

TODD COUNTY BOARD OF COMMISSIONERS

A RESOLUTION ADOPTING INFORMATION TECHNOLOGY POLICIES

Article I. Information system use policy	1
Section 1.01 Purpose and source of authority.....	1
Section 1.02 Scope.....	1
Section 1.03 Applicability	1
Section 1.04 Definitions.....	1
Section 1.05 County’s right to inspect and monitor information systems.....	2
Section 1.06 Acceptable use of information systems	2
Section 1.07 Superseding statement	2
Section 1.08 Policy interpretation/clarification	2
Section 1.09 Hardware and software	3
Section 1.10 Retention and system back-ups.	4
Article II. Email access and use.....	4
Section 2.01 Scope.....	4
Section 2.02 Account activation/termination.....	4
Section 2.03 General expectations of end users.....	5
Section 2.04 Appropriate use.....	5
Section 2.05 Inappropriate use.....	5
Article III. Internet access and use.....	6
Section 3.01 Scope.....	6
Section 3.02 Access levels.....	6
Article IV. Employee remote use.....	7
Section 4.01 Scope.....	7
Section 4.02 Access levels.....	7
Section 4.03 Policy and appropriate use	8
Section 4.04 Remote access of personally owned devices	8
Article V. Cellular Phone Use (<i>revised 11/19/19</i>).....	9
Section 5.01 Purpose.....	9
Section 5.02 Business use justification requirements	9
Section 5.03 Shared cellular phone.....	9
Section 5.04 Individual assignment and self management	9
Section 5.05 Employee acknowledgement of receipt of cellular phone	9
Section 5.06 Public information	9
Section 5.07 Use of county cell phones for personal use	10
Section 5.08 Safety and Use	10
Section 5.09 Report of lost or stolen device	10
Article VI. Reporting misuse, failure to comply and harassment	10

WHEREAS, it is the responsibility of the Todd County Board of Commissioners to establish appropriate policies regarding use of County technology resources.

NOW, THEREFORE BE IT RESOLVED, that the following information technology policies are adopted:

Article I. Information system use policy

Section 1.01 Purpose and source of authority

The purpose of this policy is to provide clear guidelines to all employees, elected officials and individuals appointed by the County Board regarding appropriate use of and access to County Information Systems, to protect Todd County Information Systems' security and assets, to manage Todd County Information Systems and to protect the right of appropriate access to public data under the Minnesota Government Data Practices Act, Minn. Stat. §13.01 et seq., and the Government Records Administration Act, Minn. Stat. § 138.17.

Section 1.02 Scope

- (a) The County's Information Systems are County-owned and publicly funded. The County's Information Systems and the information conveyed therein are the property of the County. Access to and use of the County's Information Systems is restricted by this Information Systems Use Policy. Todd County expects that all users will use the County's Information Systems responsibly.
- (b) The County's expectations regarding use of Information Systems apply to use within Todd County facilities and to remote access of County Information Systems from a non-County facility.
- (c) All equipment that uses the information systems is by definition the property of Todd County, regardless of the department or funding source used in purchase of said equipment. The only exception is if equipment is purchased and placed by the state/federal government and is intended for use by a county agency, then the state/federal government is the property owner of the hardware/software until it is released by those government units to the county or other government units.
- (d) This policy applies to any user of the county's information systems or system data for any purpose. By using the county's information systems, the user(s) agree to be bound by the terms and conditions of this policy. The responsibility lies with the individual user.
- (e) Every individual who uses an information system must sign the Agreement for Information Systems Use annually. A copy of the signed agreement will be kept in the individual employee's personnel file and updated annually.

Section 1.03 Applicability

All county employees, elected officials, appointed individuals and other users of County owned technology equipment or resources. Adoption

Section 1.04 Definitions

In this document, the following terms shall be defined as follows:

- (a) **"County"** means overall governing agency, with respect to the Todd County Board of Commissioners as decision-makers.
- (b) **"Employee(s)"** means a full-time, part-time, temporary and seasonal employee, elected and appointed officials, appointed individuals, volunteers and interns.
- (c) **"User"** means any authorized individual using the information system, both public and

employed by the county.

