



Information Technology Committee

February 13, 2025 - 11:00 a.m.

Virtual Microsoft Teams Meeting

Minutes

Opening

The meeting was called to order on February 13, 2025, at 11:00 a.m. by Mr. Matt Smith.

Attendees

Voting Members Present	Non-Voting Members Present
Dr. Mike Reagle	Mr. Cody Bryant
Dr. Julie Baker	Mr. Tyler Farsoun
Dr. Jason Beach	Mr. David Hales
Dr. Thomas Payne	Mr. Will Hoffert
Mr. Matt Smith (Chair)	Mr. Jason Luna
Mr. Braxton Westbrook	Mr. Brandon Walls
Mr. Dan Warren	Mr. Matt Silva
Mr. Eric Brown	MS. Angie Vick
MS. Elizabeth Williams	Mr. John Woodard
Dr. Lisa Zagumny	Mr. Hunter Kaller
Dr. Jeannette Luna	Mr. Allan Jones
Dr. Sandra Smith-Andrews	Mr. Brian Seiler, CIO
Dr. Curtis Armstrong	Mr. David Garrett
	Ms. Rebecca Gooch
Voting Members Absent	Non-Voting Members Absent
Dr. Mohan Rao	Mr. Greg Holt
Dr. Lenly Weathers	
Dr. Susan Wells	
Dr. Kumar Yelamarthi	
Mr. Harrison Simpson	

Approval of Agenda

Dr. Lisa Zagumny made a motion to approve the agenda, and Dr. Thomas Payne made a second. Motion passed.

Approval of Minutes

A motion to approve the minutes of the previous meeting was made by Dr. Lisa Zagumny and seconded by Dr. Julie Baker. Motion passed.

TAF Project Status Update

Mr. Matt Smith started the meeting with TAF Project Status Updates presented by Mr. Will Hoffert instead of Mr. Jason Luna's segment since Mr. Jason Luna had to step away for a few minutes.

Mr. Will Hoffert started by discussing the projects the Provost provided for the 23/24 fiscal year. As seen on the shared screen, all the projects are listed. The Volpe Library Testing Center is a completed project. There are a few that are pending a status update. The Marching Band iPads have arrived and are getting ready and set up. The Dean of the College of Fine Arts identified some questions from the stakeholders about possibly changing a little bit of the scope or extending some of the purchasing for some of those projects. For the biology greenhouse, the location of the greenhouse, which was provided by Dr. Julie Baker and had been identified by the president's office on where the foundation will be constructed, then the RFP in working with the biology office should be going out for quoting and the bid process for the actual greenhouse itself. Mr. Will Hoffert asks for questions.

Dr. Curtis Armstrong asked if the Volpe Library Testing Center was just a refresher of the current seats or if they were increasing the number.

Mr. Will Hoffert responded that it was a refresher of the current seats at identified testing center stations. Mr. Will Hoffert asks for any additional questions. Hearing none, he moves forward to the 24/25 fiscal year project updates. The initial submission from the projects received was around nine projects, with a total cost of around \$500,000 in review with the task spending subcommittee. The initial budget of \$125,000 for college-level projects was approved. They are pending prioritization as the Provost's office identifies additional money. It is not a promise, but they are working on it to see if additional funds can be applied to make up that difference in the budget. The next half-spending subcommittee meeting that Mr. Will Hoffert sees on calendars is on March 13th. They postponed the one on February 6th due to Mr. Will Hoffert's family issues and other concerns. He asked for additional questions but heard none, so the meeting was turned back to Mr. Matt Smith.

Policy 855 and 856 Update

Mr. Matt Smith turned the meeting over to Mr. Jason Luna for the Policies 855 and 856 update.

Mr. Jason Luna said the Ad Hoc subcommittee met and had a lot of excellent ideas that have been implemented into the policy. Some modifications include clarifying points, making the content more concise, and simplifying the policies to be less procedural. Overall, simplification and straightforwardness make it simple and easy to read. This was done for both policies. The subcommittee is waiting for feedback on these policies, and Mr. Jason Luna offers to show the policies off if anyone expresses interest.

