Information Security Working Group Report

During the summer of 2019 an ad-hoc Working Group met to discuss the state of the University with regard to the protection of confidential information and compliance with Federal and State laws regarding record storage and information security. Working group members included:

- Michael Raymer (WG Chair) – Department of Computer Science and Engineering
- Sheri Stover – Department of Leadership Studies in Education and Organizations (Chair, Faculty Senate Information Technology Committee)
- Craig Woolley – Chief Information Officer
- Michael Natale – CaTS
- Kenneth Coon – CaTS
- Tom Rooney – Biological Science
- Laura Luehrmann – School of Public and International Affairs (Faculty President)

This WG was charged examine current university practices and policies with regard to protections of student records required under the Family Educational Rights and Privacy Act (FERPA) of 1974. Among other tasks, the WG was asked to "work with CaTS to identify (and make appropriate recommendations regarding) technologies, platforms, and best practices as they pertain to convenient and secure storage, sharing and communication of confidential and protected information (including both FERPA and HIPAA related information). Recommendations should specifically address storage and communication of protected information via University and non-university owned infrastructure".

Several potential areas for action were identified by the group, including:

1. Development of clear guidelines for determining what information is confidential and/or protected, including FERPA and HIPAA (Health Insurance Portability and Accountability Act) protected data, financial information, and other student records.
2. Ensuring University compliance with state and federal regulations regarding records retention, storage, and security.
3. Development of clear and actionable guidelines for storage and communication of protected information.
4. Providing enabling technologies to facilitate secure storage and sharing of protected and confidential documents and records.

5. Establishing institutional infrastructure and practices for ensuring clear and timely communication between faculty, staff and the University administration regarding emerging IT threats and changes in security practices, policy, and technology to address them.

The unanimous recommendations of this group include:

1. That CaTS continue to develop and deploy a SharePoint/OneDrive based system to complement or replace FileLocker in allowing faculty, staff, and administrators to store and share confidential and protected information in an efficient and secure manner. Training and education on these platforms will assist in their efficient and effective use.
2. That CaTS develop additional training materials for faculty and staff in identifying and protecting confidential and protected information. This should be WSU-specific, highlighting what can and cannot be shared in Pilot, via email, etc., and should include multiple modes of delivery. Simple and accessible guides similar to the “Appendix: Permitted Data Usage by Service” table (https://www.wright.edu/information-technology/policies/data-security-compliance) would be welcomed.
3. That CaTS and the Faculty Senate IT committee work together to develop mechanisms and practices for ensuring that security announcements, policies, and training are broadly and effectively communicated to faculty and staff.
4. That the Faculty Senate (via the IT Committee) work together with the University Administration (via CaTS) to identify a body of faculty and/or staff in each college that is responsible for ensuring that security-related announcements, training, and software are effectively communicated to the college faculty and staff, and that concerns, questions, and requests from faculty and staff are effectively conveyed to the appropriate CaTS personnel. One model for this that has proven to be effective for the College of Education and Human Services is the formation of an ad-hoc technology committee to serve this purpose.
5. That CaTS and the Senate IT committee continue to work together to ensure that the University is in compliance with federal and state records retention regulations and laws. Possible actions to discuss include keeping a copy of all forwarded emails on university servers, the deployment of Data Loss Prevention software, and automatic archival of email records.