County Risk Sharing Authority
a service program of the County Commissioners Association of Ohio

209 East State Street • Columbus, Ohio 43215-4309
Phone: 614-221-5627 • Fax: 614-220-0209
Toll Free: 888-757-1904 • www.corsa.org
Claims Unit Toll Free: 866-455-8039

County Risk
Sharing Authority

May 8, 2020

RISK CONTROL SERVICE BULLETIN

Teleconferencing and Video Meetings

CORSA members utilization of video meeting and teleconferencing as a method of communication during the COVID-19 pandemic has likely increased significantly and high usage rates will continue well into the future long after the current crisis is concluded. As with all technologies their use brings risk. To help CORSA members address this on-point risk guidance provided by the DHS Cybersecurity and Infrastructure Security Agency (CISA) is attached to this bulletin. CORSA recommends members thoroughly review the attached recommendations and best practices given in the documents. CISA gives specific recommendations for common video conferencing tools, recommended enterprise security practices, best practices for end-users and general best practices tips. We also strongly recommend that continuously work with your IT providers regarding cybersecurity matters.

Continue to Conduct Inspections Preventative Maintenance & Repairs

Time and resources are in short supply; however, we recommend that members continue property and equipment inspections, preventative maintenance, and repairs without interruption. History proves that deference or delay of no or low-cost measures such as inspections, preventative maintenance, and repairs saves appointing authorities time and resources over time. During the economic downturn in 2008-09 CORSA saw a large increase in property claims due to deferred maintenance. In order to contain both covered and uncovered losses CORSA recommends maintaining a good inspection and maintenance schedule for all member property and contents.

As a CORSA member we encourage you to take advantage our services and resources at no cost to the member county. For your assistance in planning maintenance priorities you will find attached to this bulletin the CORSA building inspection checklist. While CORSA on-site building inspections are suspended under the current Stay at Home and/or Stay Safe Order, feel free to contact Jim Hale, CORSA Risk Management Consultant, at 614-246-1630 or jhale@ccao.org to consult regarding property risk mitigation measures. We look forward to resuming on-site services soon.

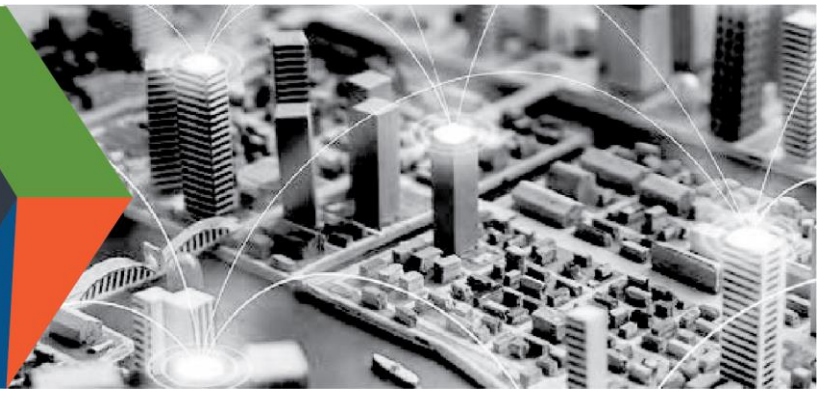
As a CORSA member you are eligible to take advantage of subsidized facility management software program. CORSA's facility management software program from Dude Solution is an excellent tool to assist in your maintenance efforts. The software features Planned Maintenance – "Planned Maintenance is a cloud-based planned maintenance scheduling solution that helps you schedule recurring maintenance tasks and generate corresponding work orders within the Work Order system."[1]

CORSA covers 75% of the cost of Maintenance Edge as a value-added Risk Management service and this service is available to all CORSA members. Planned Maintenance is part of the Maintenance Edge product. If you are interested is exploring Maintenance Edge please contact Jim Hale, CORSA Risk Management Consultant, at 614-246-1630 or jhale@ccao.org.

[1] *Please Note: The content and attachments are current as of May 6, 2020.*

CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY, SECURE TOMORROW



GUIDANCE FOR SECURING VIDEO CONFERENCING

This product is for organizations and individual users leveraging videoconferencing tools, some of whom are remotely working for the first time.