Dr. Lisa Zagumny stated she would like to look at the policies.

Mr. Jason Luna asked Mr. Will Hoffert, who was sharing his screen, to pull up Policy 855.

Dr. Curtis Armstrong expressed that he wanted to see the policies as well.

Mr. Jason Luna instructed everyone pulling the policy up independently to use the “simple markup” instead of “full markup” because the policy looks completely different than before, and simple markup is easier to read.

Dr. Sandra Smith-Andrews asked if these policies are in their Microsoft Teams folder.

Mr. Jason Luna said they are in the Microsoft Teams folder for the Ad Hoc subcommittee but not for everyone. He responded that Dr. Jeanette Luna’s hand was being raised in Microsoft Teams.

Dr. Jeanette Luna said that these policies look much improved. She asked if today’s approach is to see if these policies are ready to be voted on in the next meeting.

Mr. Matt Smith said he is glad she brought this up because it is something that he wanted to bring up with the committee. He knows everyone would probably like to push these out of ITC and up to the Administrative Council and try to make that meeting. He wanted to entertain the committee to see if everyone would like to review these policies in a more detailed fashion independently and then possibly put out an online vote so the policies can be moved out of this committee and up to the Administrative Council and not miss the window to get it approved and in front of the board for approval.

Dr. Jeanette Luna volunteered to go first and is comfortable with Mr. Matt Smith’s suggestion. She thought that Mr. Jason Luna taking the policies through Ms. Ellie Putnam was a good practice. She also suggested bringing the policies to Ms. Amy Williams in Internal Audit since she has experience with this subject matter.

Mr. Matt Smith asked if anyone had any concerns about this approach.

Mr. Jason Luna said he does not have any concerns. If the Ad Hoc subcommittee would like to meet again, he will send out another invite to discuss the changes that have been made and ensure that it meets the standard before putting out the final version for the rest of the ITC committee to vote on.

Mr. Matt Smith asked if anyone knew when the next Administrative Council meeting would be.

Dr. Sandra Smith Andrews believed it was March 5th, 2025.

Mr. Matt Smith asked if Mr. Jason Luna could fast-track a meeting with the subcommittee to get this together in a final revision by the middle of next week so the committee could get an online vote so it could go in front of the Administrative Council.

Mr. Jason Luna said that was fine and would have to go through the Administrative Council for approval per the approval chain, according to how the policies were approved. Before, it was ITC approval and then sent to the University Assembly so that it may be an information item for them.

Mr. Matt Smith agreed, saying he thought it was and then would go to the University Assembly.

Mr. Jason Luna said that they could do that.

Mr. Matt Smith said that he could work with Ms. Angie Vick to make sure it was added to agenda items and get that presented in those meetings.

Mr. Jason Luna began to discuss the changes made to Policy 855. The purpose is shorter. The review did not change. The scope didn't change much from what it was previously. A definition section was added so people know what terms mean, and he requested that if anyone finds anything in the document that they want to see added to the definition section, please let him know. He continued by saying that everything else is self-explanatory. Public information is a simple definition, simplified internal information, and confidential and restricted information has more information because they are more sensitive. For sensitive categories, many examples have been provided to give people a better idea of what could constitute confidential and restricted data. Another point that has been added is the roles and responsibilities, which are where these definitions come from. For example: What is a data owner, a data custodian, and a data user, and what are their responsibilities? In Policy 856, references were added to handle each level of information for the data owners and users. A compliance and enforcement section was also added. There was also a request to put everything in a chart format. The chart format is a lot briefer but gets a little cluttered. Mr. Jason Luna left the decision up to the committee to see which one they liked more.

