

# WSU ITSAC MEETING - Minutes - approved

## MEETING INFORMATION

---

**Date:** October 13, 2020  
**Time:** 1:00pm – 3:00pm  
**Location:** Zoom

---

### 1. Public Records Office process summary / email retention and discovery

*Alicia Foth, Public Records Coordinator*

Next request portal - intake for public record request

- Process begins - request is submitted through the Next Request portal which is the intake for public records requests. Request is reviewed, Public Records Office reaches out to departments who may have the records, additional parties may be added, and due date is given. Once records are received by the Public Records Office, they are reviewed for completion. Redactions may be added. Once processing of the records is complete, the documents are released to the requester and the file is closed.
- Record holders search, gather and submit records independently
- Record requests for former employees are directed to their former department
- Departments are responsible for transfer of records when an employee moves departments
- ITS email retention process was discussed. There is no specific email retention schedule but rather a document retention schedule which can be found at the following link:
  - <https://policies.wsu.edu/prf/index/manuals/90-00-records/90-01-university-records-retention-disposition/>
- Deb Bartlett will join Alicia Foth at the next ITSAC meeting for further discussion
- Training - Skillsoft 4 times a year - Instructor Led Training (ILT) by Procedures, Records and Forms: **Business Policies, Procedures, and Records Retention** with the next session on November 19, 2020 from 9:00-10:30 am.
- A subcommittee will be put together with the appropriate stakeholders including ITSAC members, Alicia Foth, Deb Bartlett, HRS and ITS. Tom Ambrosi will facilitate this process. Michael Case, Bryan Valley, Bill Rivers, would like to be involved.

### 2. Welcome and Approval of 08.27.20 minutes - APPROVED

*Sasi Pillay*

- FEM MEM update - process went as planned on time and as expected (Todd Weston)
- Current security threats and phishing emails will be added to the next ITSAC agenda (Michael Walters)
- ATOs requested ITS to investigate file services and will be added to next ITSAC meeting

### 3. Site Licenses

*Greg Neunherz, Dawn Barnard*

- SPSS is 98% done
- SAS emails will be sent out to the area level. If they do not respond, Sasi will connect with the Dean of that area.
- Matlab - Sasi is in conversation with Dean Mary Rezac, Department of Engineering, and will bring back to ITSAC a summary of the discussion

### 4. Data Governance Council

*Sasi Pillay, Fran Hermanson*

- Fran Hermanson and Sasi are working toward getting data stewards together for the Data Governance Council
- Council will deliberate on projects and data from across many different systems
- There is a group in place for the Workday piece, including: HRS, Payroll and Finance
- Greg Crouch has been given a copy of the presentation
- We have clearly defined projects we can attach the data group council to but need support from the top levels

## 5. MFA

*Tom Ambrosi, Todd Weston, Dan Hamilton, Greg Neunherz, Sasi Pillay*

- Greg has received concerns from numerous stakeholders and areas regarding the token and the time out.
- October 29, 2020, 8pm, MFA will be turned on for Outlook, Teams, etc.
- Sasi agrees that we could delay the October 29, 2020 date if necessary
- The token lifetime will be changed to 24 hours to align with OKTA
- There is no warning that the authentication is about to expire. After session expires, notifications do continue.
- 24-hour interval perspective was chosen for personal devices. An environment on a WSU device could be extended.
- There was discussion about an exception for a longer time. is there a process for that and if so, what is it? - There is a normal policy exception process and certain classification of users there is a 72 hour that will supersede the 24-hour group. The scope of this group is not specified.
- Are executive level exemptions allowed?
- February 5, 2021 - make sure all clients connecting to Office 365 compatible with a MAM solution protecting data and support OAF. We can still exempt people from OAF and MFA but later in 2021 Microsoft will disable OAF and it will no longer work.
- Are we deploying MAM as an opt-in or is it university wide?
- The messaging going out is telling people that their devices will not work after the date of Oct. 29. To avoid any potential issues, users should switch to a supported version of the client.
- How do MFA and MAM work together? What is that experience going to look like?
- MFA schedule was decided prior to MAM. We do have duplicate controls. We need to take a look at a cumulative control before final decisions are made.
- MFA policies are able to affect users in groups not applications
- The device policy would require an authorization on the device. The problem that we run into is that the data is secure but not if the device is not secured. MAM enforces on the device that the device must be locked. Mam builds a secure enclave on that device and any WSU data is within that enclave. When needed WSU can delete that data enclave..
- MAM in consideration, does it impact the 24-hour token? Do they work together? Why 24 hours? How do we provide support availability and users who are locked out especially after hours? The point about the extra support load on Crimson Service Desk for MFA resets cannot be overstated. The eventuality of this issue will be discussed.
- Grouper - currently generating license groups for all required and being pushed through Office 365 now. We are validating the groups and will then institute the license migration. More definitive answers soon
- Email is the only official correspondence students are allowed to have with faculty. We do not want to cause student email disruption.
- Faculty has been using Gmail for official notification. Rules are in place but not enforced.
- PINs and biometrics are "easy". MFA and passwords are cumbersome.
- Can we not propose / mandate a policy that "If you're going to access WSU data from your personal device, you must have a PIN?"
- The global policy can't be relaxed per application, but we can have a more generous policy and make stricter policies on specific application
- Communications have been sent to end-users, causing unit issues especially with Clinical Faculty
- We need a good understanding of the end-user experience and what that looks like. Keeping communications simple and short and directed toward certain constituent groups would be helpful.
- Can we get a brief summary pushed out to the wider community regarding the October 29, 2020 and the February 5, 2021 change? Some pushback is based on misunderstandings which necessitates getting clear messaging out asap.
- More information and communication are requested to assist in preparing the end-user
- Sasi encourages further feedback related to communication be sent to Jacqueline Southwick
- Laxing the global and tightening on applications is a good idea and solution
- If there is any assistance needed, anyone in this meeting will assist, help and participate
- Sasi will get the MFA/MAM teams together to discuss issues
- Sasi will re-look at the support issues

6. Other:

a) **Malwarebytes -**

*Greg Neunherz*

- Many areas are interested in Malwarebytes for remediation tools which are needed and not provided by Palo Alto
- \$22,000 annual cost for Malwarebytes remediation piece that could be of huge value
- Tom Ambrosi will investigate Malwarebytes and ITS will facilitate the discussion

b) **ITS 2020 Annual Report**

*Sasi Pillay*

- Provide comments regarding the ITS 2020 Annual Report to Jacqueline Southwick
- <https://its.wsu.edu/documents/2020/10/its-ar-final-web-v1-2020.pdf/>