The transition of Cohort 2 units into UCF IT was recently completed. Cohort 2 included the Center for Distributed Learning, College of Undergraduate Studies, the Division of Teaching and Learning, the Office of Instructional Resources, UCF Connect, and University Libraries. To date, approximately 270 staff have transitioned into UCF IT.

A key element of IT2020 is strengthening IT governance. In this regard the IT Strategic Governance Committee (ITSG) and the IT Professionals Committee (ITPros - see sidebar) were formed. Work products from these committees include a project prioritization process (ITSGC) and a structure that encompasses all UCF committees and groups that deal with information technology (ITPros).

The goal is to be as transparent and open as possible during the development of UCF IT. Ideas or concerns are welcome via email at it2020@ucf.edu or anonymously at http://ucf.qualtrics.com/jfe/form/SV_0TIpkQBeZAd3HKt.

**IT Pros Committee in its Third Year**

**IT Pros Committee in its Third Year**

The 16-member IT Professionals Committee, established as an element of the IT 2020 initiative, works to establish a comprehensive and effective UCF IT community by identifying ways to enhance IT capabilities, efficiency, effectiveness, and consistency through a transparent process.

The committee held its first meeting on July 14, 2015, and has met nearly every month over the past three years. Larry Jaffe served as the initial chairperson and was recently succeeded by Felicia Kendall. Recent topics discussed by the committee include desktop and device standards, Microsoft Teams, and governance.

Committee agendas and minutes can be found on the IT2020 website at http://itr.ucf.edu. Meetings are open for anyone to attend. For additional information, contact Felicia Kendall at Felicia.Kendall@ucf.edu.

**Trevor Colbourn Hall Update**

Construction of Trevor Colbourn Hall was completed in late July and occupants began moving in at the beginning of August—a process that continued through the middle of the month. Colbourn Hall is tentatively scheduled for demolition on Sept. 15.

In addition, the demolition of Wayne Densch I and II was scheduled to begin on August 15. Occupants of Wayne Densch I and II have been assigned new locations as follows:

- Athletics (Rowing, M/W Golf, M/W Tennis, Cheer/Dance)
  -Moving to Ferrell Commons – G (FC-G)
- TRiO Center
  -Moving to Howard Phillips Hall (Suites 217 and 221)
- COHPA (Criminal Justice, HMI, and Health Sciences)
  -Moving to Health and Public Affairs I and II, Howard Phillips Hall, and OTC 300
- Office of Institutional Equity
  -Moving to Barbara Ying Center – CMMS (BYC-CMMS) (Suite 101)

The Office of Institutional Equity will be moving to a permanent location in BYC-CMMS, which is located next to the Office of Diversity. Athletics’ occupation of the FC-G space is temporary, and they will relocate to their permanent location at the Wayne Densch Sports Complex after the expansion project is completed in the next 12-18 months. TRiO Center will be moving to Howard Phillips Hall (Suites 217 and 221), which is located across the hall from its other office suites. COHPA personnel will be moving to multiple locations on main campus to accommodate new hires and improve collocation of departments.
Simulated Phishing Campaign Results

On June 26 the Information Security Office began an anti-phishing program by sending a simulated phishing email to 6,587 employees, asking them to click on a link to check their passwords.

This initial baseline message was intended to determine the percentage of users who clicked on the link. A user who clicked on the link was directed to a web page that prompted them to enter their email address to begin the “password check.” Users who submitted data via this form were then shown a message indicating that this was a phishing test and providing tips for identifying suspicious emails and a link to the Information Security Office’s phishing resources page.

The Information Security Office found that 408 users clicked on the link and 176 entered data on the form. More than 1,000 users reported the email using the new Phish Alert Button in Outlook. Future campaigns will leverage more challenging email templates.

