

University Information Technology Committee

Minutes

Monday, 02-24-2020

303 Rinker

9:30 a.m.

Join Zoom Meeting:

<https://ufl.zoom.us/my/cacim/>

Present: Stacey Ewing, Mark McCallister, Ken Sallot, William A. Fox-Alvarez, Eric Porges, Ray G. Thomas, Bill Hamilton, Michael Baumbach, Juan Nino, Marshall Haning, Laurie Bialosky, Nico Cellinese, Charley Widmer, Megan Leroy, Ryan Yang, PJ Brucat, Ray Issa, Bojan Lazarevic, and Randell Doty.

1. Call to Order & Introductions –

Raymond Issa, Chair, University Information Technology Committee

~The Meeting was called to order at 9:30 a.m. by Chair Issa and introductions were made.

2. Approval of 27 January 2020 Minutes

~The minutes were approved.

3. Two-Factor Authentication & Administrative Liaison Report –

Mark McAllister, Director of Academic Technology

~Committee members were thanked for their helpful input on IT's strategic initiative.

~The most recent metrics of two-factor authentication were shared, including the total enrolled numbers of faculty, staff and students. 11,600 are enrolled as of mid-February with 92,000 remaining unenrolled. Enrollment growth has slowed a bit and typically peaks in the fall. Two-factor authentication will be done when onboarding new faculty and staff.

-Two-factor authentication is an effective mitigation against compromised accounts. Discussion was held regarding individuals logging-in and leaving computers in public spaces, such as the university libraries, but a primary focus of two-factor authentication is successfully avoiding phishing and brute force attacks (although the latter is typically blocked by utilizing strong and changing passwords, many of which are regulation requirements).

-Devices which can be selected for use with duo authentication during log in include a: mobile phone, tablet (iPad, Nexus 7, etc.), landline, security key

(YubiKey, Feitian, etc.), or Touch ID, which requires Chrome on macOS.

-To minimize the need for repeat log-in's, there is currently a ten hour log-in window of time (i.e. from the time of log-in to automatic log-out) for duo authentication. Ten hours was chosen to accommodate the length of a typical workday for most employees, and to lessen the possibility of wasted exam or classroom time for students with any log-in issues.

~The Faculty Senate Chair has met with VP Eldayrie and his team to address faculty and class needs.

-Best practices to protect academic integrity, particularly during the administration of exams were discussed. Past practices of eliminating student mobile phone access when taking exams (in efforts to avoid cheating with cell phone screen shots, etc.) need re-consideration.

-Increasing academic integrity between the time an exam taker logs in using a cell phone and putting their phone away was discussed.

-Exam takers could arrive with a passcode and be reminded that it must remain confidential.

-A specific window of time can be offered to students to log into/have log-on access when using a one-time passcode. While it may be ideal to avoid the proliferation of key fobs, which display randomly generated access codes, their use is generally thought to minimize security vulnerability to users.

- Fobs are available at the UF Computing Help Desk and are complimentary for faculty, staff and graduate students. Fob wholesale pricing is approximately \$4 apiece.

-Conducting field work where there is not a reliable cell signal was discussed.

-Passcodes allow account log-in's even when a device is without internet connection.

-Possible duo authentication challenges for students were discussed, including resistance to fobs and installing new apps; owning an old or no cell phone; and cost restrictions. Connectivity is typically not an issue for students enrolled in the UF Online program, so a more likely challenge for this cohort is device functionality (i.e. if it breaks, runs out of batteries, etc.)

~Faculty conduct of university business on personal devices were discussed, including such alternate options as using a fob and identifying a work desk (as opposed to a personal cellular phone) number when designating a Duo 'push' option. Committee members inquired about the application of the Sunshine laws, specifically when using the UF app installed to obtain the passcode necessary for account login. To obtain clarification, the Faculty Senate Chair will send the following inquiry to the General Counsel's Office: Does by installing and using this app on faculty's personal devices subject them to the Sunshine Law, and thereby make any information/data on the devices discoverable, even if the devices' only UF-related use is for the purpose of receiving passcodes to log in to their UF

account?

-Note: Following this meeting, the General Counsel replied to the Faculty Senate Chair and clarified that neither the ownership of the device (nor the platform used to store, create, send or receive information) are the criteria for assessing Sunshine law requirements. The "content" of the information is the relevant factor. If there is content on a personal device related to UF business (e.g., text messages on a personal phone relating to UF business) then that content is a public record and subject to retention requirements and disclosure under the Sunshine laws (with certain exemptions for research data, student records, etc.)

~UF's duo authentication timeline was discussed:

- All students are expected to enroll by the new academic year.
- IT is currently crafting language germane to instructors and the posting of syllabuses, which will be shared in March. This will provide an opportunity to guide nine-month faculty needing to place this information on their syllabi.
- IT aims to complete all enrollment by the end of the calendar year, allowing adequate time for all students and new hires to all be on board with this initiative.
- This will appear in the Provost's newsletter (*Faculty Update*) in two weeks and then in an administrative memo another two weeks. This is also being placed on the IT announcement pages.
- Email to faculty sent at the impending deadlines of one month, one week, etc. was suggested but there is some concern of email inundation.
- The Faculty Senate Chair will continue to encourage faculty to sign up now before duo authentication moves to an administrative requirement.

~Suggestions made to IT in conversing with faculty about this initiative include:

- List/identify some accommodations faculty could make if students arrive at an exam without a code or second device.
- What is the responsibility of a student and a faculty member if technology, a device, or plan unexpectedly fails? A 'Plan B' guide to minimize any emergencies or surprises would be helpful to faculty.
- Proper academic assessment of students is a concern; consideration should be given to separating situations where students arrive unprepared without a code or a second device from their ability to demonstrate classroom participation and knowledge.
- Mark McCallister will consult with peer institutions who have used two factor authentication to identify common issues and effective verbiage in preparing IT FAQ's.

~IT is working to ensure all domains are under the new authentication system. Trouble-shooting has been completed on OneDrive @ UF and ONE.UF while ProctorU and G Suite/Google Drive are underway. The committee also discussed the coordination involved in using duo authentication in UF Health, including

Eduroam, VPN, and the Epic systems.

4. Adjournment

~The meeting was adjourned at 10:44 a.m.