Appendix 2 SOP 002.2 Conduct Virtual Training in a COVID-19 Environment

Date of Issue: 2020-08-17

References: A. SOP 002.1 Prepare to Resume Corps/Sqn Trg in a COVID-19 Environment
B. Tasking Order 002 to Campaign Plan
C. Tasking Order 001 to Campaign Plan
D. Natl CJCR Sp Gp Summer 2020 Campaign Plan
E. Natl CJCR Sp Gp Order 8012-1
F. COTM 05/18

1. Purpose

1.1 The purpose of this Standard Operating Procedure (SOP) is to outline the procedures that should be followed in order to conduct virtual training in a COVID-19 environment for the 2020/2021 training year (TY).

2. Abbreviations and Acronyms

Abbreviation	Complete word or phrase
Corps/Sqn	Corps/Squadron
CoC	Chain of Command
CO	Commanding Officer
COVID-19	Coronavirus Disease-19
QSP	Qualification Standard and Plan
RMLO	Regional Medical Liaison Officer
SOP	Standard Operating Procedures
TY	Training Year
WRT	With Regards To

3. Definitions

3.1 Nil.

4. General

4.1 As Corps/Squadrons (corps/sqn) resume limited in-person and virtual training, consideration must be given to the safe conduct of activities in a COVID-19 environment. All training shall be prepared and conducted by adhering to the most restrictive guidelines by all levels of government and public health directives of the specific province, region, city, or municipality. Corps/sqn Commanding Officer's (CO) shall ensure that all conditions, as per Refs A, B, C, & D, of Appendix 2 Annex C are met.

4.2 Corps/Sqn COs are to ensure approval to conduct virtual training has been received and is in line with national/regional directives and policies. Refer to ref A of Appendix 2 to Annex C for further information.

5. Pre-Planning

5.1 Prior to conducting any virtual training activity, corps/sqn COs or their designate, must:

a. ensure the safe conduct of the activity, ensuring guidelines with regards to (WRT) the number of participants allowable on the platform are met and required staff supervision ratios, as per ref E of Appendix 2 of Annex C, are met;

b. review corps/sqn training plan, applicable Qualification Standard and Plan (QSP) and all other relevant resources & tools available;

c. determine an appropriate and authorized platform for the delivery of the virtual training, confirming the following:

(1) participants have internet accessibility, have access to a computer and the ability to attend virtual training sessions;
(2) access requirements, including applicable software and computer capabilities;
(3) accuracy of email and contact information for participants';
(4) virtual training activity timings, to include, if required, forwarding invites to participants in order for them to access the platform;
(5) process for completion of in-routine (attendance register); and
(6) appropriate adult supervision of all virtual training sessions;

d. prior to conducting the virtual training activities, ensure that a tutorial session of the platform is provided in order to ensure everyone is familiar and has a basic level of how it works to include:

(1) testing microphones, speakers, etc.;
(2) demonstrating how the chat feature works for questions during the session;
(3) explaining how to mute microphone during session in order to eliminate background noise;
(4) utilizing the turn-off video feature; and
(5) any other relevant information to ensure a successful session;

e. update training schedule, in order to ensure training is conducted as per the COVID-19 restrictions, while also ensuring that supervision ratios are adhered to; and

f. establish ground rules for the virtual training activities, to include:

(1) establishing purpose and learning objectives for the virtual training activities;
(2) ensuring participants understand expectations with regards to (WRT) attendance, wearing of uniform, and other requirements as applicable; and
(3) ensuring participants understand that although activity is virtual, if they are unwell, specifically displaying symptoms of COVID-19, they are to be excused, and they will not be disadvantaged for not completing the training.

5.2 To foster a safe training environment it is imperative that the CO or their designate consider the following:

a. maintain administrative oversight of the platform to include but not limited to:

(1) ensuring the application is current and up to date;
(2) restricting administrative privileges are restricted to those who require them;
(3) disabling features not being used (e.g. file sharing); and
(4) reviewing default settings for available security options (e.g. waiting rooms, passwords, invitations, etc.).

b. ensure session connection information is shared via a secured means;
c. advise participants to not share sensitive information during the session; and
d. establish a reporting mechanism for inappropriate conduct by adult leaders and participants.

5.3 Attachment 1 to Appendix 2 of Annex C provides a pamphlet outlining recommended guidelines for video-teleconferencing from the Canadian Centre for Cyber Security.

6. Virtual Arrival

6.1 Upon arrival for the virtual training activity, staff will ensure the following:

a. begin session 15-20 minutes earlier than scheduled time in order to allow cadets time to access the platform;

b. confirm all participates have accessed the site, trouble shoot any issues that arise;

c. ensure that there are no medical concerns, and that all participants are ready to participate, as applicable;

d. ensure attendance is registered, and compliant WRT conduct, dress, as applicable, etc.;

e. review previously provided ground rules and expectations;

f. conduct an icebreaker and answer any questions before getting started; and

g. introduce training and conduct virtual training.

7. Conduct of the Activity

7.1 For the duration of the virtual training activity staff must ensure the following:

a. frequent breaks and wellness checks are provided;

b. adequate opportunities for participants to ask questions are provided;

c. ongoing monitoring and supervision in a virtual setting, as per Natl CJCR Sp Gp Order 8012-1 Supervision of Cadets; and

d. continued reminders, as required, to staff and cadets as necessary for the safe conduct of virtual training activities.