Dr. Curtis Armstrong asked if Mr. Jason Luna could make all of these available so the committee could look at them more conveniently because the screen share made reading challenging.

Mr. Jason Luna agreed that he would send them over as they currently exist to Mr. Will Hoffert to get loaded into the ITC file section.

Mr. Matt Smith circled back to what has been discussed. Mr. Jason Luna would fast-track a meeting to finalize everything to get them on the committee's Microsoft Teams channel by February 21st. By that following Tuesday, all votes needed to be in, whether that means a thumbs up or down, so it could be moved on to the Administrative Council, which is meeting on March 5th, according to Dr.

Sandra Smith-Andrews via Microsoft Teams chat. Then, it can go from the Administrative Council to the University Assembly's agenda to get these approved, and then the Board of Trustees could review these items in their June meeting. This should give everyone ample time to review the items as a committee. It passed Friday, Monday, and the weekend to review the materials. Then, a vote was taken the following Tuesday, the 25th. He asked Mr. Jason Luna if he was good with this.

Mr. Jason Luna confirmed that he was good with this.

Mr. Matt Smith asked for any additional discussion regarding this agenda item. He heard none, so he moved on.

Enterprise and Microsoft Teams Applications Update

Mr. Jason Luna started the conversation by discussing Read.AI joining meetings and summarizing meetings across campus. It is realized that this is not just a Microsoft Teams issue. This is because these are enterprise applications within the Office 365 environment. As Office 365 has gained popularity, the number of third-party vendors offering federated sign-in has also grown. Federated sign-in is seen when a website asks the end-user to sign in with their Google, Facebook, or Microsoft accounts. Many websites are increasingly accepting Microsoft as a federated sign-in, and Tennessee Tech University users could, when they are logged into their Tennessee Tech University account, click "Sign-in with Microsoft" and pass through after accepting some permissions. Included in the screenshot on the screen is what that permissions screen looks like, and most people click accept and go on about their day. It was realized that there is a considerable enterprise application catalog of services that are not approved, and some of the permissions are a little disturbing. The question of what access is being given to these applications remains.

Mr. Jason Luna shared his screen showing the application list. Currently, there are 984 applications, and that list grows exponentially. Within the last week, there had been five new application registrations. Some additional questions are as follows: What is being talked about here? What is being looked at mainly? The answer was permissions. One application that had disturbing permissions is TeamForms. Currently, users can give consent to access their data. This becomes a problem, and issues arise for permissions that TeamForms requested. For example, permissions to create, edit, and delete items and lists in all site collections, like SharePoint. Microsoft Teams operates on SharePoint. So, this application could create, edit, and delete items in SharePoint lists or Microsoft Teams folders for whoever granted it access. The following permission is to read items in all site collections. So, everything that exists can be read, it is enumerated, and that data is stored in unknown locations. TeamForms was not an approved application. ITS has no information and has never gone through the SDSRF process but has access to Tennessee Tech University information. It is scary because this person had given this application access to much information. If they have access to it, this application has access to it. What is wanted to be done is to have the ability for users to not consent without it going through a review process for anything unapproved. That is what was being looked at. Mr. Jason Luna asked for any questions.

Dr. Jeanette Luna said that she had questions. On the screen Mr. Jason Luna was showing, she saw Adobe was on the list, which many users utilize, and an SDSRF is already in place. She assumed there would be a list of acceptable Microsoft Teams plugins because they are already deemed safe. So, there seemed to be a nice learning opportunity here for faculty because many users clicked

through the permissions. As ITS goes through the process, it would be great if they could communicate to the faculty and staff by providing a heads-up and saying that around 800 applications are accessed through Microsoft Teams. ITS will be removing permissions for those applications, and here is why. There have been meetings in which Dr. Jeanette Luna has discussed sensitive information, and Read.AI was added to the meeting. She thought that AI should not be in the meeting since sensitive information was being discussed and that information should not be fed back to any large language model. She thought that people adding it to the meetings understood that. So, asked ITS to consider this a nice learning opportunity for the campus.

Mr. Jason Luna circled back around to Adobe in Microsoft Teams. He brought up his screen and showed an Adobe application that had been added that morning. It is a newer application that does not have a homepage URL and is potentially a rogue application. The concerning thing about this one is one of the permissions is user impersonation. It can access protected content for users. This is a rogue application, and it is not the real Adobe. The real Adobe has a homepage URL and much more information about the product than the one just created. People have clicked through things that are not real and given permissions to rogue applications.

Mr. Matt Smith said there were more questions and had Mr. Brandon Walls talk first since he first raised his hand in the Microsoft Teams meeting.

Mr. Brandon Walls wanted to add more to Mr. Jason Luna's words. He said that their Microsoft Teams, Systems, and ISO worked together on this. The Systems team manages the integrations and some permissions while working with Mr. Jason Luna's team to manage the security side. Mr. Brandon Walls wanted to point out that there are a couple of different Adobe products with enterprise agreements, which creates some additional things for account provisioning. It is a bit complex, but the main thing is that user impersonation is serious. It will allow an application, even a legit application, to do anything on behalf of the user. It can read their e-mails or act as that user. So, when looking at these applications, some of this is a matter of determining if that level of access is appropriate for that kind of application. These are some eye-opening things, and they have only recently been uncovered. Mr. Brandon Walls continued by saying that Tennessee Tech University has been a Microsoft Office 365 customer for over a decade, and Microsoft will not come in and start tightening the controls for Tennessee Tech University. ITS will have to evaluate these applications methodically. These 900-something applications represented both legitimate and illegitimate applications. So, part of the difficulty of this is determining which are legitimate and which are not, and which ones are universally authorized and which ones are not. It could potentially be disruptive, but Mr. Brandon Walls appreciated the earlier comment about the communication. How this is communicated to campus will gain an understanding of what is trying to be done. It is important to be perceived that ITS is not trying to shut down any valuable tools. For example, Read.AI. This one has been asked to be blocked, but there are options for Read.AI if the proper channels are followed. An enterprise version of this application gives Tennessee Tech University the data governance that allows control of the data. In those cases, it may be possible to provide access to these again. The main goal is to button up the hole in the process. To ensure that folks do want access to these tools, they go through the proper process so that ITS can vet the application and properly onboard it for use with the campus.

Mr. Eric Brown wanted to add a few things to the conversation. Starting with that, he appreciates the people going through this process and looking at this because, from a cyber standpoint, this is the leakiest part of the organization right now. The tools are excellent and provide a benefit, but what is being given away very quickly for the convenience of a quick report was scary. Mr. Brandon Walls touched on this, and what Mr. Eric Brown wanted to ask was tampering with budget constraints and all other constraints that are on any of these efforts if Tennessee Tech University could also look at whatever it would take to establish the data governance so that we did have access to a model in-house that could provide those supports like Dr. Jeanette Luna was mentioning. Chat can help rework things. What can be done is provide a safe, Tennessee Tech University-governed resource to provide some of those utilities to provide meeting summation utilities, but in a way that could stay in-house. The tools are needed, and the tools need to be helpful, but on the other side, some of the permissions on these tools are horrifying. Mr. Eric Brown thanked everyone for their efforts in this. He also asks if the costs for those models could be looked at. What would it take to bring that resource inside because of budgetary constraints? If nothing else, would it be possible to get a model online in-house? That way, it is at least known the in-house model is not being influenced by whatever inflows and outflows there may be. The tools are helpful, so it is essential to find a way to accommodate that, but the purge needs to happen sooner rather than later because everyone has seen that some amazing holes will have to be dealt with.