The goal of the anti-phishing program is to raise awareness of the threat of phishing and provide feedback for users who click on the links provided in the emails. The new Phish Alert button in Outlook, which is located below the sender information, makes it easy for users to report suspicious emails. Please refer to https://infosec.ucf.edu/phish-alert-button for more information. Information security is everyone’s responsibility, and improving everyone’s ability to identify phishing attempts will help keep UCF secure.

Hidden Artists Exhibition

You might find them in front of the classroom or in the office down the hall and yet never suspect they make art. They are UCF’s “Hidden Artists,” a group of faculty and staff members from various departments who create art on their own time. Founded by Judy Bragg Pardo, retired senior art specialist at SDES, Hidden Artists have exhibited at the John C. Hitt Library since 2008.

Now in its 11th year, the Hidden Artists exhibit will be on display in the library through Sept. 28, 2018. A reception is planned for Sept. 13, 2018, from 4-6 p.m. at the library in Room 223. The event is open to the public and will include refreshments, as well as an opportunity to talk with the artists.

For more details about the exhibit and Hidden Artists group, please contact Chris Saclolo at Christopher.Saclolo@ucf.edu.

Data Center Migration Update

UCF IT has begun transitioning the university’s main data center from the College of Sciences Building (CSB) to a commercial data center in Southeast Orlando. During this transition, dozens of racks of equipment in CSB will be consolidated to just four racks offsite. This shift will save the university thousands of dollars annually in power and cooling costs and also reduce the costs associated with maintaining an on-campus data center facility.

The goal of the anti-phishing program is to raise awareness of the threat of phishing and provide feedback for users who click on the links provided in the emails. The new Phish Alert button in Outlook, which is located below the sender information, makes it easy for users to report suspicious emails. Please refer to https://infosec.ucf.edu/phish-alert-button for more information. Information security is everyone’s responsibility, and improving everyone’s ability to identify phishing attempts will help keep UCF secure.

Hidden Artists Exhibition

You might find them in front of the classroom or in the office down the hall and yet never suspect they make art. They are UCF’s “Hidden Artists,” a group of faculty and staff members from various departments who create art on their own time. Founded by Judy Bragg Pardo, retired senior art specialist at SDES, Hidden Artists have exhibited at the John C. Hitt Library since 2008.

Now in its 11th year, the Hidden Artists exhibit will be on display in the library through Sept. 28, 2018. A reception is planned for Sept. 13, 2018, from 4-6 p.m. at the library in Room 223. The event is open to the public and will include refreshments, as well as an opportunity to talk with the artists.

For more details about the exhibit and Hidden Artists group, please contact Chris Saclolo at Christopher.Saclolo@ucf.edu.
Vendor Risk Management Program Process Improvement

The Information Security Office’s (ISO) Risk and Compliance team has been working to simplify and streamline the Vendor Risk Management (VRM) program. Earlier this year, the process was moved to ServiceNow, and a central home for the program was created on the Infosec website. In the recently completed Phase 2, the focus was to make the process easier to understand for UCF units engaging new vendors and reduce the time it takes for a contract to be executed — all while continuing to ensure that vendors are meeting university security and compliance requirements.

New VRM/contract process flow

Improved and Simplified Documentation
One improvement is a revamped “Secure Handling of UCF Data” agreement. This document is meant to be included in any agreement or contract where Restricted or Highly Restricted Data are involved. The new version combines and improves upon two previous documents: the Secure Handling of UCF Data rider and the Minimum Security Requirements checklist. This more robust document provides legal confidence in a vendor’s protection of UCF data, while reducing the number of documents passed to vendors. Acceptance of the agreement allows ISO to focus on other critical areas of review.

University-level Process Improvement: Contracts
Previously, it was recommended that the VRM process was completed in full before a contract was submitted to General Counsel. In the new model, UCF units still submit proposed vendors to ISO first. However, as soon as the data involved in the engagement can be finalized, UCF units can submit the contract to General Counsel for review. General Counsel will ensure the Secure Handling of UCF Data agreement is integrated into the contract as an element of its overall review process. While this occurs, the ISO continues with an in-depth review of the vendor. In the end, ISO prepares a report that contains security risks and concerns identified in the ISO review and General Counsel’s review, and negotiation of security-related contract terms. By performing both review processes in parallel, the overall university-level process of vetting a vendor and executing an agreement should move more quickly.

“What do I need to do?”
UCF business units should familiarize themselves with the new Secure Handling of UCF Data agreement and updated Frequently Asked Questions (FAQs), which explain how the document changes simplify the VRM submission process and requirements. Both can be found at https://infosec.ucf.edu/vrm. Finally, UCF units should expect to engage ISO and General Counsel in parallel once the VRM process has begun.

New Chinese-American Library Association President

Ying Zhang, the department head of acquisitions and collection services at the UCF Libraries, has been elected the 2018-19 President of the Chinese-American Librarians Association (CALA).

With more than 700 global members, CALA is the largest ethnic caucus affiliated with the American Library Association (ALA). Its core missions are to advocate diversity and inclusiveness in libraries, advance professional interests and development opportunities among the members, and foster cooperation on allied interests with other organizations nationally and internationally.

As president, Zhang is leading CALA on all of its missions.

This year, Zhang has been invited to speak and represent CALA at the annual conferences by the Library Society of China (LSC), ALA, and International Federation of Libraries Associations (IFLA). Each attendance allows Zhang to act as an ambassador for UCF, and to showcase in the U.S. and the world UCF’s commitments in diversity, international focus, and the aspiration to become the “America’s best partnership university.”

Zhang (far left) was invited to speak at the 2018 Chinese Library Exhibition, organized by the Annual Conference of the Library Society of China. Pictured are members of the Chinese-American Librarians Association along with the ALA director for library international relations, and librarians from Mongolia and Singapore.
Information Technology Infrastructure Library (ITIL) is a set of best-practice guidelines for IT service management that provides guidance on the provision of quality IT services and the underlying processes, functions, and other capabilities. UCF IT is adopting the ITIL framework in order to sustain and improve the delivery of highly effective, responsive IT services.

UCF IT’s ITIL implementation began with Change Management in 2016. This process has now been rolled out to almost all departments in UCF IT, resulting in fewer unplanned outages and improved efficiencies across production environments.

Following Change Management, Incident Management was implemented later in 2016 with the goal of providing customers with a consistent service experience, and also for informing the IT staff working the issues regarding the incident criticality, the expected customer resolution time, and the requirements in communicating effectively with the customer. All UCF IT staff now handle incidents the same way and customers benefit by receiving the customer experience they deserve.

The third and final core ITIL process, Problem Management, was recently implemented in May 2018. This process works synchronously with Change and Incident Management. The Problem Management process manages the lifecycle of all problems including detection, investigation, analysis, resolution, and prevention. Using Problem Management enables UCF IT staff to provide higher availability of UCF IT services and reduces the inefficiencies of firefighting or resolving repeat incidents.

Targeted phishing continues to be a significant threat to information security. One such example is the “sextortion” email, in which an attacker threatens to release a webcam video of the recipient viewing adult content. Recently, a variation of this scam has emerged. In the new version, the attacker includes a password that the recipient has previously used. It is suspected that the passwords were collected from publicly available data breaches. This increases the legitimacy of the threat, and most likely is a significant factor in a recipient’s decision to pay the amount demanded.

In a recent SANS blog post, analysts were able to identify 334 Bitcoin addresses that they believed to be part of this scam. Of those addresses, 123 payments were made to 56 addresses, for a total of $235,000. The average payment was $1,900 and the highest payment was $4,900. Since Bitcoin transactions are anonymous, the lack of unique payment addresses suggests that the attackers are not interested in tracking who has paid.

Several UCF employees have received this scam email. With recent data breaches leaking users’ information from websites such as Panera and Reddit, we expect more targeted emails to arrive in users’ inboxes. Users are encouraged to use the Phish Alert Button to report these or other suspicious messages and, if a system compromise is suspected, to contact their IT department.