As the authority for securing telework, the **Cybersecurity and Infrastructure Security Agency (CISA)** established this product line with cybersecurity principles and practices that individuals and organizations can follow to video conference more securely. Although CISA is providing this general risk advisory guidance, individuals and organizations are responsible for their own risk assessments of specific systems and software. For optimum risk mitigation, organizations should implement measures at both the organizational and user levels.

BACKGROUND

- The Federal Government, state and local governments, the private sector, and general public have pivoted to widescale remote work and online collaboration.
- Video conferencing has emerged as a pervasive tool for business continuity and sustained social connection. Although increased telework and online collaboration tools provide necessary capabilities, video conferencing has increased the attack surface exploited by malicious actors.
- Once niche products, many of these tools were meant for a subset of the business community and were not scaled for crisis-driven ubiquity. Entire industries, sectors, and stakeholder sets are now profoundly dependent on online tools—simultaneously.
- Amid the unanticipated exponential growth and unprecedented popularity of these platforms, many video conferencing users have not implemented necessary security precautions—or might be unaware of the latent risks and vulnerabilities.

FOUR PRINCIPLES AND TIPS TO SECURE VIDEO CONFERENCING

1. CONNECT SECURELY

Risk: The initial settings for home Wi-Fi networks and many video conferencing tools are not secure by default, which—if not changed—can allow malicious actors to compromise sensitive data while you work from home.

Mitigation: Change default passwords for your router and Wi-Fi network. Check that you are using Wi-Fi encrypted with WPA2 or WPA3. Verify your video conferencing security settings and use encrypted video conferencing tools whenever possible.

Tips: Here are some simple actionable tips for connecting securely at home.

- ✓ **Change default password to strong, complex passwords** for your router and Wi-Fi network.
- ✓ **Choose a generic name for your home Wi-Fi network** to help mask who the network belongs to, or its equipment manufacturer.
- ✓ **Ensure your home router is configured to use WPA2 or WPA3** wireless encryption standard at the minimum, and that **legacy protocols such as WEP and WPA are disabled.** See CISA's Tip on Home Network Security for additional information.

CONNECT WITH US
www.cisa.gov

For more information,
email cisaservicedesk@cisa.dhs.gov

Linkedin.com/company/cybersecurity-and-infrastructure-security-agency

@CISAgov | @cyber | @uscert_gov

Facebook.com/CISA

Tips, *continued*:

- ✓ **Avoid using public hotspots and networks.**
- ✓ **Only use video conferencing tools approved by your organization** for business use.
- ✓ **Enable security and encryption settings** on video conferencing tools; these features are not always enabled by default.

2. CONTROL ACCESS

Risk: Uncontrolled access to conversations may result in disruption or compromise of your conversations, and exposure of sensitive information.

Mitigation: Check your tool's security and privacy settings. Enable features that allow you to control who can access your video chats and conference calls. When sharing invitations to calls, ensure that you are only inviting the intended attendees.

Tips: Here are some simple actionable tips to help control access to your conversations.

- ✓ **Require an access code or password** to enter the event. Try not to repeat codes or passwords.
- ✓ **Manage** policies to ensure only members from your organization or desired group can attend. Be cautious of widely disseminating invitations.
- ✓ **Enable "waiting room" features** to see and vet attendees attempting to access your event before granting access.
- ✓ **Lock the event** once all intended attendees have joined.
- ✓ **Ensure that you can manually admit and remove attendees** (and know how to expeditiously remove unwanted attendees) if opening the event to the public. Be mindful of how (and to whom) you disseminate invitation links.

3. MANAGE FILE AND SCREEN SHARING AND RECORDINGS

Risk: Mismanaged file sharing, screen sharing, and meeting recording can result in unauthorized access to sensitive information. Uncontrolled file sharing can inadvertently lead to users executing and clicking malicious files and links, which could, in turn, lead to system compromise.

Mitigation: Disable or limit screen and file sharing to ensure only trusted sources have the capability to share. Users should be aware of sharing individual applications versus full screens.

Tips: Here are some simple tips for controlling file and screen sharing.

