Create Climate Justice Net (CCJnet)
USER SECURITY BEST PRACTICES GUIDE
Last Updated: May 22, 2018

A. Purpose

The purpose of this Guide is to ensure that, when using the CCJnet, a user's data, content, and the user generally, is as protected as possible from malicious or adverse actions by state and non-state actors alike. This Guide recognizes that there is no such thing as perfect digital security, but a few basic precautions may serve to protect the user as well as the CCJnet community as a whole.

B. Scope

This policy applies to any user that accesses and uses the CCJnet.

C. Device Security

1. When accessing the CCJnet, users should be connected to a secure form internet. Users should avoid connecting to unsecured networks (i.e., those networks that do not require a password to access). Logging into the CCJnet via an unsecured network may compromise the privacy and data of not only the user, but other users of the CCJnet and the CCJnet itself. If users connect to an unsecured network, users should take basic precautions and only connect through a trusted VPN or the TOR network.

2. Operating Systems: When accessing the CCJnet, users should, to the greatest extent possible, ensure that their operating system is running on the latest update for that system. CCJnet recommends configuring your system to automatically update.

3. Applications and Other Software: All software applications (such as mail clients, web browsers, VPN's, anti-virus, password managers, etc.) should be updated as updates become available. Software that is not updated and utilized while accessing the CCPnet may invite digital security threats that could harm the user, other users, and the CCJnet itself. Users should ensure that the email account attached to the user's CCJnet account is as secure as possible (this means strong passwords, regular updates, and encryption when possible).

4. Firewalls: Operating systems used to access the CCJnet should have a firewall activated to prevent unauthorized applications, programs, and services from accepting incoming connections.

5. Physical Security of Digital Devices:

    a. If your computer or other digital device that you use to login to the CCPnet is left in an "unsecure" location such as a hotel room, your

residence (if no one is home), or an office (if no one is at the office), ensure that it is completely powered down and that you are logged out of the CCJnet.

b. If your computer is temporarily confiscated by law enforcement, that device may be unsecure. There is no way to be sure that your device has not been maliciously modified and users should exercise caution if the user chooses to continue using that device.

D. Account Security

The following minimum security measures should be implemented by all users.

1. A user's CCJnet account should be protected by a unique password. Ideally, this password is generated by a secure password manager. Recommendations:
    a. Passwords should be at least 8 characters in length and contain upper and lowercase letters, numbers, and special characters (e.g., !@#$%^&); or
    b. Randomly selected words (4 words minimum) with a special character separating each word.
    c. Users should not share their passwords with anyone. In the event that you forget your password, follow the procedures here.
2. Users should ensure that their login credentials and passwords are unique to the CCJnet. Login credentials should not be duplicated from other services (e.g., your email login information should not contain the same password as your CCJnet password).
3. Passwords should be changed at least twice per year.
4. Users should not open attachments to messages or posts unless they trust or know the user who sent or posted the attachment. This includes links to websites that are not within the CCJnet.