Mr. Jason Luna responded by saying that, working with Mr. John Woodard, a message went out later that day or the following morning regarding that, and one of the things that is part of that is a tutorial on how to use the already built-in Microsoft Teams functionality to do precisely what Read.AI is doing. There is a data processing agreement with Microsoft regarding data privacy for using the tools within Microsoft Teams. So, an alternative for Read.AI, Fireflies.AI, and other tools that do meeting recordings, transcripts, and summations, Microsoft Teams does it natively. There is a tutorial that will be part of that message that will walk people through using the Microsoft Teams tool.

Dr. Jason Beach apologized for showing up late and asked if his question had already been answered. His question is whether these are applications installed through the Microsoft vetted store, side-loaded applications, or both.

Mr. Jason Luna said these applications, the enterprise applications, which are shown on the screen, can be both. He continued by saying that some of them may have a client and some may not, but these have been added via federated sign-in.

Dr. Jason Beach asked if Mr. Jason Luna has a split by software that has been added through the Microsoft Store versus the ones that have been sideloaded.

Mr. Jason Luna said there is a list of applications that have been registered. And these are all Tennessee Tech University applications that have gone through the process. So, it has been identified as an enterprise application. This is what has been done: Application registrations and enterprise applications come in via federated sign-in.

Mr. Brandon Walls jumped in and said some of these 900-something applications are also our single sign-on registrations. So, that number is a little smaller. There are about 120 or so authorized single sign-on applications. Some of these applications start with a "TTU-." These are added to the name because Microsoft threw all the applications into the same list. So, it helps everyone distinguish these applications.

Dr. Jason Beach asked if Microsoft's process of vetting programs is being considered in this process.

Mr. Brandon Walls said some settings allow ITS, as things are tightened down, to establish consent rules that say if it is a verified Microsoft application, here is the consent and permissions that ITS will allow for just those applications. The downside to this is that if every permission is needed, it will force an admin consent request, which ITS will get an e-mail saying this person wants access to this application and, of course, could generate a lot of traffic in this regard. So, the stance is that nothing gets user consent when ITS gets where they want to be unless it is an approved application, in which case ITS will go in and grant all that consent from an administrative standpoint. So, there is no opportunity for the users to think about it. There is the vetted application, and ITS knows what permissions it needs. ITS would grant that on behalf of the university, and then that gets everyone out of these users who are making that decision stance that is currently happening.

Dr. Jason Beach asked if the vetting process that ITS will use will align with Microsoft's vetting process or if ITS will use one of its own.

Mr. Brandon Walls assumed this would be very akin to the SDSRF process, and the applications would be viewed like any other application. It is not so much a Microsoft alignment. If most of these applications are legitimate and well-established, like Adobe and even Read.AI, they may be recognized as legitimate applications and have been validated by Microsoft. The question is whether Tennessee Tech University has vetted it if it meets requirements and passes all the checks, and if they have security reports. Are there options to manage the data, and does it have single sign-on? It is possible to stop others from using Tennessee Tech University credentials from signing up with the free editions that don't have all the controls. So, part of the process is to identify ways of onboarding these to align with the existing software management policies. The vetting process would kind of align with what is currently being done for other software.

Mr. Jason Luna asked Dr. Jason Beach to clarify what he meant when he said the Microsoft review process and what exactly is being referred to.

Dr. Jason Beach asked to submit a software client that could be as used as a plug-in for Microsoft Teams. It would go through some sort of vetting process to be on the Microsoft Store, just like Apple has a vetting process. Microsoft has a vetting process, too. What Dr. Jason Beach was trying to delineate is whether Tennessee Tech University is going to stick with the established vetting of these companies or if will be done in-house.

Mr. Jason Luna said just because something is in the App Store does not mean it is safe. ITS will not rely on Microsoft to tell them something is secure. What ITS is concerned about is the

permissions that a user grants the application, and Microsoft does not care about that. Microsoft can say this application is secure and they have done the right things to be in the store, but the end-user can still give permissions. ITS does not want to provide the end-users with the ability to have an application impersonate them, which is one of the permissions an individual can grant. So, ITS is trying to walk back the permissions that a user can grant an application. Not necessarily the use of the application or knowing that the application is safe. The level of access these applications have to Tennessee Tech University data is trying to be controlled. Just because the application is secure does not necessarily mean the permissions are not crazy.

