WARREN TOWNSHIP
MIDLAND COUNTY, MICHIGAN

Technology Use and Information Security Policy

Policy No.: 1001
Adopted: July 20, 2026
Effective: July 20, 2026
Supersedes: None
Status: Adopted by the Warren Township Board

1. Purpose

Warren Township uses computers, email, mobile devices, cloud services, websites, and other technology to conduct public business. This policy establishes practical rules for using those resources responsibly, protecting Township information, preserving public records, and reporting security problems.

The policy is intended to be proportionate to a small township. It establishes minimum expectations without requiring the Township to purchase or operate technology it does not have.

2. Who and What This Policy Covers

This policy applies to every person who uses Township technology or conducts Township business through technology, including employees, elected and appointed officials, board and commission members, volunteers, contractors, consultants, and vendors (collectively, "users").

"Township technology" includes Township-provided or Township-managed computers, phones, tablets, networks, email accounts, websites, social-media accounts, software, cloud services, storage, printers, scanners, telephone and voicemail systems, credentials, and data. This policy also applies when a personal device, account, or service is used for Township business.

"Technology Administrator" means the Township official, employee, contractor, or service provider designated by the Township Board or an official acting within lawful administrative authority to administer a Township system. The title does not create a new Township office or transfer any statutory duty.

3. Acceptable Use

Township technology is provided primarily for official Township business. Users shall exercise good judgment, professionalism, and reasonable care.

Incidental personal use is permitted only when it:

- is brief and does not interfere with Township duties or operations;
- creates no material cost, security risk, or legal exposure for the Township;

- does not use confidential or nonpublic Township information; and
- complies with this policy and all other applicable laws and Township policies.

The Township may limit or discontinue personal use at any time. No user may use Township technology in a way that suggests the Township endorses a personal opinion, business, product, candidate, or political campaign.

4. Prohibited Use

Users shall not:

- engage in unlawful, threatening, discriminatory, harassing, obscene, or fraudulent activity;
- access, alter, disclose, destroy, or attempt to obtain information or systems without authorization;
- share passwords, multi-factor authentication codes, or accounts, or approve an unexpected sign-in request;
- bypass or disable security controls, monitoring, filtering, updates, backups, or protective software;
- install software, browser extensions, applications, equipment, or remote-access tools without authorization;
- connect an unknown or untrusted storage device to Township equipment;
- send confidential, personal, financial, election-security, law-enforcement, personnel, or other protected information through an unapproved account or service;
- use Township technology for private business, personal financial gain, campaign fundraising, electioneering, cryptocurrency mining, or other activity unrelated to Township business;
- knowingly introduce malware or continue using a device or account after signs of compromise without reporting it;
- impersonate another person or misrepresent a personal statement as an official Township position; or
- delete or alter a Township record contrary to an approved retention schedule, a Freedom of Information Act request, litigation hold, audit, investigation, or preservation instruction.

5. Accounts and Basic Security

Each user is responsible for activity performed through the user's assigned accounts and devices.

Users shall:

- use a long, unique password or passphrase for each Township account and never reuse a Township password for a personal account; a password should be at least 15 characters where the system permits;
- enable and use multi-factor authentication for every Township account capable of interactive user sign-in, including email, banking, financial, payroll, website, domain, cloud, social-media, remote-access, and administrative accounts, and never disable or bypass it;
- use an approved password manager when the Township makes one available;
- keep devices reasonably secured, supported, and updated, and lock the screen when the device is unattended;

- use only Township-approved accounts, storage, software, and methods for Township information;
- verify unexpected requests involving money, bank information, credentials, gift cards, sensitive information, or account changes through a known and separate communication method; and
- immediately report a lost device, suspicious sign-in, phishing message, mistaken disclosure, malware warning, or other suspected incident under Section 11.

Passwords shall be changed promptly when compromise is known or reasonably suspected. The Township should not require arbitrary periodic password changes or complex character formulas unless a particular system requires them.

The Township shall select new and replacement services that support multi-factor authentication. Continued use of an existing service that cannot support multi-factor authentication requires a documented exception under Section 12 and reasonable compensating safeguards. Noninteractive service credentials, application tokens, and similar machine credentials shall be individually protected, limited to the minimum necessary access, and replaced promptly when compromise is known or reasonably suspected.

