Doc Name	INFORMATION TECHNOLOGY SECURITY POLICY
Issue No	ISSUE 1.0
Issue Date	Apr 10, 2023

Preamble

The Chilliwack Curling & Community Centre (CCCC) Information Technology (IT) resources are essential to its business. This policy aims to ensure the protection and secure use of the CCCC's IT resources by CCC personnel.

Scope

This policy applies to all CCC personnel who use the CCCC's IT resources, including but not limited to computers, laptops, mobile devices, audio-visual technology, cloud services, and email. This policy falls within the CCCC's overall Information Technology Policy (defined separately) and is to be taken in conjunction with this other policy.

Definitions

CCC personnel	Members, employees, contractors, volunteers of the Chilliwack Curling Club Society
contractors	persons contracted by the Chilliwack Curling Club Society
employees	persons employed by the Chilliwack Curling Club Society

IT department	person or persons responsible for the CCCC's Information Technology resources
IT resources	IT resources refer to any hardware, software, data, or personnel involved in the delivery and management of information technology services. This includes: 1. Hardware: Physical components such as servers, computers, mobile devices, and networking equipment. 2. Software: Applications, operating systems, and utilities used to manage and process information. 3. Data: Information stored and processed by IT systems, including databases, spreadsheets, and files. 4. Personnel: IT staff, including administrators, developers, support specialists, and security personnel. 5. Network infrastructure: Telecommunications and networking components that support the transmission of information. 6. Cloud services: Virtualized IT resources provided over the internet, including storage, processing, and software services. 7. Audio-visual technology: audio-visual technology can also be considered as a part of IT resources. This includes: a. Audio equipment: Microphones, speakers, and other audio hardware. b. Video equipment: Cameras, displays, and other video hardware. c. Audio-visual software: Applications for recording, editing, and processing audio and video content. d. Conferencing systems: Technology for conducting virtual meetings, webinars, and video conferences. e. Streaming Services: streaming services can also be considered as part of IT resources. Streaming services refer to platforms and technologies that deliver audio and video content over the internet in real-time or near real-time. These resources are essential in supporting communication, collaboration, and presentations within the CCCC

	organization, including internal and external broadcasting to CCCC audiences.
members	persons holding a certificate of membership with Chilliwack Curling Club Society
volunteers	persons registered with the Chilliwack Curling Club Society, who voluntarily undertake an agreed service to the Chilliwack Curling Club Society and are not a member, employee or contractor of the Chilliwack Curling Club Society

Policy

1. Password Management

- CCC personnel must use strong passwords and change their passwords regularly to ensure the security of the CCCC's IT resources.
- Passwords must be at least eight characters long and must include a combination of letters, numbers, and symbols.

2. Anti-Virus and Anti-Malware

- The CCCC will provide anti-virus and anti-malware software to protect IT resources from malicious software, viruses, and other malicious attacks.
- CCC personnel must keep their anti-virus and anti-malware software up to date and perform regular scans.

3. Firewall

- The CCCC will install and maintain a firewall to protect IT resources from unauthorized access and block malicious traffic.

- CCC personnel must not disable or bypass the firewall without the approval of the CCCC's IT department.

4. Physical Security

- CCC personnel must take steps to secure their IT resources from theft, loss, or damage, including but not limited to:
    - Locking their computers when they are not in use.
    - Keeping their laptops secure when travelling.
    - Reporting any lost or stolen IT resources immediately.

5. Email Security

- CCC personnel must be vigilant in avoiding email scams and phishing attempts.
- They must not open attachments from unknown sources, provide sensitive information in response to emails, or click on links in suspicious emails.

6. Mobile Devices

- CCC personnel who use mobile devices for CCCC business must take steps to secure their devices, including but not limited to:
    - Using password protection.
    - Installing anti-virus software.
    - Enabling remote wiping in the event of loss or theft.

7. Reporting Security Breaches

- CCC personnel must report any suspected security breaches immediately to the CCCC's IT department.

8. Training

- The CCCC will provide training to CCC personnel on IT resource security to help them understand the importance of IT resource security and how to protect the CCCC's IT resources.

9. Ongoing Review

- The CCCC will regularly review and update its IT resource security measures to ensure that they remain effective and to address any new security threats.

10. Policy Enforcement

- The CCCC will enforce this policy by regularly monitoring the use of the CCCC's IT resources and taking appropriate action when violations occur.
- In order to address violations of the CCCC Security Policy, the CCCC will provide additional training and resources to the individual(s) in question to help them understand the importance of IT resource security and how to protect the CCCC's IT resources. This can help prevent future violations and ensure that all CCC personnel securely use the CCCC's IT resources.

--- End of INFORMATION TECHNOLOGY SECURITY POLICY ---