- ✓ **Toggle settings to limit the types of files that can be shared** (e.g., not allowing .exe files).
- ✓ **When recording meetings, make sure participants are aware** and that the meeting owner knows how to access and secure the recording. Consider saving locally rather than in the cloud. Change default file names when saving recordings. Consult with your organizational or in-house counsel regarding laws applicable to recording video conferences.
- ✓ **Consider sensitivity of data** before exposing it via screen share or uploading it during video conferences. Do not discuss information that you would not discuss over regular telephone lines.
- ✓ **See CISA's Tip:** Risks of File-Sharing Technology for more information.

4. UPDATE TO LATEST VERSIONS OF APPLICATIONS

Risk: Outdated or unpatched video conference applications can expose security flaws for hackers to exploit, resulting in a disruption of meeting privacy and potential loss of information.

Mitigation: Ensure all video conferencing tools, on desktops and mobile devices, are updated to the latest versions. Enable or opt-in to automatic update features, or else establish routine updates (e.g., once weekly) to check for new versions and patch security vulnerabilities.

Tips: Here are some helpful tips to keep applications updated and secure.

- ✓ **Enable automatic updates** to keep software up to date.
- ✓ **Develop and follow a patch management policy** across the organization that requires frequent and continual application patching.
- ✓ **Use patch management software** to handle and track patching for your organization.
- ✓ **See CISA's Tip:** Understanding Patches and Software Updates for more information.

SECURITY SETTINGS OF COMMON VIDEO CONFERENCING TOOLS

In addition to the guidance above, CISA recommends that organization administrators and individual users become familiar with the security settings and capabilities of their preferred video conferencing platform(s). Listed below are links from several popular video conferencing user guides (and their administrative policy settings) that can help individuals and organizations reduce the risk of unwanted interruptions, compromise, or exposure of sensitive data.

CISA recommends that administrators and users examine video conferencing tool user guides in their entirety; the links below are informational only and are not exhaustive. CISA is providing this general risk guidance and has not independently confirmed the veracity of each company's sites or claims. CISA does not certify, endorse, or recommend usage of one product over another product. Although administrators and users may improve video conference security by implementing capabilities noted below, cybersecurity events may still occur even if vendors and users take every possible precaution. CISA does not guarantee the security of these products; users are encouraged to verify, to every extent feasible, the security of vendor-provided products and to implement desired security controls.

Product	Control Access	Connect Securely	File and Screen Sharing and Recording	Update Versions
Zoom	Managing group policy in Zoom			
	✓ Assigning roles ✓ Enable waiting rooms ✓ Enable passwords ✓ Identify guest participants ✓ Enable two-factor authentication	✓ Encryption ✓ Security settings ✓ Audio watermark	✓ Limiting file types ✓ Managing meeting participants (including screen sharing)	✓ Updates for Windows ✓ Updates for MacOS ✓ Updates for Android ✓ Updates for iOS

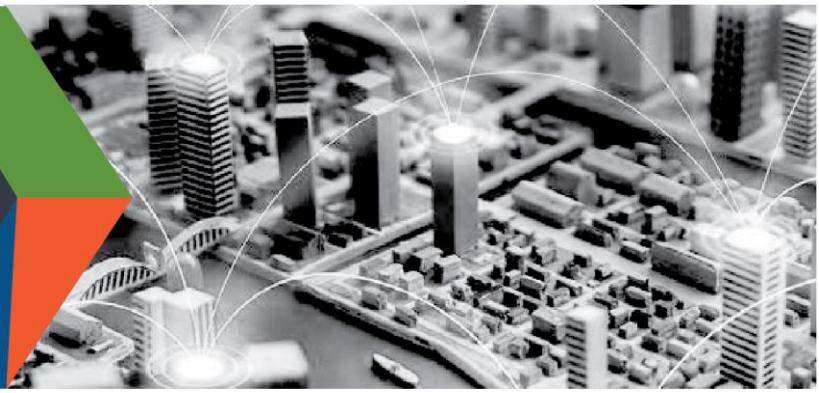
Product	Control Access	Connect Securely	File and Screen Sharing and Recording	Update Versions
Microsoft Teams	Managing policies in Teams			
	✓ Identification and authentication ✓ Managing meeting policies ✓ Assigning policies for users ✓ Managing meeting settings ✓ Control meeting participation ✓ Control automatic meeting entry	✓ Communication and encryption	✓ Desktop sharing ✓ Content sharing	✓ Teams updates
GoToWebinar	✓ Password protect your webinar ✓ Remove individual from webinar ✓ Manage attendees	✓ Encryption and security features	✓ Screen sharing	✓ Automatic updates
Cisco WebEx	Managing group policy			
	✓ User management ✓ Password settings	✓ Encryption	✓ Policy settings for screen, video, and file sharing	✓ Manual updates
Adobe Connect	Managing group policy			
	✓ Manage a meeting ✓ Invite attendees and grant or deny access ✓ Modify participant list ✓ Remove individuals from a group	✓ Security overview ✓ Secure connections	✓ Screen sharing controls ✓ Sharing content ✓ Recording and playback	✓ Application updates
GoToMeeting	Group Administration			
	✓ Password protect your meetings ✓ Invite others ✓ Manage attendees ✓ Lock your meeting ✓ One-time meetings	✓ Encryption	✓ Share your camera ✓ Manage attendees ✓ Share your screen ✓ Keyboard and Mouse control ✓ Record a session ✓ Manage and share session recordings	✓ Automatic updates

Product	Control Access	Connect Securely	File and Screen Sharing and Recording	Update Versions
Slack	Slack workspace administration			
	✓ Manage members ✓ Manage permissions	✓ Encryption	✓ Block download to unmanaged devices ✓ Guest invitation ✓ Screen sharing	✓ Download latest version

FEEDBACK

CISA has provided information on the above list of products as examples of video conferencing solutions; the list is not exhaustive, nor is the recency and accuracy of the linked information controlled by CISA. CISA welcomes service providers and vendors to submit additional information that can be included in this reference guide to CyberLiaison@cisa.dhs.gov.

CISA
CYBER+INFRASTRUCTURE
DEFEND TODAY, SECURE TOMORROW



CYBERSECURITY RECOMMENDATIONS FOR CRITICAL INFRASTRUCTURE USING VIDEO CONFERENCING

This videoconferencing product is for executives charged with securing critical infrastructure networks, and for critical infrastructure employees to help them think through related cybersecurity and physical issues.

RAPID INCREASE IN ADOPTION AND DEPLOYMENT OF VIDEO CONFERENCING

American companies and government agencies are increasingly adopting workplace flexibilities such as telework. Advances in information technology, such as the increased availability of video conferencing software and video conferencing capabilities incorporated into other products like collaboration software, facilitate telework. Users are likely to need video conferencing and other collaboration solutions to stay connected as they telework. It is critical that cybersecurity requirements and risk exposure for products be counterbalanced appropriately against remote access product benefits such as convenience, usability, speed, and stability.

The following advisory guidance is intended to support the incorporation of cybersecurity considerations when adopting or expanding the use of video conferencing software and related collaboration tools. The guidance also includes suggestions for individuals using these tools to host and attend meetings—information that is particularly critical as organizations increasingly broadcast sensitive discussions over these platforms.

As the authority for securing telework, the **Cybersecurity and Infrastructure Security Agency (CISA)** established this product line. We plan to continue refining it and consider releasing additional products related to the secure use of online collaboration tools and video conference solutions to further support the ongoing efforts of cybersecurity leaders during this period of maximum telework. Please send your feedback to CyberLiaison@cisa.dhs.gov.

POTENTIAL THREAT VECTORS

Cyber adversaries, from nation-state actors to insiders and criminal organizations, seek to acquire information on research and development, critical infrastructure, and personally identifiable information. Additionally, some actors, seek to disrupt the operations of American institutions and misuse systems for politically motivated causes. Some tactics include cyber actors:

- Actively exploiting unpatched vulnerabilities in client software to gain access to organizational networks and carry out cyber exploitation and cyberattacks;
- Exploiting communication tools to:
    - Take users offline by overloading services, or

  - Eavesdropping on meetings or conference calls;
- Hijacking video-teleconferences by inserting pornographic images, hate images, or threatening language;
- Compromising remote desktop applications (used in some telework solutions to enable remote desktop sharing for collaboration and presentations) to infiltrate other shared applications; and
- Attempting to penetrate sensitive meetings by using social engineering to deceive individuals into divulging information (e.g., meeting links) or by inferring meeting links from other links that use a common structure (e.g., company_name_YYYY_MM_DD).

Some video conferencing products may unintentionally expose information to nefarious cyber actors. For example, some of these products may share or sell customer information to third parties or target users to integrate product use with their personal social media accounts. This data sharing can unintentionally expose employee and organizational information beyond intended recipients.

RECOMMENDED ENTERPRISE SECURITY PRACTICES

1. Assess your organizational needs and determine the appropriate product to use in the enterprise. Also consider the mission need for your organization to collaborate with outside entities. Examine supply chain concerns (e.g., vendor reputation, data center locations) and whether the service under consideration addresses your organization's other security, legal, and privacy requirements.
2. Establish an organizational virtual meeting policy or recirculate the policy if it already exists. Ensure updated guidance is continuously available. Develop a one-page summary of policies applicable to virtual meetings that is easily digestible by end users.
3. Limit and minimize the number of collaboration tools authorized for use in the enterprise to reduce the attack surface and the overall amount of vulnerabilities. Develop a list of approved collaboration and videoconferencing tools for your organization. Review and update security settings continuously. Scan for and remove all unauthorized collaboration tools and associated clients from the enterprise. Centrally manage authorized clients and configuration settings enterprise wide. Maintain the latest version by promptly updating client software and removing all obsolete versions.
4. Prohibit end users from installing client software (including removing local administration rights). When an outside entity initiates a meeting using a collaboration tool not on an approved product list, instruct users to join web (browser) based sessions that do not require installation of client software.
5. Prevent users with administrative privileges from using collaboration tools on the system while logged on with those privileges. Administrators should not perform non-privileged operations on the systems they are administering (e.g., using email, browsing the internet, performing office automation tasks, engaging in recreational use).
6. Prohibit the use of collaboration tools and features that allow remote access and remote administration. While not the main purpose of collaboration tools, some vendors may advertise remote access software as collaboration tools and some collaboration tools may allow remote access and remote administration.
7. Clearly articulate to employees the privacy and document retention implications of your organization's collaboration tools, including any data sharing or utilization of participation or attention tracking features.

8. Ensure that your organization's telework policy or guide addresses requirements for physical and information security. Verify that users have updated telework agreements. Consider whether organizational information technology priorities need to be adjusted given the different contexts of largescale telework.

BEST PRACTICES FOR END-USERS

1. Only use organization-approved software and tools for business, including company-provided or -approved video conferencing and collaboration tools to host/initiate and schedule meetings.
2. Tailor security precautions to be appropriate for the intended audience and content of a meeting. Do not make meetings "public" unless they are intended to be open to anybody. For meetings that will be broadly attended, ensure you have the capability to mute all attendees and limit the ability of attendees to share screens.
3. Particularly when conducting meetings with a large audience, have a preestablished plan that details:
    a. The circumstances in which a meeting will be terminated if it is disrupted,
    b. Who has the authority to make that decision, and
    c. How the meeting termination will be executed.
4. For private meetings, require a meeting password and use features such as a waiting room to control the admittance of guests. For enhanced security, use randomly generated meeting codes and strong passwords and do not reuse them. Do not share a link to a teleconference on an unrestricted, publicly available social media post. If possible, disable the ability of participants to join a meeting before the host and automatically mute participants upon entry.
5. Provide the link to the meeting directly to specific people and share passwords in a separate email. If possible, require unique participant credentials, monitor meeting members as they join, and lock an event once all desired members have joined. Use features to permit removal of any meeting guest during the course of the meeting.
6. Manage screensharing, recording, and file sharing options. Consider saving locally versus to the cloud based on the specific circumstances (e.g., need to share the recording with a wide audience or the public, using company-issued equipment versus personal equipment). Change default file names when saving recordings. Make sure to consult with your organization's counsel about laws applicable to recording videoconferences and sharing materials through them. Set participant expectations on session recording, screen recording, and screen shots.
7. Consider sensitivity of data before exposing it (via screen share or upload) to video conference and collaboration platforms. When sharing a screen, ensure only information that needs to be shared is visible; close or minimize all other windows. If displaying content from organizational intranet sites in public meetings, hide the address bar from participants before displaying the content. Use common sense—do not discuss content you would not discuss over regular telephone lines. When having sensitive discussions, use all available security measures (e.g., waiting rooms and strong passwords), ensure all attendees of the meeting have a need to know, and make attendees aware of expectations for session security. Examples of information that may be unsuited to discussing via video teleconferencing software include: National Security Information, Sensitive Law Enforcement Information, Critical Infrastructure System Operations or Vulnerabilities, Continuity of Operations Plans, Personally Identifiable Information, Advanced Research and Development Projects, and

Proprietary Business Information.

8. When joining meetings initiated by third parties that use collaboration tools not approved by your organization, do not attempt to install software—join web (browser) based session instead. Do not use work email addresses to sign up for unauthorized/free tools.
9. If logging into a collaboration tool via a web browser, be careful to accurately type the domain name of the website. Be wary of links sent by unfamiliar addresses, and never click on a link to a meeting sent by a suspicious sender. Verify that meeting links sent via email are valid.
10. Ensure that your visual and audio surroundings are secure and do not reveal any unwanted information (e.g., confirm that whiteboards and other items on the wall are cleared of sensitive or personal information; confirm that roommates or family members are not within earshot of sensitive conversations). If available, make use of background replacement or blurring options in the collaboration tool.
11. Move, mute, or disable virtual assistants and home security cameras to avoid inadvertently recording sensitive information. Do not have sensitive discussions with potential eavesdroppers in your workspace or in a public area. Consider using headphones.
12. Check and update your home network. Change default settings and use complex passwords for your broadband router and Wi-Fi network and only share this information with people you trust. Choose a generic name for your home Wi-Fi network to avoid identifying who it belongs to or the equipment manufacturer. Update router software and ensure your Wi-Fi is encrypted with current protocols (such as WPA2 or WPA3), and confirm that legacy protocols such as WEP and WPA are disabled.

REPORTING

To report a cyber incident, call CISA at 1-888-282-0870 or visit www.cisa.gov.

CISA
CYBER+INFRASTRUCTURE

TIPS FOR VIDEO CONFERENCING

TIP 1: ONLY USE APPROVED TOOLS

Only use organization-approved software and tools for business, including company-provided or -approved video conferencing and collaboration tools to initiate and schedule meetings.

1. **Don't install unapproved clients.** When joining meetings initiated by third parties that use collaboration tools not approved by your organization, do not attempt to install software—join web (browser) based session instead. Do not use work email addresses to sign up for unauthorized/free tools.

2. **Ensure links are correct.** If logging into a collaboration tool via a web browser, be careful to accurately type the domain name of the website. Be wary of links sent by unfamiliar addresses, and never click on a link to a meeting sent by a suspicious sender. Verify that meeting links sent via email are valid.

TIP 2: SECURE YOUR MEETING

Tailor security precautions to be appropriate for the intended audience. Plan for what to do if a public meeting is disrupted. Take precautions to ensure your meeting is only attended by intended individuals.

1. **Consider attendees.** Do not make meetings "public" unless they are intended to be open to anyone. For meetings that will be broadly attended, ensure you have the capability to mute all attendees and limit the ability of attendees to share screens.

2. **Have a plan to terminate a meeting.** Particularly when conducting meetings with a large audience, have a preestablished plan that details:

   a. The circumstances in which a meeting will be terminated if it is disrupted,

   b. Who has the authority to make that decision, and

   c. How the meeting termination will be executed.

3. **Secure private meetings.** For private meetings, require a meeting password and use features such as a waiting room to control the admittance of guests. For enhanced security, use randomly generated meeting codes and strong passwords and do not reuse them. Do not share a link to a teleconference on an unrestricted, publicly available social media post. If possible, disable allowing participants to join a meeting before the host and automatically mute participants upon entry.

4 **Control attendees.** Provide the link to the meeting directly to specific people and share passwords in a separate email. If possible, require unique participant credentials, monitor meeting members as they join, and lock an event once all desired members have joined. Utilize features to permit removal of any meeting guest during the course of the meeting.

TIP 3: SECURE YOUR INFORMATION

Tailor your security precautions appropriate to the sensitivity of your data. Only share data necessary to accomplish the goals of your meeting.

1 **Manage screensharing, recording, and file sharing options.** Consider saving locally versus in the cloud based on the specific circumstances (e.g., need to share the recording with a wide audience or the public, using company-issued equipment versus personal equipment). Change default file names when saving recordings. Make sure to consult with your organization's counsel about laws applicable to recording videoconferences and sharing materials through them. Set participant expectations on session recording, screen recording, and screen shots.

