of information shared with the university community members about password security, the Information Security Office (ISO) continues to see security risks. These risks are associated with the use of a weak password, the inappropriate use of an Andrew password for various online applications, and the rotation of previously used passwords. Some individuals willingly share their passwords with other colleagues and family members or are lured into providing their username and password in response to a phishing email. Recent large-scale security breaches (e.g., Target, Adobe, PayPal, and eBay) are good reminders of the importance of using a strong password.

**PASSWORD MANAGEMENT 101**

To help Carnegie Mellon affiliates select a strong password, ISO established Guidelines for Password Management. These guidelines recommend using a strong password that meets the following criteria: at least 8 characters in length; contains both upper and lowercase alphabetic characters; at least one numerical character; at least one special character (e.g., H@v3$av3D).

The guidelines also recommend changing your password periodically and employing different passwords for various accounts. Avoid using your Andrew password for other accounts; if those systems are compromised, you may risk disclosing the information you access with your Andrew password.

**CARNEGIE MELLON ACCOUNTS VS. PERSONAL ACCOUNTS**

Keep in mind that applications supported by the university, such as Google Apps @ CMU and Box, are accessed using your Andrew credentials through the University Web Login service. This is different than direct access to a personal Gmail or Box account. The university requires a set of security controls and encryption for supported third-party applications, which may not be offered for free personal accounts.

**WHAT IF YOU CAN’T REMEMBER ALL THE PASSWORDS YOU HAVE?**

A strong password can be difficult to remember. One solution is to use a passphrase instead of a password. A passphrase can be a quote, sentence or song lyric, can contain spaces, and is easy to remember. For example, I wa1K my D0g @ 6 pm is a strong, easy to remember passphrase, especially if you walk your dog at 6 pm. Notice how some of the letters were replaced with numbers and special characters to make it even stronger. A passphrase with spaces is permitted for Andrew accounts.
Besides the use of a passphrase, you can use Identity Finder’s Vault to store a list of your passwords with the ability to access them using a master password. Apple’s Keychain utility can be used to store login credentials, and the free applications KeePass and Norton Identity Safe are good alternatives for Windows. Other password managers may charge an annual or one-time license fee.

Whether you use a password management application or not, avoid writing down your password on a sticky note next to your computer or in plain view. If for any reason you write down a password, make sure it is kept in a secure location (e.g., in a locked drawer) and is properly destroyed when no longer needed.

WE WILL NEVER ASK YOU FOR YOUR PASSWORD.

ISO recommends that you avoid sharing your password with anyone. Even when contacting the Computing Services Help Center, you should not send personal information via email.

Many community members have been tricked into providing their username and password in response to an email sent from what appears to be a legitimate university department ( phishing email). We will never ask for this information in an email message.

WHAT IF YOUR PASSWORD IS COMPROMISED?

If you have shared your password with a colleague, friend or family member or have an account with services that were breached, you should change your password immediately. If you shared your Andrew password in response to an email or a phone call, change your password now and contact it-help@cmu.edu.

In the event that ISO detects an Andrew account password compromise, your account may be locked to protect your personal data. If this happens, you will need to contact the Computing Services Help Center to reset the password. This process is much easier if you’ve already set your three password security questions: see cmu.edu/computing/accounts/passwords/change.html for more information.

ISO will also notify you through the Computing Services Network Incident System Console (NISC) if it detects that you were among those who received a phishing email, even if you didn’t fall for the deception. ISO also encourages you to report any phishing email you receive.
OVER THE SUMMER, Computing Services has been busy updating our public computing clusters and classrooms, improving connectivity, updating operating systems, adding more powerful hardware, HD projectors and larger, sharper displays.

CLUSTERS UPDATES
Almost all of the clusters have been updated or enhanced in some way, but the most notable improvements are the 30 new Mac Pros available on the third floor of the College of Fine Arts (CFA).

Walk into either CFA 323 or the CFA 318 cluster and 30 sleek, silent, black aluminum cylinders attached to big, beautiful 27-inch Thunderbolt displays will greet you. Each Mac Pro has a 3.0GHz Intel Xeon E5 processor running 8 cores and 32GB of 1866MHz RAM. There are instructor computers with the same specs at the front of the room, each connected to either a projector or LCD display. CFA 321 (sound room) has also been upgraded with Mac Pro hardware.

