Document Number:	POL_3108
Document Name:	Information Technology
Effective Date:	1st Aug 2019
Document Status:	Approved

1.0 Purpose

This policy sets out the responsibilities of RMA employees that apply the use of information technology and software. The purpose is to ensure that RMA's information assets stored on the computing network are effectively protected from unauthorized access and that licensed software is used in full compliance with the applicable agreements.

Guidelines for acceptable use of the Internet and e-mail are provided in the Code of Business Conduct and Ethics.

2.0 Policy Details

Every employee has responsibility for the proper use and protection of RMA's equipment and information. It is your duty to ensure that RMA's computing and communications resources are used for their intended business purpose and that information contained on or transmitted with these resources is protected from unauthorized access.

Confidentiality

Electronic communication, unless protected by special measures such as encryption, is not secure. There is no guarantee of the confidentiality or the privacy of any communication you send over the Internet or other external system. E-mail and attachments may be intercepted, read, stored, copied, modified, and/or redistributed without your knowledge by persons seeking unauthorized access to information or to computer networks. If you have sensitive information to transmit, you should find other means or consult with the for assistance.

Confidential information should not be left as voice messages on internal or external systems. When using a cell phone in a public place, be careful not to disclose confidential information about RMA.

The Executive Director is responsible for ensuring that all RMA data and records are removed from any computer that is taken from RMA's premises for servicing or disposition.

Network Access

Employees and other authorized users are given access to RMA's systems and data based on their business needs, subject to prior approval from the Executive Director. Access requires the use of a personal identifier and confidential password. You must not display your password or share it with others. You are fully accountable for all actions taken with the use of your confidential password.

The Executive Director is responsible for disabling network access for employee and contractor terminations.

Remote access to RMA's network will be granted only where there is a justifiable business need and approval from the Executive Director. If you have remote access, you are responsible for using the remote computer with appropriate care for the security of the information you are handling.

Software

Only software that is licensed for use by RMA shall be installed on the RMA's computers, and strict compliance with the terms and conditions of the licensing agreements is required. Employees must not:

- Install software from any source on an RMA workstation, network or portable computer unless specifically directed by the Executive Director. This applies to software downloaded via the Internet, including shareware and games.
- Duplicate any licensed software or related documentation. Duplication of software for back-up purposes may be done only by the Information Technology Manager.
- Give RMA's software or user documentation to other parties such as contractors, consultants and program participants.

All software acquired by RMA must be purchased through the Executive Director. Software acquisition channels are restricted to ensure that RMA has a complete record of all software that has been purchased for the RMA's computers and can register, upgrade and support the software accordingly.

The Executive Director will make both scheduled and random audits of RMA computers to monitor compliance with this policy.

Data and Network Recovery

The Executive Director is responsible for making back-ups of corporate data, storing the data in a secure off-site facility, and maintaining data restoration capability.

Data that is stored on the local drive of a computer is not subject to data back-up. When you are using the computer without a direct or remote connection to RMA's network, you are responsible for transferring data from the local drive to a network directory as soon as possible. Failure to do so exposes RMA to the risk of losing valuable data.

3.0 Policy Scope

This Policy applies to Rocky Mountain Adaptive Sports Centre ("RMA"). The term "employees" is used to refer collectively to the employees, volunteers, directors and officers of RMA, and consultants, contractors and other persons engaged by RMA to act on its behalf.

4.0 Related Policies

POL_3100_ Operations Policies_General_Code of Business Conduct and Ethics

5.0 Policy Owner

Board Chair

6.0 Definitions

N/A

7.0 Procedures

N/A