- (d) **“Authorized individual”** means any user given permission by a county board official, Department Head or supervisor to complete a specific task.
- (e) **“Information systems”** means any system(s) used to create, store, send, and receive data, and all its peripherals.
- (f) **“Data”** means any and all information received, sent, stored, processed, transferred, or communicated in any way by or through the county information systems.
- (g) **“Designee”** means a person appointed by the county for a certain function.
- (h) **“Remote access”** means any connection to county information systems from a location other than user’s designated work area.
- (i) **“Inactivity”** means taking no action or not acting (i.e. if scanning for viruses is part of the policy, then not scanning would be inactivity).

Section 1.05 County’s right to inspect and monitor information systems

Todd County and/or designees may monitor and inspect all information system activity with or without notice, and therefore, users should have no expectations of privacy in the use of these resources.

Section 1.06 Acceptable use of information systems

Todd County provides the use of information systems to conduct the business of the organization. Use of these systems will be granted by the County Administrator, Department Heads and/or Supervisors with regard to job function. Once given access, users are expected to use these systems in a responsible manner at all times. All usage should be able to withstand public scrutiny without embarrassment to Todd County. Usage which appears to be criminal in nature will be turned over immediately to the responsible legal authorities.

- (a) Acceptable information systems uses are those that conform to the purpose, goals and mission of the agency and to each employee’s job duties and responsibilities.
- (b) Use of the information system by anyone other than an employee, user or authorized individual is prohibited.
- (c) Activity or inactivity that results in additional costs due to loss of time or resources or use of information systems that does not fit the above criteria is in violation of this policy.

Section 1.07 Superseding statement

This policy supersedes the previous computer use policy and any other policies or practices written or otherwise conveyed.

Section 1.08 Policy interpretation/clarification

Employees needing clarification of this policy as it relates to the use of information systems are required to present their questions to their Department Head or supervisor. If the Department Head or supervisor cannot answer the question, then the question will be submitted in writing to the MIS Director for presentation to the County Administrator for clarification and resolution.

Section 1.09 Hardware and software

Only Todd County employees are authorized to use Todd County information systems. Todd County permits supervised use of information systems by other authorized persons when such use is pre-approved by the MIS Director.

- (a) **Hardware.** If an employee needs to use computer equipment in a department other than the one to which he or she is assigned, the employee must obtain prior approval from the employee's Department Head and the Department Head in the other department. MIS personnel are exempt from this provision if such use is necessary to perform required work duties.
- (b) **Software.** Use of software applications on Todd County's information systems must be in accordance with the license agreements that govern the use of each software application.
 - (i) All software installation must be pre-approved by the MIS Department. This ensures proper licensing compliance for Todd County. This also allows for a record of possible computer issues posed by the installation/download.
 - (ii) Todd County employees may not reproduce or copy licensed software to any storage media unless for backup or archival purposes or when authorized by the software developer or manufacturer.
 - (iii) No software should be downloaded and directly installed by the end-user without approval from the MIS Department. All downloaded software poses a threat of virus to the county. There is also a threat of adware/malware/spyware being installed unintentionally when the selected software is downloaded. Software found on a system that was not pre-approved by the MIS Department will be promptly removed and documented. A copy of the documentation will be provided to the appropriate Department Head and further disciplinary action may be taken if necessary.
- (c) **Virus protection.** The MIS Director is authorized to take necessary measures to protect Todd County's information systems from virus infection.
 - (i) All computers attached to the Todd County network must have standard, supported antivirus software installed. This software must be active, be scheduled to perform virus checks at regular intervals, and have its virus definition files kept up to date.
 - (ii) Any activities with the intention to create and/or distribute malicious programs onto the Todd County network (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.) are strictly prohibited.
 - (iii) If an employee receives what he/she believes to be a virus, or suspects that a computer is infected with a virus, it must be reported to the MIS Department immediately.
 - (iv) No employee should attempt to destroy or remove a virus, or any evidence of that virus, without direction from the MIS Department.
 - (v) Any virus-infected computer will be removed from the network until it is verified as virus-free.
 - (vi) Never open any files or macros attached to an e-mail from an unknown,