Other clusters updates include:
- Updated iMacs in Morewood Gardens, West Wing, and the Residence on Fifth.
- The Wean 5201 Collaborative Teaching Cluster has updated iMacs with solid-state drives and larger monitors.
- Baker 140D has been reconfigured as a ten seat teaching cluster with updated iMacs and more student desk space.
- Baker 140E and F now contain updated lecterns and improved projection including secondary LCDs mounted toward the back of the room to help with visibility for those seated in the back.
- The Hill Residence Service Center on Margaret Morrison Street now contains an updated Web Station and printer.
- Operating System updates include OS X 10.9 (Mavericks) on all Macs; Windows computers continue to run Windows 7.

CLASSROOM UPDATES
The following classrooms have been updated with HDMI connectivity:
- Baker Hall: 235A, 235B, 237B
- College of Fine Arts: 102
- Hamburg Hall: 237, 1002, 1003, 1004, 1511
- Mellon Institute: 355, 488
- Wean Hall: 4709, 6423, 8427
Campus affiliates continue to take advantage of our university license with lynda online training. If you haven’t already, sign on to cmu.edu/lynda/ with your Andrew ID and password and enjoy learning on your own time and at your own pace. The lynda online library offers more than 2,400 courses taught by industry experts. Classes are designed for all levels of learners and can be viewed on your computer, iPhone, iPad, Android phone or tablet, or other mobile device.

**NOT SURE WHAT YOU WANT TO LEARN?**

In lynda, click My Courses, select Recommended then Update interests. You’ll be presented with a simple survey to determine which lynda courses best meet your criteria. As lynda adds content, new courses that match your interests will automatically be added to your recommendation list.

**LEARNING THROUGH LYNDÁ**

**Lynda Top 5**

Over the past year, the following lynda courses were most popular on our campus:

1. C/C++ Essential Training
2. Foundations of Programming: Object Oriented Design
3. SQL Essential Training
4. SQL Server 2008 Essential Training
5. User Experience Fundamentals for Web Design

**Faculty: Get a solid start with a lynda foundation!**

The lynda playlist feature is ideal for faculty members who want to assign prerequisite training for their course. Faculty can browse lynda for relevant topics and create a "Prerequisite" playlist to share with students. Faculty members may also take advantage of the lynda Playlist Center. These playlists, which are curated and frequently updated by the lynda content team, can be used as targeted learning paths. To access playlists, log in to cmu.edu/lynda/ and click the Playlist Center link at the top of the page.
CARNEGIE MELLON UNIVERSITY will go live with Workday and open the CMUWorks Service Center in late December 2014. The first payroll in January 2015 will be run in Workday. Between now and go live, many campus readiness activities will take place to prepare all employees to use the new system and take advantage of the new service center. Please visit the CMUWorks website at cmu.edu/hr/cmu-works/ regularly for important communications, project updates, and training information.

CMUWORKS PROJECT UPDATE

Since the last CMUWorks project update in the August 2013 Cursor_ (cmu.edu/computing/news/cursor/aug2013.pdf), many key milestones were achieved thanks to the dedication and commitment of the project team and collaborating campus partners. The project team completed system design, build, and unit testing, continued change management activities, convened the Readiness Advisors to help prepare campus for go live, conducted user acceptance testing, and finalized the project timeline and go live date to ensure implementation success.

The final stage of the CMUWorks project will focus on conducting Operational Readiness Testing (ORT) and end-to-end testing (Workday to/from other campus university systems, such as Oracle), building reports, delivering training, and finalizing transition plans for go live.

WHAT WORKDAY MEANS FOR YOU

The implementation of Workday will benefit all staff, faculty, and student workers. The table on the next page provides a high-level overview of the functions that Workday will support, the existing systems Workday will replace, and what Workday means for Carnegie Mellon University and members of the community. Important information about system decommissioning activities, transition dates, and training opportunities will be provided as the go live timeframe nears.

A WORD FROM THE PROJECT EXECUTIVE

I feel privileged to have been entrusted with the success of CMUWorks. This project is critical to enhance the delivery of HR, Payroll and Benefits Services to our faculty and staff population. It also positions us for greater financial stability when developing our systems' infrastructure to maintain best in class practices. The success of this initiative will ensure the university's competitiveness in the 21st century and provide a firm foundation for continued excellence.

I am impressed...

with the hard work and dedication exhibited by the CMUWorks teams. Their continued participation, expertise, and contributions will result in a successful project launch.

