Policy of Presque Isle Conservation District Board
SUBJECT: COMPUTER USAGE AND CARE
ADOPTED BY THE BOARD OF THE PRESQUE ISLE CONSERVATION DISTRICT ON: ___4/19/2022_____

The following policy shall govern
Computer Usage and Care

Purpose: The objective of this policy is to ensure that each individual to whom a company computer is issued understands proper maintenance and care of the machine assigned to them, and to set in place a process for administering the preparation and issuance of new IT equipment to staff or Directors.

Presque Isle Conservation District (PICD) staff and directors may be issued a laptop computer and/or tablet to empower them to perform their job duties and interface with each other more effectively. The PICD computer will be equipped with necessary hardware and software. All such material is owned by PICD and is intended to be a work resource to be used only in performing PICD job duties. No software of any kind should be purchased or obtained without the express approval of the District Manager. In addition, no software of any kind should be downloaded or installed except by our District Manager or under their supervision.

The use of software and software services that are not authorized by PICD or which have been improperly duplicated and distributed may be a violation of federal copyright laws. Employees shall not violate or knowingly permit the violation of federal copyright law in the use of software, hardware or software services. Unauthorized use or misuse of PICD computers or software may be subject to disciplinary action.

Reporting Problems or Operational Needs:
Problems or Operational needs related to the computer or network access should be promptly reported to the District Manager via email at presqueisle.cd@gmail.com with a detailed description of the problem or need, including a full description of any error messages received and screenshots when possible. For issues requiring immediate attention or if the issue includes not being able to access their computer or the wireless network at the PICD office, the employee should call the office number at 989-734-4000 if the District Manager is not present.

General Use of PICD Computers and IT Equipment:
• Use of PICD equipment should be for PICD purposes only, and each computer should be used only by the person to whom it is assigned. Reasonable and prudent personal use is permitted provided it does not interfere with work or jeopardize IT security.
• It is the responsibility of each person assigned a PICD computer or other equipment to protect the property and to keep it safe and secure at all times, especially while traveling. Never leave your computer or case unattended or unprotected.

• Employees should not plug their phone into their computer or tablet for charging as phones can be vectors for viruses.

Care of IT Equipment:

• IT equipment including hardware such as laptops, tablets, keyboards, monitors, WiFi/hotspot units, and modems should be protected from prolonged heat exposure or high fluctuations in temperature, and should be protected from spills and drops. Computers should be transported at all times in an appropriately padded bag, and should at no time have any items stacked on them. The equipment should be kept clean using appropriate cleansing materials.

• The equipment should be used in such a manner as to prevent damaging electrical spikes and surges; this means using surge protectors whenever possible.

• Any damage, obvious or suspected, should immediately be reported to the District Manager to prevent further damage over time, and an appointment should be immediately scheduled to have the item checked over.

• If a laptop is showing any signs of battery issues such as not charging properly or not holding a charge, the employee should promptly contact the District Manager.

• Under no circumstances should anyone attempt to take any action to repair or modify PICD equipment or the router without express approval by the District Manager.

• Under no circumstances should access to computers or IT equipment be granted to a non-PICD individual without the express consent of the District Manager or a Director.

Procedure for Acquiring New Software Downloads:

In the event that new software is needed, a request to purchase, install, add or download software must first be approved by the District Manager (and also by the Board if it is over $250), and if approved, will be authorized and purchased by the District Manager. Installations of any kind must then be performed or approved by the District Manager. Original software should be given to the District Manager for storage.

Procedure for Backing up Data:

Each employee using a laptop is responsible for backing all active work stored locally on their laptop or tablet.

Maintenance of Equipment: Laptops should undergo routine updates automatically and will prompt the user when a restart is needed.

Guidelines for Data Protection and Management:

- Each employee is individually responsible for protecting and securing access to PICD data and computers.

PICD employees may not:

• Release any PICD data or information to any person without the express prior approval or direction from the District Manager or a Director.

• Seek to benefit personally, directly or indirectly, or permit others to benefit, directly or indirectly, from any data or information which has come to the employee by virtue of their work assignment or employment at PICD.

• Knowingly include or cause to be included in any record or report any false, inaccurate or misleading data or entry.

• Remove or cause to be removed copies of any data, official record or report from any file from any person or from the PICD office or location where it is kept, except as authorized in the performance of an employee's duties.

• Operate or request others to operate any of PICD's equipment for personal business or gain.

• Make copies of software or literature in violation of copyright law or PICD policy.

• Abuse or permit abuse of PICD's computer equipment.

• Aid, abet, or act in conspiracy with another to violate any part of these guidelines.

• Share passwords with any other person.

_____[*Ralph Viegelahn*]_____Chairperson