Eastern Michigan University

<u>Technology Resources for Working Remotely</u>

Effective Monday, March 16, 2020, EMU instituted a policy that all EMU employees who have not been otherwise informed or designated by their supervisor will be expected to work remotely until further notice.

University email is the official form of communication for all EMU employees – so all EMU employees are expected to monitor it for updates. Please also continue to check EMU's COVID-19 website for further information and updates.

EMU IT has numerous resources available for working remotely.

1. **AnyConnect VPN**. VPN is a secure connection required to access some EMU systems like Banner, WebXtender, and the Z: drive. (NOTE: VPN connections require Duo authentication, but a Duo prompt does not display on the page.)
    a. Request VPN access
    b. Installing AnyConnect VPN (Windows and Mac)
    c. Connect to the EMU network using VPN *("https://www.emich.edu/it/network/vpn.php")*
    d. Mapping the "Z" drive.

2. **University Licensed Software**. Employees are eligible to install certain software (like Microsoft Office) on their personal computers free of charge. Please refer to IT's University Licensed Software page for details.

3. **Google Hangouts Meet** (meet.google.com) Initiate, or participate in, video meetings with others

4. **Google Hangouts Chat** (chat.google.com) Send and receive instant messages between individuals or a group

5. **Google Drive** (drive.google.com) Access your files from anywhere

6. **Jabber** Jabber is a softphone (software phone) application that you can use to make and receive phone calls from your computer as if you were using your campus phone.

7. **Managing VoIP Calls and VoiceMail**
    a. Access your voicemail messages from anywhere
    b. Request access to forward your VOIP phone to another number (must have physical access to your VoIP phone to complete this request)
    c. Receive voicemail messages via email

8. **Zoom** (emich.zoom.us or within Canvas) Similar to Google Hangouts Meet but with additional functionality like breakout rooms, waiting rooms, and whiteboards. Instructors who wish to use Zoom for delivering course content are encouraged to use Zoom from within Canvas. Individuals who already have a personal Zoom account registered with their emich.edu email address are encouraged to login at emich.zoom.us to convert their account to a University licensed account. More information about using Zoom and securing your Zoom meetings can be found on I.T.'s Zoom Video Conferencing page.

Securing your Zoom Meetings

Zoom has received a lot of media attention related to security issues. While Zoom is working to address these issues, there are a number of things you can do to secure your meetings from uninvited guests.

- Request that participants refrain from posting your meeting link in public forums or on social media. If someone has the link, they can join your meeting.
- Familiarize yourself with Zoom's settings and features.
  - The Waiting Room feature allows a host to control who joins small meetings.
  - Enable the "*Require a password when scheduling new meetings*" setting. This automatically adds a password to the Zoom meeting invitation sent to each invitee.
  - Allow only signed-in users to join. If someone tries to join your meeting but is not logged in to Zoom using the email address on the invitation, they will be required to login before they can access the meeting.
- Stay up to date by reviewing security tips on the Zoom blog.
- Watch Zoom's six minute video to familiarize yourself with how to secure your Zoom meetings and virtual classrooms.