Amir Rahnamay-Azar Ed. D.,
Vice President for Finance and Chief Financial Officer,
CMUWorks Project Executive

"
| Core HR Transactions (e.g., Hire, Change Job, Separations, Compensation, etc.) | HRIS (Human Resources Information Systems), including the HREM (Human Resources Employee Module) and the HR Data Warehouse | All core HR transactions will be performed in Workday; HRIS, HREM, and the HR Data Warehouse will house historical data and remain available as read only systems  
- All employees will have access to view personal compensation information in Workday |
|---|---|---|
| Payroll | ADP for Payroll (outsourced Payroll processing) | Instead of logging into iPay, all users will log into Workday to view pay checks and W2s (from go live on) and view/update direct deposit and W4 information  
- iPay will remain read only for historical payroll information |
| Employee and Faculty Self Service | HR Connection | All employees will access Workday to update demographic information (e.g., address, emergency contact, etc.) |
| Benefits | HR Connection and Bessa | All employees will view benefit information, update benefits when possible due to life and job events, and select benefits during open enrollment in the fall of 2015 |
| Position Management | TMS (Talent Management System) – Position Module | Position Management in Workday will enable CMU to create accurate FTE reports, manage and analyze our workforce, facilitate compliance, and streamline data entry for the recruiting and the job requisition process |
| Absence / Leave Management | Excel spreadsheets (e.g., PTO requests) | All employees can request time off and view their PTO balance in Workday  
- Managers will be able to approve time off requests from any device with Internet access (including smart phones) |
| Time Tracking | PRS (Payroll Roster System)  
Green Time Sheets | All non-exempt employees will enter/submit time electronically in Workday  
- Managers will approve time electronically in Workday |
| Faculty Information Management (promotion and tenure data) | Excel spreadsheets (e.g., faculty promotion and tenure) | Academic appointment information will be maintained in Workday  
- Faculty members will be able to view tenure status and appointments |

VISIT THE CMUWORKS WEBSITE at cmu.edu/hr/cmu-works/ regularly for important communications and up-to-date project information and to view the latest CMUWorks Project Newsletter. You can subscribe to the newsletter by emailing cmu-works@andrew.cmu.edu with the subject heading 'subscribe'. We invite you to submit questions or suggestions about the CMUWorks project to cmu-works@andrew.cmu.edu.

CONTRIBUTED BY AMANDA PERKINS
RESEARCHERS AND ADMINISTRATORS ON CAMPUS will be pleased to learn of the SPARCS project—an effort with the goal of supporting administrative aspects of the research proposal and award process including proposal development, submission, budget considerations and research compliance.

An acronym for Sponsored Programs and Research Compliance System, SPARCS is a collaborative Carnegie Mellon project to implement an enterprise tool that modernizes and supports administrative aspects of our university’s research initiatives. The SPARCS project team is comprised of members of Computing Services, the Office of Sponsored Programs, the Office of Research Integrity and Compliance and campus stakeholders. Researchers and administrators from many colleges and departments are participating in the implementation of the new system. SPARCS will deliver the following technology modernization and process improvements:

- Eliminate duplicate data entry and paper processing resulting in improved productivity of campus units and central research support offices (Office of Sponsored Programs, Office of Research Integrity and Compliance).
- Minimize faculty time spent on administrative aspects of Institutional Review Board (IRB) protocols, grant proposals and submissions.
- Reduce errors, improve productivity and reduce proposal rejections due to formatting through automated data validation.
- Minimize “human error” that could lead to compliance violations and financial penalties via module cross communication and validation.
- Streamline workflow and improve communication with the research community by leveraging new technology and redesigning processes.
- Document history of proposal/award/compliance to meet audit requirements.

The SPARCS project team developed an implementation schedule that will deliver modules and functionality in phases into fiscal year 2017. The first to be delivered will be the Conflict of Interest (COI) Module in October 2014 that enables the following:

- Enterprise-wide disclosure to improve compliance
- Automated notifications and workflow
- Standardized reporting
- Retirement of current Kuali solution and paper based processing

Remaining SPARCS modules include the Institutional Review Board (IRB) Module; the Institutional Animal Care & Use Committee (IACUC) Module and the Grants and Contracts Module. You can learn more about SPARCS in future issues of Cursor_, through campus-wide announcements, or through the SPARCS web site at cmu.edu/research-office/sparcs/). Questions or comments can be addressed to sparcs@andrew.cmu.edu.
PERSONALLY IDENTIFIABLE INFORMATION (PII) is any piece of information that can potentially be used to distinguish or trace a person's identity. PII also refers to other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.¹