6. Township Information and Public Records

Users may access confidential, personal, or nonpublic information only as needed for their authorized Township duties. Such information shall not be disclosed except as authorized by law and the responsible Township official.

A writing prepared, owned, used, possessed, or retained by the Township in the performance of an official function may be a public record under the Michigan Freedom of Information Act, regardless of whether it is created or stored on a Township or personal device or account. Not every electronic communication is necessarily a public record, and applicable exemptions may protect some records from disclosure. The Township's FOIA Coordinator and legal counsel determine how the Township responds to a request.

Users shall:

- use a Township email account for Township business whenever one is provided;
- promptly transfer Township-business communications created on a personal account or device into an approved Township system when reasonably possible;
- cooperate with the Township Clerk, FOIA Coordinator, and legal counsel in locating and preserving responsive records;
- immediately forward any FOIA request received directly to the Township's FOIA Coordinator;
- retain and dispose of records only under applicable, approved State of Michigan retention and disposal schedules and Township procedures; and
- preserve potentially relevant information immediately upon notice of a FOIA request, claim, lawsuit, audit, investigation, or legal hold.

Automatic forwarding of Township email to a personal or outside account is prohibited unless specifically authorized in writing for a legitimate operational need.

7. Email, Messaging, and Board Communications

Users shall treat email, text messages, chat, voicemail, and social-media messages concerning Township business as official communications. Messages shall be professional, accurate to the user's knowledge, and sent only to appropriate recipients.

Users shall be alert for phishing. Unexpected links, attachments, password requests, payment instructions, or changes in banking information shall be independently verified before action is taken. A suspicious message should be reported through a known phone number or in person, not by replying to the message.

Members of a public body shall not use email, text messages, group chats, social media, telephone calls, or serial communications to deliberate toward a decision, build consensus, or make a decision outside a meeting conducted in compliance with the Michigan Open Meetings Act. Members shall not conduct private electronic deliberations during an open meeting. Technology may be used for scheduling, distributing agendas or factual background materials, and other administrative communications that do not become unlawful deliberation. Questions about a proposed communication should be referred to the Township attorney.

Rules for operating and moderating an official Township social-media account should be established separately and reviewed by counsel. This policy does not authorize a user to remove public comments or block an account based on viewpoint.

8. Personal Devices and Remote Work

A personal device may be used for Township business when the responsible Township official permits it and the use is reasonably necessary. The device shall:

- use a passcode, password, biometric lock, or comparable access control;
- install supported security and operating-system updates within a reasonable time;
- automatically lock after a reasonable period of inactivity;
- not be shared in a way that exposes Township information to another person; and
- use approved accounts and applications for Township information.

Users shall avoid storing Township information locally on a personal device longer than necessary. A lost, stolen, compromised, or replaced device that has accessed Township information shall be reported immediately.

The Township may remove Township account access or Township-managed data from a personal device when access is no longer authorized. This policy does not authorize the Township to erase unrelated personal content. A user must preserve, return, or transfer Township records and information when requested and when the user's service ends.

The use of a personal device does not prevent a Township-business record from being subject to FOIA, retention, discovery, subpoena, audit, or other lawful process. The Township will seek only information reasonably related to Township business and will use lawful, appropriately limited methods.

Except as expressly permitted by law, the Township will not require a user to disclose a password or other access information for the user's personal internet account.

9. Artificial Intelligence and External Online Services

Artificial-intelligence tools may be used for low-risk assistance, such as brainstorming, formatting, or drafting nonconfidential material, only when the tool and the type of use have been approved by the Township Board, Township Supervisor, or Technology Administrator acting within lawful authority.

Users shall not enter confidential, personal, financial, personnel, election-security, law-enforcement, privileged, password, security-configuration, or other nonpublic information into a public or unapproved AI tool or online service.

AI output shall not be treated as verified. The user remains responsible for independently reviewing accuracy, citations, completeness, bias, confidentiality, accessibility, and legal compliance before the output is relied upon, filed, or released. AI shall not make a final legal determination or a final decision concerning employment, benefits, permitting, taxation, enforcement, or another matter affecting a person's rights.