- suspicious, or untrustworthy source.
- (vii) Never open any files or macros attached to an e-mail from a known source (even a coworker) if you were not expecting a specific attachment from that source.
 - (viii) Be suspicious of e-mail messages containing links to unknown Web sites. It is possible that the link is a malicious executable (.exe) file disguised as a link. Do not click on a link sent to you if you were not expecting a specific link.
 - (ix) Files with the following filename extensions are known to potentially carry a virus: exe, bat, pif, scr, and double extensions (doc.pif for example).
 - (x) Never copy, download, or install files from unknown, suspicious, or untrustworthy sources or removable media.
 - (xi) If instructed to delete e-mail messages believed to contain a virus, be sure to also delete the message from your Deleted items or Trash folder.

Section 1.10 Retention and system back-ups.

- (a) Individual computers are not backed-up by the MIS Department. Individual computers will be backed-up in accordance with departmental guidelines, when necessary. Data that is specific to individual computers, should be archived to a network drive or hard copy maintained if necessary to retain the data. If data retention is not necessary, the data should be cleaned from the system.
- (b) Data that needs to be retained is to be stored on a file server. The MIS Department is responsible for the backup of centralized servers. In special circumstances where servers are not centralized within MIS but within specific departments, trained and authorized office personnel will perform the backup duties, with assistance given by the MIS Department when necessary.

Article II. Email access and use

E-mail is a critical mechanism for business communications at Todd County. Use of Todd County's electronic mail systems must be in accordance with the goals of the county. The objectives of this policy are to outline appropriate and inappropriate use of Todd County's e-mail systems in order to minimize disruptions to services and activities, as well as comply with applicable policies and laws.

Section 2.01 Scope

This policy applies to all e-mail systems and services owned by Todd County, all e-mail account users/holders at Todd County and all county e-mail records.

Section 2.02 Account activation/termination.

- (a) E-mail access at Todd County is controlled through the MIS Department using individual accounts and passwords.
- (b) Employees will be given e-mail access when the appropriate Department Head authorizes and notifies the MIS Department.
- (c) E-mail access will be terminated when the employee terminates their association

with Todd County, unless other arrangements are made (such as temporary forwarding of account information to other county staff).

- (d) Todd County is under no obligation to store or forward the contents of an individual's e-mail account including address book to the employee after the term of their employment has ceased.

Section 2.03 General expectations of end users.

- (a) Employees of Todd County with e-mail accounts are expected to check their e-mail in a consistent and timely manner so that they are aware of important county announcements and updates, as well as for fulfilling county tasks. Arrangements should be made in the case of absences so that communications are answered in a timely manner.
- (b) E-mail users are responsible for mailbox management, including organization and cleaning.
Users are expected to have a reasonable amount of knowledge to complete these tasks.
- (c) E-mail users are also expected to comply with normal standards of professional and personal courtesy and conduct.

Section 2.04 Appropriate use.

Individuals at Todd County are encouraged to use e-mail as a means of communication. The types of activities that are appropriate include:

- (i) Communication with county employees and business contacts;
- (ii) Communication with the public as needed and deemed appropriate;
- (iii) Communication with other business-related officials.

Section 2.05 Inappropriate use.