The following are examples of sensitive information that can identify you when linked with your full name or initials, and are considered PII:

- Social Security Number (full and truncated)
- Driver's license and other identification (e.g. passport and state ID)
- Citizenship, legal status, gender, race and ethnicity
- Birth date and place of birth
- Home and cell phone numbers
- Personal email, mailing and home address
- Internet Protocol (IP) or Media Access Control (MAC) address
- Mother's middle and maiden names
- Family information: marital status, spouse and children information, emergency contact and guardian information
- Biometrics, x-rays, fingerprints, retinal scans, voice signatures, etc.
- Financial information, medical information and student education record
- Employment information

¹ National Institute of Standards and Technology: Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).
SAFEGUARDING YOUR PII

Carnegie Mellon makes every effort to protect PII. Only those individuals with a job requirement to use or process PII can access the data.

Unauthorized access to PII, whether intentional or unintentional, may lead to data breach and Identity Theft. Identity Theft tops the list of fraud complaints reported by the US Federal Trade Commission (FTC). Scams and robbery are some techniques thieves use to steal your identity. Another method is to prowl social networking sites, chatrooms, text messages and online forums to gather information you freely provide.

A number of campus affiliates have shared their Social Security Number (SSN) and other PII with Computing Services when they’ve reported account or network issues. Computing Services urges you to not share your PII information in an email for any reason, especially your SSN number and Andrew password.

To protect PII:

• Limit what you share on social networking sites.
• Avoid providing personal information in response to an email, phishing attempt or phone scam (e.g., username, password, SSN, credit card, bank account number).
• Avoid providing your SSN number, personal, or financial information to individuals claiming to represent IRS, your bank or service providers (e.g. phone company).
• Do not open email attachments or links sent by individuals you don’t know. Such email may contain malware designed to access information on your computer.
• Avoid sending PII in an email to university entities.
• Verify the identity and authority of anyone requesting PII.
• Avoid leaving documents with PII in plain sight.
• Shred all documents containing PII, and follow the university Guidelines for Media Sanitization and Disposal (cmu.edu/iso/governance/guidelines/data-protection/media-sanitization.html).
• Make sure your operating system and software are updated and anti-virus software is installed on your computer (cmu.edu/computing/security/).
CLOUD COMPUTING

The use of cloud services for personal use (e.g., Google Apps, Apple iCloud, Dropbox, SkyDrive) has been growing rapidly. Their popularity can be attributed to negligible cost and online accessibility from multiple computing devices. However, when using cloud services, you should ensure that your data is protected by following these tips:

- Use a strong password that is different from your Andrew password.
- Use caution when storing sensitive data in the cloud. For example, avoid storing Personally Identifiable Information (PII) such as Social Security Numbers, driver license numbers, health insurance and credit card numbers.
- Educate yourself on the unique security and privacy features of the cloud services you use most frequently.
- Beware of “Terms of Use” agreements that don’t respect the privacy or security of your data.

DON’T LOSE YOUR NETWORK ACCESS

You are responsible for the content and actions of your computer! If you use Peer-to-Peer (P2P) file sharing applications (e.g., Bit Torrent, LimeWire, etc.) be aware that the content of the “shared” folder on your computer may be publicly available to others on the internet. This means others can download music, movies, games or other digital files directly from your computer. This process of file sharing can be a source of illegal distribution of copyright protected material and can result in disciplinary action or loss of network connectivity. There are legal alternatives for acquiring copyright protected content. For more information, refer to the following:

- University’s Fair Use Policy — cmu.edu/policies/documents/FairUse.html
- Copyright Violation Guidelines — cmu.edu/iso/governance/guidelines/copyright-memo.html
- Digital Copyright and DMCA — cmu.edu/iso/aware/dmca/

DMCA PROCESS FOR STUDENTS

When requested, Carnegie Mellon is legally required to stop unauthorized downloading and/or distribution of copyrighted materials. If we receive a Digital Millennium Copyright Act (DMCA) notice and identify your computer as the offender, you will have 72-hours to resolve the issue with the Student Life Office. If it is not resolved, you will lose your network access and will not be able to register new devices or computers. For more information, see cmu.edu/iso/aware/dmca/.

COMPROMISED COMPUTER PROCEDURE

If you suspect your computer has been compromised, stop using your computer and report the problem immediately. Students should contact the Computing Services Help Center (412-268-4357 or it-help@cmu.edu). Faculty and Staff should contact the ISO (412-268-2044 or iso@andrew.cmu.edu). For more information visit cmu.edu/iso/governance/procedures/compromised-computer.html.

PROTECT YOUR DATA
SECURE YOUR MOBILE DEVICE

Mobile devices, including Smart Phones, are portable computers that should be secured the same as any computing device. Adhere to these practices

• Lock your phone with a PIN, password or pattern.
• Avoid storing sensitive data on your phone.
• Use caution when connecting to public wireless networks; instead connect to secure wireless networks when available (e.g. CMU-SECURE).
• Update your mobile device apps frequently.
• Disable Bluetooth when not in use.
• Adhere to information in ISO’s Mobile Device Security and Usage Guideline at cmu.edu/iso/governance/guidelines/mobile-device.html

DID YOU KNOW?
The Symantec 2014 Security report revealed that 81% of social networking customers fall for various scams on a number of social networking sites. An alarming 12% of these customers reported that someone hacked into their account and pretended to be them! The report also stated that 25% of customers continue to share their social networking password with friends and family members.

PHISHING ATTEMPTS: DON’T BE FOOLED

Phishing is a form of social engineering that can be presented in a number of ways. One example is where a malicious person attempts to lure someone into providing sensitive information (e.g. Andrew ID and password). Another type of Phishing attempt might encourage you to infect your computer by visiting a malicious website or by opening a malicious email attachment. Protect yourself from falling victim to these attempts:

• Never provide your Andrew password or any password in email. Computing Services will NEVER ask for your Andrew account password.
• Learn how to differentiate between legitimate and malicious links by playing Anti-Phishing Phil at cmu.edu/iso/aware/phil/.
• Don’t open unexpected email attachments. If you know the sender, first verify that it was sent by them. If you don’t know the sender, delete the message.
• Be cautious of emails that communicate a sense of urgency (e.g. "respond immediately", "urgent message").
• Update and run your antivirus software frequently.

DID YOU KNOW?
In January 2012, nearly 19% of students at Carnegie Mellon’s Pittsburgh campus clicked on a phishing email link that lured them into changing their Andrew account password?
SOCIAL NETWORKING PRECAUTIONS

Social networking is extremely popular and fun! But it’s important to protect your data. Follow these tips:

• Use a strong password when creating a social networking account and change it every six to twelve months. Do NOT use your Andrew password for social networking.

• Avoid using the same password on a social networking site that you use to access online banking or your health records.

• Be cautious of what you share. Avoid posting sensitive information or information that may lead to identity theft (e.g. SSN, full name with birth date, etc.).

DID YOU KNOW?
The Symantec Internet 2014 Security report revealed that 38% of mobile customers have experienced mobile cybercrime. Also, 52% of mobile customers are using poor security practices by storing sensitive and work information on mobile device cloud services.

• Periodically review your privacy settings.
• Beware of phishing attempts made through social networking.
• Set your account privacy options to limit information people can learn about you through a search engine.

COMPUTING SERVICES
QUESTIONS?

it-help@cmu.edu
412-268-4357 cmu.edu/computing/
GOOGLE APPS @ CMU EMAIL OPTION FOR FACULTY, STAFF AND GRADUATE STUDENTS

Undergraduate students made the move to Google Apps @ CMU last fall. Are you interested in joining them? If you currently use the Cyrus email service, you are eligible and you can schedule a migration any time. Check with your departmental IT support staff first, then visit google.cmu.edu and click the "schedule a migration" link.

Google Apps @ CMU is easy to use and familiar to many on campus. The service allows you to store documents, create appointments and share files with others who use Google Apps. And, you have 30 GB of storage! You’ll continue to use the same email address (AndrewuserID@andrew.cmu.edu) with your Andrew userID and password. However, if you plan to use a mobile device with the Gmail app, you will need to create a Google Apps password. Please see google.cmu.edu/ for steps.

CONNECTING WITH CAMPUS AFFILIATES

When you transition to Google Apps @ CMU, you can continue to send and receive meeting invitations. When a guest receives an invitation, they will use the attached iCalendar file to add the event to their own calendar. The CMU directory is also integrated with Google Apps making it easy to find affiliates.

PORTAL & MYANDREW RETIREMENT

HAPPY RETIREMENT: PORTAL, MYANDREW

After many years of loyal service, the Carnegie Mellon Web Portal at my.cmu.edu/ and the MyAndrew web page at cmu.edu/myandrew are retiring!

