University of Wisconsin Whitewater | Instructional Communication and Information Technology

Middle Tier Committee

Thursday, December 16, 2021, 2 p.m. to 3 p.m.

Matt Aschenbrener x	Heather Chermak	Lauree Miller	Lynsey Schwabrow x
Trisha Barberx	Tricia Clasen	Kristin Plessel x	Stephanie Selvick x
Frank Bartlett x	Janelle Crowley x	Elena Pokot x	Bill Trippett x
Jackie Briggs x	Louann Gilbertson x		

Agenda

1. **Review and approve October 14, 2021 meeting minutes** (handout)

2. **Review Active and Completed Projects**

    a. **Completed** (handout)

        i. **DUO Transition Update** (handout)

        ii. **Touchnet Nelnet transition**

    b. **Active** (handout)

        i. **Office 365 => Next Steps, Emeriti inactive accts** (handout)

        ii. **Additional MS apps (new)**

        iii. **Email template review (new):** This project is to address the email addresses for employees who started at UW-W as students (around 75 individuals). Because one's Net-ID does not change based on role, neither does one's email address except in the case of a legal name change. Shared Governance groups, particularly ASA/Terry Tumbarello would like to see what it would take to have former students have an employee-looking email. Elena explained this is not a simple change--since the established naming condition was a campus decision, her recommendation is that any potential change also be a campus-driven process. There are many approaches and EP will put together a list of options with pros/cons/costs/benefits so campus can weigh the options and decide.

    c. **Jabber to Webex App Migration** (handout)

    This migration will take a mixed and transitional approach in shifting from Jabber to Webex. As you use Jabber, think about what you do and if you have any questions or concerns, let us know. Admissions heavily relies upon Jabber, so will need to work with them on the transition.

3. **IT Security**

    a. **UWSA Policy 1039. Information Security: Risk Management** (handout)

    Once risks are identified, we must decide what to do about them, which need to be addressed, and report to the UW System. Elena Pokot explained the Risk Disposition level was delegated to vice chancellors by the previous administration and we need to reestablish the team.

    An example of an identified risk: the use of administrative rights on computers (why we reduced the number from thousands to a few hundred). With this risk, we shared with the UW System that we reviewed our risk, reduced as much as possible, and now accept the current level of risk.

    Risk can be reevaluated and PCI compliance (2007) is a good example. Previously, we decided not to accept the risk to process credit cards on campus, only do it via phones. Many things have changed since

this decision was made. Several campus units (parking and bookstore) have asked for a review of this decision. Technology has developed well enough so we can replace some phone processing with internet processing. This revised approach is a good example of accepting risk partially and mitigating risk when needed. This new approach for PCI compliance will be given to UWSA.

b. UWW Email Policy language change (handout)

The policy change is to remove language about alumni and has been approved by the chancellor.

c. UWW Workstation Administrative Privileges Practice directive changes (handout)

Kristin Plessel suggested changing the language to " continuing to have administrative risk presents **an untenable** risk" on page 2.

d. Securing Access to UWW network: VPN Posture checking (handout)

Next step, see Action plan of handout page 2 (Recommendations - Remote Access). When joining the UWW network via WiFi from a personal device connection you must have already installed AV software.

Next step after that, with no timeline yet, is instituting similar checking with wired network connection.

e. IT hardware asset purchase process (handout)

Per the UWSA Asset Management policy all campuses must report all IT assets. Anything already purchased through ICIT is on the inventory and doesn't need to be reported separately. Some areas still purchase technology themselves (like UC and FP&M). Elena Pokot explained our next step is to determine how to maintain our inventory. The easiest way is to have ICIT accept all IT assets purchased but not to change how they are purchased. Instead, have them come through us upon arrival, so we can log the assets and then deliver them to purchasing offices. The impact of this approach is small and affects several offices like tech liaisons, Housing, UC, FP&M but not the population at large. ICIT is working with purchasing on this item.

4. IT Continuity of Operations Plan – Discussion (handout)

Action: Elena to change slides to fix email information - it is now in the cloud.

Elena asked the group about the handout: Is everyone comfortable with what we have in place? Are the restoration of service targets appropriate/acceptable? Does anyone have recommendations on how to proceed with assessing risk management/continuity plans?

Frank Bartlett asked about the timeline for SIS, particularly the column that states it would be brought back in 2 weeks. Does this mean operations would completely stop for that time? Elena answered that this is the amount of time it takes to get replacement hardware. While that seems like a long time, the alternative would be to invest half million dollars to have a parallel structure elsewhere so we can return operations in 1 -2 days. We should keep in mind this is the risk assessment, as per ICIT's responsibilities. It is up to campus to determine if this is acceptable.

Stephanie Selvick asked if it is the Administration who will determine if these are acceptable risks. Kristin Plessel noted that we have plans in place to address these outages if they were to occur. Louann Gilbertson stated that business operations need to have 'what-if' scenarios and plans - contingency plans in place and up-to-date to make sure they know what to do in the event of a catastrophic event. Disaster operations are the purview of

leadership - ICIT puts the disaster plan together, but relies upon individual units to plan for disruptions in access to the systems.

Kristin Plessel pointed out that in an emergency situation, the primary focus is on immediate safety, not necessarily daily operations, which would be dealt with after safety is secured.

Frank Bartlett asked if there is information they could put in their department's plan that would address network outages and also asked who is responsible for providing information?

Elena Pokot stated that campus plans need to have a sense of what needs to be done but individual departments must assess the essential functions for their department. She suggests offices ask themselves: which aspects of your operations can be suspended?

Elena Pokot will meet with Louann Gilbertson to determine next steps and what ICIT can recommend in terms of guidance on how individual offices can structure business continuity plans.

Next Meeting? End of February