- (a) Todd County's e-mail systems and services are not to be used for purposes that cause excessive strain on systems.
- (b) Individual e-mail use will not interfere with others' use of Todd County's e-mail system and overall network system.
- (c) E-mail use at Todd County will comply with all applicable laws, all Todd County policies, and all Todd County contracts.
- (d) The following activities are inappropriate uses of Todd County systems and services and are prohibited:
 - (i) Use of e-mail for illegal or unlawful purposes, including but not limited to copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, soliciting for illegal pyramid schemes, and computer tampering (e.g. Spreading of computer viruses).
 - (ii) Use of e-mail to produce or forward chain letters or group personal e-mails.
 - (iii) Viewing, copying, altering, or deletion of e-mail accounts or files belonging to Todd County or another individual without authorized permission.
 - (iv) Sending of unreasonably large e-mail attachments. The total size of an

individual e-mail message sent (including attachment) should be six megabytes or less. If larger attachments need to be sent, contact should be made with the MIS Department.

- (v) Opening e-mail attachments from unknown or unsigned sources. Attachments are the primary source of computer viruses and should be treated with caution. All work-related attachments must be scanned prior to opening. Only work-related attachments should be opened. It is the responsibility of the individual to know the type of attachment that they are opening. If unsure, contact must be made with the MIS Department prior to opening. Sending and receiving of personal attachments is prohibited.
- (vi) Excessive personal use of Todd County e-mail resources. Todd County allows limited personal use so long as it does not interfere with staff productivity, preempt any business activity, or consume more than a trivial amount of resources.
- (vii) Todd County prohibits personal use of its e-mail systems and services for unsolicited mass mailings, non-Todd County commercial activity, political campaigning, dissemination of chain letters, and use by non-employees.

Article III. Internet access and use

Internet access for Todd County has become a crucial part of daily business. Use of the internet through Todd County's systems must be in accordance with the goals of the county.

Section 3.01 Scope.

This section applies to all systems owned by Todd County connecting to the internet, all activity generated, and all information accessed and created.

Section 3.02 Access levels.

- (a) While some persons may have limited or no access to the internet, others may need full access to fulfill the requirements of their daily job duties. Many applications/programs are now run through secure segments via a web portal.
- (b) Department Heads are responsible for defining appropriate internet access levels for the persons in their department and conveying that information to the MIS Department.
- (c) General expectations of end users:
 - (i) Employees of Todd County are expected to use the internet in a responsible way that will not cause undue strain on the network. Internet use that causes bandwidth degradation is prohibited (e.g. Streaming video non-work related).
- (d) Appropriate use.

Individuals are encouraged to use the internet to further the goals and objectives of Todd County. The types of activities that are encouraged include:

- (i) Accessing or sharing information necessary as related to the performance of an individual's assigned responsibilities;
- (ii) Use of the internet to access work-related programs/applications through secure segments.
- (iii) Use of the internet to access web training as it relates to job function.

(e) Inappropriate use.

Individual internet use will not interfere with others' use of the network system.

- (i) Users will not violate the network policies of any network accessed through Todd County systems.
- (ii) Internet use at Todd County will comply with all federal and state laws, all Todd County policies, and all Todd County contracts. This includes, but is not limited to, the following:
 - 1) The internet may not be used for illegal or unlawful purposes, including, but not limited to, copyright infringement, discrimination, obscenity, pornography, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, illegal gambling, soliciting for illegal pyramid schemes, and computer tampering (e.g. Spreading computer viruses).
 - 2) Use of the internet that causes strain on the network due to non-work related activity, e.g. Access streaming video for non-work functions. Internet use must not consume more resources than necessary to complete a job-related function.
 - 3) Excessive personal use of Todd County internet resources. Todd County allows limited personal use as long as it does not interfere with staff productivity, preempt any business activity, or consume more than a trivial amount of resources. Todd County prohibits use of the internet for non-employees.

Article IV. Employee remote use

Remote access may be necessary for Todd County information system users due to on-call status and 24-hour coverage needed in some areas, and also vendor support. Because of this need, Todd County may provide this access, and also provides guidelines to protect the county's network resources wherever the connection may come from.