Inputs and outputs used to perform an official Township function may be Township records and shall be retained when required by an applicable schedule or preservation obligation.

10. Monitoring and Privacy

Township technology and Township accounts are Township resources. To the extent permitted by law, the Township may access, preserve, review, monitor, or disclose information on those resources for maintenance, security, records management, legal compliance, investigation of suspected misconduct, or continuity of operations.

Users should not expect personal privacy in information created, sent, received, or stored through Township technology. Any access or monitoring shall be authorized, reasonably related to a legitimate Township purpose, and conducted consistently with applicable law. This section does not require continuous monitoring and does not eliminate any privacy right provided by law.

11. Reporting and Responding to Security Incidents

Users shall report a suspected security incident immediately to the Township Supervisor or Township Clerk using known official contact information. If the incident may involve the user's email account, the report should be made by phone or in person rather than from that account.

Reportable events include:

- a lost or stolen device used for Township business;
- a suspicious login, unexpected authentication request, or compromised password;
- clicking a suspicious link, opening a suspicious attachment, or sending information in response to a suspected scam;
- malware, ransomware, unusual device behavior, or unauthorized access;
- information sent to the wrong person or exposed through an incorrect permission;
- missing, altered, or improperly destroyed Township records; and
- notice from a vendor of a breach or security problem affecting Township information.

The user should stop the affected activity, disconnect the device from networks if it is safe to do so, preserve relevant messages and evidence, and follow instructions from the Township's designated incident lead or

Technology Administrator. Users shall not conceal an incident or make an external breach notification on the Township's behalf unless authorized.

The Township's designated incident lead shall coordinate appropriate technical, legal, insurance, law-enforcement, records-preservation, and public-notification steps. Whether notice is legally required shall be determined from the facts and applicable law with advice of counsel.

Current official contacts: Township Hall, 4506 W. Baker Road, Coleman, MI 48618; 989-465-9811; supervisor@warrentwpmi.gov; clerk@warrentwpmi.gov. These role-based contacts should be kept current.

12. Administration, Training, and Enforcement

The Township shall provide basic security-awareness information or training appropriate to the access and duties of users. Users shall complete training reasonably assigned as a condition of access to Township technology. Officials and users with access to email, financial, personnel, election, administrative, or confidential systems should receive periodic phishing and account-security refreshers.

Access shall be limited to what a user reasonably needs and shall be changed or disabled promptly when duties change or service ends. Township equipment, records, credentials, and access methods shall be returned or transferred as directed. No departing user may retain a working Township account or the only copy of a Township record.

Violations may result in restriction or loss of access and any other consequence authorized by applicable law, employment policy, contract, appointment terms, or lawful Township authority. Employee discipline shall be handled under applicable personnel procedures. Contractor and vendor violations may be addressed under the applicable agreement. For elected officials, this policy does not create a power of removal, discipline, or censure that the Township does not otherwise possess; however, access to particular Township systems may be limited when reasonably necessary to protect those systems and permitted by law.

An exception to this policy must be documented and approved by the Township Board or an official with lawful authority over the affected resource. An exception may not waive a legal duty.

The Township Board should review this policy at least every two years and after a material change in law, technology, operations, or risk. Technical procedures and contact information may be updated administratively when the policy's substantive requirements are not changed.

13. Effective Date and Construction

This policy takes effect on the date stated above after adoption by the Warren Township Board at an open meeting. It shall be interpreted consistently with applicable federal and Michigan law and other duly adopted Township policies. If a provision conflicts with controlling law, the law controls and the remaining provisions continue in effect to the extent permitted.

Nothing in this policy creates a contract of employment, alters the legal duties or independent authority of an elected office, or guarantees that a Township system will be available, secure, monitored, or backed up at all times.

ACKNOWLEDGMENT OF RECEIPT

I acknowledge that I received and had an opportunity to review the Warren Township Technology Use and Information Security Policy. I understand that I am responsible for complying with the policy when I use Township technology or conduct Township business through technology. I understand that questions should be directed to the Township Supervisor, Township Clerk, or designated Technology Administrator.

I understand that this acknowledgment confirms receipt and understanding; it does not waive any right or alter any duty established by law.

Name: _____

Position or role: _____

Signature: _____

Date: _____