MICROSOFT TEAMS TIPS & TRICKS

The following document provides a few guidelines for ensuring a secure experience with **Microsoft Teams** that you create and manage.

TIP 1. MEMBERSHIP IS A PRIVILEGE

Only add people into your Microsoft Team who truly need access to the group. To ensure that your **Team's** files, data, and work are secure, start by limiting Team access to those whom you trust with all of this information. Anyone in a **Team** has the capability of sharing anything to which they have access.

TIP 2. ENCRYPTION DOES NOT MEAN SECURE

Although Microsoft Teams encrypts files that are shared through the app, you should still keep sensitive data as secure as possible. When sharing sensitive data (student information, grades, personal info, etc.), **use a secure service such as FileLocker to host/share these files**. FAU users have FileLocker accounts accessible via **https://filelocker.fau.edu**

TIP 3. TEAMS ARE ONLY AS STRONG AS THEIR WEAKEST LINK

In MS Teams, it is possible to attain a link that grants a user access to a particular Team or Channel. Inviting people to your team or meeting via a shareable link may seem quick and easy, but remember that this link can be posted anywhere by anyone. **Avoid using links as invites to Teams, Channels, etc.** If you need to add someone as a temporary member, use the usual process to manage team members and limit their access to a **Guest** role.

TIP 4. SECURE THOSE INVITES

Keep in mind, once a meeting has started and invites have gone out, there is no way to prevent these invitees from rejoining if they get removed/kicked from the meeting. **Make sure that your invitees comprise only of people who absolutely need to attend this meeting**. Although users can be removed from a meeting, they will be able to rejoin if removed.