8. Departure

8.1 Upon completion of the virtual training activity, the staff must confirm and complete the following:

a. review the purpose and learning objectives for the virtual training;

b. conduct a confirmation of key learning points via a short on-line quiz or other confirmation methods;

c. conduct a debrief with participants, focus feedback on what they learned, and what they found challenging in the virtual setting;

d. assign any homework and promote the learning objectives for the next session. Identify what's in it for them and their continued progression within the cadet program in preparation for a gradual resumption of activities when conditions permit;

e. remind staff and cadets of the necessity for 'Virtual Training' as per the Natl CJCR Sp Gp continued safe delivery of the cadet experience while operating in a COVID-19 environment; and

f. announce the next scheduled virtual training activity.

Attachment :

i. Canadian Centre for Cyber Security – Video Teleconferencing Guidelines

Communications Security Establishment | Centre de la sécurité des télécommunications

UNCLASSIFIED

CANADIAN CENTRE FOR CYBER SECURITY

VIDEO-TELECONFERENCING

MAY 2020 | ITSAP.10.216

By using video-teleconferencing (VTC) applications, your organization can meet and work with employees, clients, and partners who are in different geographic locations. However, there are security and privacy risks that you should consider before selecting and implementing VTC applications in your organization. Identifying the threats and risks related to these tools ensures that you implement the appropriate security measures and best practices to protect your organization's virtual work environment.

BENEFITS

VTC applications can increase productivity and improve collaboration between your employees, clients, and partners. These applications are more engaging than phone calls and offer face-to-face interaction between participants. Many of them have built-in collaboration tools (e.g. screen and file sharing, recording capabilities).

You can host meetings of various sizes without needing the physical space to do so.

There are many applications that are available for free or offer subscription options with a sliding fee scale, depending on the services that your organization needs.

RISKS

There are a lot of VTC applications to choose from. The security of your organization's systems and information is affected by how the vendor prioritizes security and how you use and secure these applications.

Threat actors can take advantage of vulnerabilities and software flaws and use brute force attacks to steal information or gain access to private discussions.

If sensitive information is discussed or shared on a VTC application, you may be at a higher risk of a data breach or a privacy breach, which can jeopardize your organization's reputation and relationships with clients and partners.

THREATS

Threat actors are targeting VTC applications to disrupt meetings, overload services, eavesdrop on calls, and steal information. Threat actors use different methods to attack VTC applications:

- **Brute-force attacks:** A threat actor automatically scans a list of possible meeting IDs to try to connect successfully.
- **Meeting bombing:** A threat actor joins a meeting to listen in on the conversation or disrupt the meeting by sharing inappropriate or explicit content.
- **Screen scraping:** A threat actor collects screen display data from a compromised system.
- **Malware**: A threat actor can infect devices by sharing malicious attachments, links, or applications to malicious hosts (e.g. websites, software).
- **Phishing**: A threat actor may attempt to initiate a VTC by imitating a trusted contact (e.g. with a non-functioning camera).
- **Insider threat:** Vendor personnel may accidentally or purposely compromise your organization's VTC meetings. An employee may mistakenly share information (e.g. meeting credentials) without having the proper training.

Never share sensitive information over VTC applications. Use other methods if you need to share sensitive information (e.g. secure encrypted messaging).

AWARENESS SERIES

SECURITY BEST PRACTICES

To mitigate the risks associated with using VTC applications, your organization needs to take precautions when selecting, implementing, and using the application. Consider the following tips:

CHOOSE THE APPLICATION

- Download applications from trustworthy vendors.
- Use existing corporate solutions whenever possible.
- Use a VTC application with security controls that can be customized to meet your requirements (e.g. security controls may differ between free and paid versions of the application).
- Use vendors that abide by Canadian privacy laws to ensure your information is protected from unauthorized users and sharing.
- Test the application before organizational use.

SECURE THE APPLICATION

- Keep applications up to date or consider using a solution that does not require participants to install software unless necessary (e.g. VTC web versions do not require user updates).
- Change default settings, as they are often less secure.
- Disable features you are not using (e.g. file sharing, screen sharing, transcript generator).
- Ensure administrative privileges are restricted to those who require them.

SECURE YOUR MEETINGS

- Secure a meeting with a passphrase or password.
- Keep the meeting link and password private.
- Ensure participants can only join the meeting if the host is present.
- Use a waiting room for participants, if available.
- Keep the number of meeting administrators or hosts to a minimum.
- Never share or discuss sensitive information on teleconferencing applications.

INCIDENT RESPONSE

If you suspect any malicious activity on your VTC meetings:

1. Stop the meeting.
2. Identify the information at risk (i.e. sensitive business or personal information shared in the meeting).
3. Change meeting IDs and passwords for any recurring or scheduled meetings.
4. Report activity to Cyber Centre: **contact@cyber.gc.ca**

TIPS FOR YOUR EMPLOYEES

Security training is an effective way to protect your organization from cyber threats and create a strong security culture. You should remind employees of the following best practices before they use VTC applications:

- Use only approved VTC applications for work purposes.
- Never share sensitive information over VTC.
- Keep the meeting ID and password private.
- Use strong passphrases for accounts.
- Use multi-factor authentication if available.
- Type the VTC web address manually into a web browser to avoid clicking on potentially malicious links.
- Use a secure Wi-Fi network.

See our related alert, *AL20-011 Considerations when using video-teleconferencing products and services*, which is available on our website.

Need help or have questions? Want to stay up to date and find out more on all things cyber security?
Visit the Cyber Centre website at cyber.gc.ca