Information Technology Council
Steering Committee

DIVISION OF INFORMATION TECHNOLOGY

Information Technology Council Steering Committee Minutes Summary		
Date: November 10, 2021	**Time:** 1:00pm-2:00pm	**Location:** Virtual - Zoom
Type of Meeting: (Face to face, phone) Virtual	**Duration:** 60 minutes	**Please Read:** Minutes from 10/18 Meeting Minutes from 10/18 Meeting (S) **Please Bring: n/a**

List of Invitees: Derek Richardson (Chair), Jeffrey Hollingsworth, Marcio Oliveira, Axel Persaud, Gerry Sneeringer, Joseph Gridley, Philip Piety, Yifei Mo, Mary Shelley, Julie Wright, Jim Zahniser, Jack Blanchard, David Dahl, Peter Keleher, Lisa Petersen, Jonathan Resop, Hallie Oines; Eunha Yim; Melissa Dressler

Topic / Agenda Item	Description	Lead, if relevant
Welcome, Introductions and Approval of minutes	Welcome and introductions. Motion to approve the minutes and seconded. No objections, no abstentions. Minutes approved.	Derek Richardson
Privacy Policy Draft Review	The Senate tasked the IT Council with creating a privacy policy for the campus. There is no current policy that sufficiently covers this area. UMD hired a Chief Privacy Officer, Joseph Gridley, who has been working with the Security Working Group on the creation of the policy. Would like to vote today on the policy, if possible. Any minor changes can likely be approved here, but any major modifications would have to be discussed and approved at a future meeting. Joe provided an update on the process of creating this policy. It outlines our responsibility for maintaining privacy as stipulated, but also outlines the expectations of privacy for data on campus. All of the data activities on campus will be covered by this policy, regardless of the person's position in relation to the university. This policy also covers data received by a 3rd party source. Principles include respect, equity, transparency, and responsibility. The degree to which we provide individual notice when data is collected and/or used needs to be defined. It will be a living process because there is no practical way to do this every time data is collected and used. We can be transparent with the usage of data by providing links on pages visited (dashboards) to access a privacy statement around that page, but need to clearly outline that we won't have a way to notify individuals each and every time that occurs.	Joe Gridley

	This group is being asked to provide feedback as to the implementation of this as email may not be the best way to communicate with people. Most people receive a large volume of email from the University and tend not to read them all explicitly. Having a way to view how data is being used is ideal without over-communicating. Currently, the process to provide this data to an individual is manual, arduous and not necessarily fully accurate. Questions: Should we better outline the information that the system holds, versus information that the individual holds? E.g. LinkedIn. Profiles are not collected by the University, but are connected. This is where the applicability may come into play. There may not be any direct interaction with the data by the University, but the University may use that information. There is also potential for a bad actor to use the information because of the engagement of third party access to data. This, however, really would not be carved out in the policy, but rather developed in a standard that is written as a result of this policy. One standard that will be issued very quickly after this will define the expectations and responsibilities should there be a need to access data by organizations involved in a legal investigation. The first round of standards will involve misconduct investigations, use of institutional data for research, privacy expectations and engagement of 3rd parties. All standards are reviewed in IT Council. If we want to make a publicly available directory, it would go through a privacy impact assessment process to examine the sensitivity of the data and the risk to the individual should data be collected. These are risks that we would assess at the same level of the security review. We will not retroactively apply the new policy to things that already exist. As part of the launch of the program, we will be outlining the data elements that are available and will conduct a “red flags” review. If only name and contact information is available, it is not going to raise red flags. If, however, it also lists other, more sensitive data, that will be more problematic. Data classification work becomes essential at this point. From a communication perspective, how will people address concerns that they may have? Several forums were held to request feedback. Would like to have some standards that can be issued in congress with this release of the policy that outlines some of the possible use of data so that the community has an expectation up front at the time of the policy implementation. Opt out information has been requested as an option right away. Standards will be written once the policy is approved. Will an FAQ be developed similar to what we did with the Email Standard? Yes, this is absolutely appropriate. There are links that will be placed where existing placeholders are that will include what is	

	developed as a result of these discussions as well as those from the Senate. Some concerns were raised relating to violating policy - there are well defined procedures within the campus for students, faculty and staff that would also address these privacy issues. There is a gray area when it comes to knowingly violating the policy. Unit head responsibility is listed in the policy. This is not intended to address a faculty member who purchased software without going through the approval process. It is really meant to address whether a unit head or director has approved the purchase of a software or service despite violating the privacy policy. This will be a judgment call ultimately within the current adjudication processes. The remaining hot button is what the expectation of privacy is. OGC thinks granting any expectation of privacy renders them unable to access data for investigative purposes. The other perspective is that all data should be held private. The statements in the policy was the attempt at balancing these polar opposite perspectives. This would be another place where an FAQ would be helpful. This is the first topic that will be addressed by a standard. No further discussion. Motion to vote on the policy as written provided and seconded. All in favor - Role Call Vote - Passed If this committee would be willing to review, by email, a draft FAQ before this goes to the Senate it would be greatly appreciated.	
	All other agenda items will be addressed during the next meeting as time has expired.	
Other Topics	None	
Adjourn	Meeting adjourned at 2:00pm	

Information Technology Council
Steering Committee

Action Items (rolling list, update each meeting)				
Action Item	**Status**	**Notes**	**Due Date / Revised Date**	**Lead/Assigned To**
Add investigation of appropriate technology to provide secure high speed transmission of HPC related files.		Added 09/20		Jeff Hollingsworth

Attachments/Notes: