Guidelines for Using Cloud-based Collaboration and Remote (Live) Conferencing Platforms

Following are guidelines designed to assist New Jersey public agencies using cloud-based collaboration and remote video conferencing platforms. These platforms allow organizations to receive, create, store, access and share electronic records and information through the use of third-party facilities like Microsoft's Office 365 and Google's G Suite. Examples of standalone conferencing platforms include GoToMeeting and Zoom.

The Division of Revenue and Enterprise Services (DORES) is providing these guidelines because more public agencies are planning for safe and secure use of these platforms in the face of the COVID-19 pandemic and the continuing trend toward remote work (telework).

Guidelines

1. Only install platforms that are approved by your information and technology officials. Installation of unapproved software exposes the organization to information security risks.
2. Consult with your information and technology officials regarding the required security settings for remote video conferencing sessions. These settings revolve around controlling participation, muting/unmuting and removing participants, enabling/disabling chat, screen sharing and annotation features and locking sessions.
3. In using a cloud-based collaboration and remote conferencing platform, use a password that adheres to the organization's policy on passwords.
4. Open meetings only to those whose participation is necessary for accomplishing the meeting's objectives and double-check to make sure that you have selected the correct invitees.
5. While away from your office, use only safe Internet carriers (avoid using hotel, coffee shop or unsecured wireless access points).
6. Use agency-owned hardware whenever possible.
7. If using a personal device, keep it current with patches, updates and the latest software versions. If you are using an agency-issued device, make sure you connect it to the agency's network at least once a month to ensure it receives all required patches, updates and software versions.
8. Know which laws and regulations pertain to the subject matter being posted, discussed, displayed or shared. For example, you may be dealing with tax, personal health, personally identifiable and/or proprietary information/records. **Take steps to prevent the display of, sharing and/or disclosure of such information to unauthorized parties. If you are not certain that a connection or platform is secure, do not display, share or disclose such information by remote means until you can obtain access to a secure connection or platform.**
9. Do not store tax, personal health, personally identifiable and/or proprietary information/records in the Cloud unless you are cleared to do so by your records and information technology officials. If you are not cleared to store this content in the Cloud, store it on the agency's on-premises platform – for example, on shared drives or image and content management systems that your agency controls directly. Note that in order to file information/records on your on-premises platform from a remote location, you will need to have software that allows you to access your on-site computing systems. This is usually accomplished through remote desk top software or via virtual private networks (VPN). Consult with your information technology officials regarding your options here.
10. Do not record audio-video sessions that deal with sensitive or confidential information unless cleared to do so by your records and information technology officials. Also, disable or temporarily shut off voice activated devices (for example, Alexa, Google and Siri) prior to participating in confidential voice or video calls.

11. Remember that records/information created and stored on collaboration/online conferencing platforms are public records, and therefore are subject the State's public records retention/disposition law and Open Public Records Act. Contact the Division of Revenue and Enterprise Services (DORES), Records Management for guidance on retention requirements for such records/information. (DORES Records Management Services - 609-777-1020 or 609-292-8711).
12. Be mindful that any public body meetings that you conduct via remote conferencing will be subject to the State's various open public meeting (OPM) laws, and that all requisite OPM actions and procedures apply.
13. When participating in a collaborative dialogue or a remote meeting initiated and/or hosted by a third party, be sure to adhere to guidelines 7-11 above:
    a. Do not disclose confidential/sensitive information/records to unauthorized parties;
    b. Do not record or store confidential/sensitive information on cloud-platforms unless authorized to do so;
    c. Seek guidance from DORES Records Management Services on how to comply with records retention requirements; and
    d. Adhere to OPM requirements where applicable.