Village of Avoca – Personal Identifiable Identification

Purpose:	PII – Personal Identifiable Identification					Policy	#31
Effective:	September 1, 2023		Author: Eric R. Tyner				
Approved by Board:	Mayor: ERT	Trustee: DJR	Trustee: MMRS	Trustee: LJG	Trustee:	Filed: 8-12-23	Clerk: CK

I. Purpose:

The purpose of this policy is to ensure the safe and effective use of the internet and information technology (IT) resources by all employees, contractors, and visitors of the Village of Avoca. The policy outlines acceptable use and defines the responsibilities of all individuals accessing the organization's network and IT resources. By adhering to this policy, we can protect our information assets and prevent security incidents. Being informed is a shared responsibility for all users of the Village of Avoca's information systems. Being informed means, for example:

1. Knowing these acceptable use policies and other related rules and policies,
2. Knowing how to protect your data and data that you are responsible for,
3. Knowing how to use shared resources without damaging them,
4. Knowing how to keep current with software updates,
5. Knowing how to report a cyber event or incident (e.g., phishing attempt., ransomware attack, or other suspicious activity)
6. Participating in training.

II. Policy:

The policies and procedures specified in this policy apply to all Village of Avoca's information, computer systems, and data that are used for official Village of Avoca business regardless of location. Compliance with this policy is mandatory for all employees, contractors, and visitors of the Village of Avoca.

1. Authorized Use

Users must not use other users' passwords, user IDs, or accounts, or attempt to capture or guess other users' passwords. Users are also restricted from using business equipment for personal use, without authorization from the Village of Avoca. Users must not hide their identity for malicious purposes or assume the identity of another user.

2. **Privacy**

User files may be subject to access by authorized employees of the Village of Avoca during official business. Accordingly, users should have no expectation of privacy, and their activity may be monitored.

3. **Restricted Access**

Users must not attempt to access restricted files or portions of operating systems, security systems, or administrative systems to which they have not been given authorization. Accordingly, users must not access without authorization: electronic mail, data, programs, or information protected under state and federal laws. Users must not use IT resources for personal gain or profit. Nor can users release another person's restricted information.

4. **Proper Use of Resources**

Users should recognize that computing resources are limited, and user activities may have an impact on the entire network. They must not:

a. send unsolicited emails, spam, or phishing emails. Email usage should be professional and appropriate.
b. use audio, video, or real-time applications such as weather monitoring, internet radio, video streaming (e.g., Netflix, Amazon Video), or social media (e.g., TikTok, Facebook, Twitter).

5. **Protecting Information and Shared Resources**

The Village of Avoca recognizes the importance of securing various types of information. Users must:

a. Use strong passwords and follow password guidelines.
b. Follow established procedures for protecting files, including managing passwords, using encryption technology, and storing backup copies of files.
c. Protect the physical and electronic integrity of equipment, networks, software, and accounts on any equipment that is used for Village of Avoca's business in any location.
d. Not visit non-business-related websites.
e. Not open email from unknown senders or email that seems suspicious.
f. Not knowingly introduce worms, viruses, or other malicious code into the system; nor disable protective measures (i.e.: antivirus, spyware firewalls).
g. Not install unauthorized software.
h. Not send restricted or confidential data over the Internet or off your locally managed network unless appropriately encrypted.
i. Not connect unauthorized equipment or media, which includes but is not limited to laptops, thumb drives, removable drives, wireless access points, PDAs, and MP3 players.

6. Civility

The use of the internet and related technologies to access, transmit or receive materials that are offensive, harassing, obscene, or otherwise illegal is prohibited. Examples of such material include, but are not limited to, pornographic materials, discriminatory material, pirated software, copyrighted material without permission, and threatening material.

7. Applicable Laws

Users must obey local, state, and federal laws, including laws on copyright, intellectual property, and notification laws. The Village of Avoca is required to protect and secure various types of information as defined in the Federal Trade Commission Identity Theft Act Red Flag Legislation ("FTC Act"), the Criminal Justice Information Services Security Policy and through contractual obligations related to merchant services (credit card acceptance). The Village of Avoca must abide by the New York State Technology Law § 208, which requires notifying any users of a loss of confidentiality of private information.

III. Enforcement

Violations of this policy may result in disciplinary action up to and including termination of employment, revocation of access rights, and/or legal action. The Village of Avoca reserves the right to monitor all internet and technology usage to ensure compliance with this policy.

IV. Acknowledgment:

All users must acknowledge that they have read and understand this policy and agree to comply with its provisions.