Dr. Jason Beach said that currently, users have unfettered access. What is being said is that ITS wants to look at the preferences and be able to restrict those based on the user, but not necessarily restricting the applications.

Mr. Jason Luna said this statement is correct. He continued by saying that if the application has gone through the process and ITS has a data privacy agreement, ITS will use admin consent to specify what the application has access to. The user will not be presented with any other options. They will not have the ability to agree to anything else.

Dr. Jason Beach thought this was a good move, but from his perspective and the end-user side of things, it is hard to know exactly what software can do without being able to install it first. That is an issue that is commonly experienced. Before an SDSRF is submitted, many faculty members have talked to him about not going through the process if they do not know if the software will work for their class or if it is as robust as initially thought.

Mr. Jason Luna was glad that Dr. Jason Beach brought this up because, once ITS strips Read.AI from the enterprise application, nothing restricts the ability of end-users on campus from going to Read.AI and signing up with their personal account. Nothing stops them from going to the website and signing up, but what does not want to happen is signing up with their Tennessee Tech University account that gives an application access to Tennessee Tech University data. They can still use the application, whatever it may be, with their personal accounts.

Dr. Jason Beach said that it was great and really answered the questions because this was something that he did not know the answer to when speaking to faculty members when they wanted to try these technologies out. He was unaware that on-campus faculty members could use their personal e-mail to test and try out. Dr. Jason Beach also wished to congratulate ITS on finding parody, which was discussed earlier with Microsoft features that emulate what Read.AI does. It is fantastic to show faculty, staff, and students that the software can do what they are asking it to do already, and in many cases, it may be more streamlined. He thinks providing opportunities and parity for the software people ask for is very helpful.

Mr. Brandon Walls chimed in to add some clarification. This is not restricted to apps in the App Store or their Microsoft Teams plug-in type applications. Currently, Team Apps must be approved. Those are already locked down and it has never been opened, but if you go to any random website that offers some sort of productivity tool or whatever, not necessarily in the Windows Store or the

App Store. It could be any application that supports this integration with Office 365, and as soon as someone attempts to sign it, that is where it does that. So, it could be any application.

Dr. Thomas Payne expressed appreciation for a prior discussion, emphasizing the need for clarity in processes related to application approvals. He suggested that having a streamlined communication channel or a flowchart could reduce confusion around application access, particularly for faculty members. He acknowledged the importance of understanding why certain applications require specific permissions and believed improved communication could alleviate the volume of inquiries arising from misunderstandings. Additionally, he pointed out that while the technical aspects of application management may be straightforward, the cultural adaptation to these processes remains a challenge.

Mr. Jason Luna said that Mr. John Woodard had shared the self-help article. So, the knowledge base article shows how it can be done in Microsoft Teams. What is not being shown is the AI summary, which is Copilot, which is part of Microsoft, and Tennessee Tech University has a data privacy agreement. When talking about these applications, ITS must be able to define what level of access is being given to them.

Dr. Thomas Payne asked if ITS does that. In other words, if ITS is getting all these hits, is there a good feeling of how many of them are coming at ITS? Once vetted, are those on a list and cleared from administrative approval?

Mr. Jason Luna said not at this moment. He said that because right now, no restriction is in place to prevent people from signing in with their Tennessee Tech University accounts. So, it will not be known until that functionality is turned on. The first step in the plan is to stop allowing user consent for application registration across the board. ITS will have a better idea of how to answer that question better once that step is taken. The next step is to review the current permissions of the currently used applications. If only very low-level access is requested, for example, reading a user's email address, enabling sign-in, or other low-level stuff, that is not really concerning. After that, permissions will start getting walked back to those that make sense for those applications.