Deployed as central locations for tools, services, and information for the campus community, the MyAndrew web service and the Web Portal have slowly become collections of links to other pages. Services previously available there are either no longer needed or have been integrated elsewhere.

The MyAndrew and Carnegie Mellon Web Portal pages were recently updated to offer links to services they previously hosted. If you are in the habit of navigating to services through the Web Portal or MyAndrew, be sure to visit my.cmu.edu/ and cmu.edu/myandrew/ to bookmark the links that you need. To ensure a smooth retirement, the updated MyAndrew page will be available until September 9th and the Web Portal page until November 30th.

Computing related services that were previously available through the portal or MyAndrew will continue to be accessible through our web site at cmu.edu/computing/ or through the quick links provided on Computing Services’ student, faculty, or staff web pages:

- cmu.edu/computing/students/
- cmu.edu/computing/faculty/
- cmu.edu/computing/staff/
COMPUTING SERVICES currently offers several programs to support individuals, workgroups, and their devices. The Computing Services Help Center (it-help@cmu.edu) is available for free to students, faculty, and staff. Academic and administrative groups and individuals can also take advantage of several fee-based and free support offerings.

Last year, Computing Services began an effort to develop more focused and sustainable support models for the 2015 fiscal year. Working with customers and advisory teams, we have streamlined and evolved some of our offerings to better meet the needs of clients now and in the future.

EXECUTIVE IT SUPPORT
As part of the sustainability effort, DSP Platinum, also known as Executive Class Support, has been spun-off from DSP and is now a separate group: Executive IT Support. This reorganization will enable the Executive IT team to leverage existing synergies with Media Technology Services and tailor support to the unique needs of individual clients and the specific devices they use, including mobile and conferencing technologies. This service is billed per individual.

DESKTOP SUPPORT PROGRAM
The new Desktop Support Program model is focused on providing managed computer administration and deployment to departments. This new model is billed per device, rather than by consultant time. DSP consultants provide device-centered support in teams to enable a more efficient allocation of staff resources and a more consistent response to end users.

For fiscal year 2015 DSP, will offer two tiers of support: Business Class and Enterprise Class.

• Business Class includes support for desktop and office productivity software as well as remote telephone and email support.
• Enterprise Class includes Business Class support and adds additional time for in-person support as well as department-specific software installation and assistance.

FOUNDATION SERVICE FOR DESKTOP MANAGEMENT
Computing Services also offers the Foundation Service for departmental desktop management and deployment. A free service that is available to departmental IT administrators, the Foundation Service offers the same central toolset used by Computing Services for desktop computer management and support.

Through the Foundation Service, IT administrators can take advantage of desktop management software, endpoint protection and more, making deployment and administration safer, faster and more efficient. Consulting on Active Directory management, Group Policy and file storage management are also available as part of the Foundation Service. The service is currently available for Windows, with Mac support coming early in 2015. Software licensing fees may apply.

For more information about the Desktop Support Program, visit the DSP web page at cmu.edu/computing/dsp/ or send email to dsp@andrew.cmu.edu.

For more information about Executive IT Support, email exec-it@andrew.cmu.edu.

For information about our Foundation Service, email it-help@cmu.edu.
In March 2014, Computing Services announced support for Apple’s latest Mac operating system, OS X 10.9 (Mavericks), followed in May by the retirement of support for OS X 10.7 (Lion).

Mavericks is a major OS upgrade and incorporates many improvements and new functionality, along with an updated look and feel.

One thing Mavericks does not come with: a price tag! With previous versions of the Mac operating system, the university negotiated license agreements with Apple and provided downloads of the software from our servers. Because Apple has made Mavericks free to download from the Mac App Store, university affiliates can go directly to that source to download the software.

Before upgrading, we recommend that you contact your departmental IT administrator or DSP consultant to ensure that Mavericks will work in your environment.

Training on the Mac OS X 10.9 operating system is available free of charge to all university affiliates through cmu.edu/lynda/

To review the Computing Services OS X support statement, visit cmu.edu/computing/software/all/mac/

For information on how to upgrade, visit Apple at apple.com/osx/how-to-upgrade/

OS X YOSEMITE

Yosemite is currently in public beta. Computing Services will assess our core software and services for compatibility with Yosemite when it becomes available this fall.

Stay tuned to cmu.edu/computing/news/ for updates.