2 **Protect sensitive information.** Consider sensitivity of data before exposing it (via screen share or upload) to video conference and collaboration platforms. When sharing a screen, ensure only information that needs to be shared is visible; close or minimize all other windows. If displaying content from organizational intranet sites in public meetings, hide the address bar from participants before displaying the content. Use common sense—do not discuss content you would not discuss over regular telephone lines. When having sensitive discussions, use all available security measures (e.g., waiting rooms and strong passwords), ensure all attendees of the meeting have a need to know, and make attendees aware of expectations for session security.

TIP 4: SECURE YOURSELF

Take precautions to avoid unintentionally revealing information. Ensure home networks are secured.

1 **Don't reveal information unintentionally.** Ensure that your visual and audio surroundings are secure and do not reveal any unwanted information (e.g.; confirm that whiteboards and other items on the wall are cleared of sensitive or personal information, confirm that roommates or family members are not having sensitive conversations in the background). If available, make use of background replacement or blurring options in the collaboration tool.

2 **Consider your surroundings.** Move, mute, or disable virtual assistants and home security cameras to avoid inadvertently recording sensitive information. Do not have sensitive discussions with potential eavesdroppers in your workspace or in a public area. Consider using headphones.

3 **Check and update your home network.** Change default settings and use complex passwords for your broadband router and Wi-Fi network and only share this information with people you trust. Choose a generic name for your home Wi-Fi network, to avoid identifying who it belongs to or the equipment manufacturer. Update router software and ensure your Wi-Fi is encrypted with current protocols (such as WPA2 or WPA3), and confirm that legacy protocols such as WEP and WPA are disabled.

For more information, please visit cisa.gov/telework.

CORSA Building Inspection Checklist

Location _____

Elected Official / Department Head _____

Inspector, Title _____ Date _____

Building Maintenance Supervisor for this Location _____ Phone# _____

✓ Indicates checked and found satisfactory.

X Indicates unsatisfactory - complete Hazard Report and correct immediately.

N/A Indicates checked and found not applicable to this location.

Exterior

☐ Exterior building appearance satisfactory

☐ Exterior lighting adequate

☐ Sidewalks clear, good condition

☐ Steps and railings secure

☐ Doors secure and unobstructed

☐ Handicapped access available and marked

☐ Parking lot surface and lighting adequate

Public Areas, Waiting Rooms

☐ Entry floor mats (to prevent water accumulation) - in good condition

☐ Eliminate slip / trip hazards

☐ Furniture stable, in good repair

☐ Restrooms clean, accessible

Basement

☐ Identify water damage, dampness, moisture

☐ Hallways unobstructed

☐ Boiler Room - clear access, no combustible storage, boiler inspection posted (if applicable)

☐ Electrical Panels - clear access, good working appearance

☐ Storage areas in orderly condition

Stairways

☐ Handrails secure

☐ Stair treads in good condition

☐ Adequate lighting

☐ Stairways unobstructed

☐ Exits marked

☐ Doors kept closed

Elevators

- ☐ Clean, clear of debris
- ☐ Adequate lighting
- ☐ Inspection certificate posted

Fire Protection

- ☐ Fire extinguishers marked, tested, tagged
- ☐ Building evacuation route posted
- ☐ Evacuation alarm pull stations marked, system tested periodically (if applicable)
- ☐ Sprinkler system tested periodically (if app.)
- ☐ Fire drills conducted periodically

Office Environment

- ☐ Clear, adequate walkways around desks and equipment - eliminate slip / trip hazards
- ☐ Carpets and floors in good condition
- ☐ Trash collected and removed daily
- ☐ All electrical equipment grounded
- ☐ Electrical equipment away from water source
- ☐ All extension cords grounded, heavy duty
- ☐ Eliminate excessive use of extension cords
- ☐ Surge protectors is use
- ☐ Adequate storage for supplies & materials away from heat / combustion source
- ☐ Exits marked and unobstructed
- ☐ Eliminate loose objects that could fall from overhead
- ☐ Approved step-stool available for overhead access
- ☐ First aid kit available

Copies of this report sent to: _____

CORSA Building Inspection Hazard Report

Inspector, Title _____ Inspection Date _____

Location	Hazard Description	Corrective Action Recommended	Person Contacted/ Action Taken