Mr. Brian Seiler said that the objective is to limit the permissions of specific applications utilized by Tennessee Tech personnel in meetings. Despite efforts to block these applications for staff, there remains a possibility that they may still appear due to external entities or collaborations with different organizations. Testing will be conducted to assess the effectiveness of these blocks. Ultimately, the goal is to ensure that any applications present in meetings do not have permissions granted by Tennessee Tech users.

Mr. Jason Luna said the discussion revolved around assessing and identifying current permissions associated with specific applications to mitigate potential security risks. It emphasizes that while the applications remain accessible, users cannot log in using their Tennessee Tech credentials. The messaging will clarify that users cannot access specific applications with their account, explicitly referencing the domain.

Mr. Brandon Walls discussed the implementation of restrictions regarding user access. He emphasized that three steps can be taken once user consent is no longer allowed. First, access could be entirely blocked, prompting users to contact an administrator for permission. Alternatively, users might be allowed to request access through a pop-up message along with a justification for their request. However, there is concern about potentially overwhelming workloads if the number of requests becomes too high. He suggested the importance of monitoring these requests to understand their necessity and indicated that several individuals could be assigned to process approvals or denials. The overarching goal is to prevent unauthorized access from third-party applications.

Dr. Thomas Payne asked Mr. Brandon Walls if ITS has the granularity to grant access but not specific permissions. In other words, if there are a lot of requests for a particular application, could ITS say the application is acceptable, but the permissions are not, and would they be able to block that on a more wholesale basis?

Mr. Brandon Walls understood what is being said when an application requires specific permissions—labeled as A, B, C, and D—upon signing in, users must either grant these permissions or request approval from an administrator. Failure to obtain the necessary permissions could result in the inability to use the application entirely. The impact of denied permissions varies by application; for example, certain functionalities, such as access to a calendar, may be essential for the application to operate effectively. Ultimately, granting individual permissions may lead to the application becoming inoperative depending on its requirements.

Mr. Matt Smith warned that five minutes were remaining and highlighted the importance of housekeeping items. He reminded attendees that Jason would share policy documents (855-856) on the team's channel for review before the upcoming vote on Tuesday. He also invited participants to propose agenda items for the next ITC meeting and emphasized the necessity of submitting those items two weeks in advance for adequate preparation. He underlined the importance of effective communication during changes to ensure everyone is informed and engaged. Mr. Matt Smith encouraged members to reach out with any additional items for discussion or questions.

Dr. Jeanette Luna had a question for Mr. Brian Seiler. Staff evaluations and things like that are coming through now. She knew that many department chairs wanted to ensure that kudos are given to their Tier 2 support people, but there is no suitable mechanism to provide feedback for Tier 2. Tennessee Tech University has this significant support for its college. Still, they have not received anything other than the considerable administrator evaluation that went out in December. She asks if ITS could consider collecting some of that feedback so she can brag about people other than her faculty.

Mr. Brian Seiler said that Mr. Will Hoffert and Mr. John Woodard are over the Tier 2 support staff. They would certainly look at something like that, which is very much appreciated. Positive feedback is always great, and any feedback is valuable.

Mr. Matt Smith asked for any additional questions.

Mr. Braxton Westbrook had a brief question about TAF applications. He asked if a form or website portal exists to submit those whenever that cycle opens.

Mr. Will Hoffert said there is a form that gets filled out and that work is done with the Provost's Office, the Deans, and the departments to put in the requests for proposal.

Mr. Braxton Westbrook asked if Mr. Hoffert could share where to find that form.

Mr. Will Hoffert said he will try to get that posted in the ITC.

Adjournment

Mr. Matt Smith asked for a motion to adjourn at 11:59 AM. A motion to adjourn was made by Dr. Lisa Zagumny and seconded by Mr. Braxton Westbrook. Motion passed.

Minutes prepared by Tyler Farsoun