Section 4.01 Scope

This policy applies to all Todd County employees, elected officials or appointed individuals who utilize Todd County or personally owned computers to remotely access the organization's data and networks. Any and all work performed for Todd County on said computers through a remote access connection of any kind, is covered by this policy. Work can include (but is not limited to) e-mail correspondence, application access, web access, utilizing intranet resources, and any other county application used over the internet. Remote access is defined as any connection to county information systems from a location other than user's designated work area.

Section 4.02 Access levels

Department Heads, along with the MIS Department will determine the need for remote access to the Todd County network. Passwords will be assigned for these remote connections. It is the responsibility of the user to ensure the password is protected and kept private. If a user feels a password has been compromised, the user must contact the Department Head and the MIS

Department immediately. It is the responsibility of the Department Head to contact the MIS Department when an employee terminates employment with the county to ensure remote access is removed promptly and system security is maintained.

Section 4.03 Policy and appropriate use

It is the responsibility of any individual subject to this policy with remote access privileges to ensure that their remote access connection remains as secure as his or her network access within the office. It is imperative that any remote access connection used to conduct Todd County business be utilized appropriately, responsibly, and ethically. Therefore, the following rules must be observed:

- (a) Remote access for users through Todd County's network for recreational purposes is prohibited.
- (b) Employees will use secure remote access procedures established by the MIS Department. Employees agree to never disclose their passwords to anyone, particularly to family members if business work is conducted from home.
- (c) All remote computer equipment and devices used for business interests must display reasonable physical security measures. Computers will have installed whatever antivirus software deemed necessary by Todd County's MIS Department.
- (d) Employees will make no modifications of any kind to the remote access connection without the express approval of Todd County's MIS Department.
- (e) Employees with remote access privileges must ensure that their computers are not connected to any other network while connected to Todd County's network via remote access, with the obvious exception of internet connectivity.
- (f) No individual is to use internet access through company networks via remote connection for any unacceptable uses (refer above) and must act in accordance with all employee policies.
- (g) If a personally or company-owned computer or related equipment used for remote access is damaged, lost, or stolen, the authorized user will be responsible for notifying their Department Head and Todd County's MIS Department immediately.
- (h) The remote access user also agrees to immediately report to their Department Head and Todd County's MIS Department any incident or suspected incidents of unauthorized access and/or disclosure of county resources, databases, networks, etc.
- (i) The remote access user also agrees to and accepts that his or her access and/or connection to Todd County's networks will be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. As with in-house computers, this is done in order to identify accounts/computers that may have been compromised by external parties.

Section 4.04 Remote access of personally owned devices

- (a) An individual subject to this policy, who desires to use a personally owned device to access the County's network, must have approval from the MIS Director.
- (b) The County will not offer reimbursement for business use of personal technology resources.
- (c) The individual must acknowledge that under some circumstances, certain data on the personal device may become private.

Article V. Cellular Phone Use

Section 5.01 Purpose

The purpose of this article is to establish county-wide appropriate usage and assignment policies for cellular phones and equipment.

Section 5.02 Business use justification requirements

Cellular phones and service are provided for official county business use only and are made available to employees, elected officials and appointed officials in positions where the associated benefits justify the additional operating costs. The department head, along with MIS Director, shall review and approve requests for cellular equipment and services consistent with the county's internal procedures.

Based on business needs, the Department Head will determine which positions in their departments require a County-issued cell phone. These work-related needs include, but are not limited to:

1. When safety of self or others may be at risk.
2. When the employee's main work location is in the field where land lines and other primary radio/telephone communications are not available.
3. When the employee's work function requires the use of a cell phone.
4. To provide immediate communication with department staff and/or other agencies as required to coordinate programs or to provide customer service.
5. When it improves job performance efficiency.
6. When there is a need to be able to contact the employee on short notice.
7. When the employee's role is related to emergency response.

Section 5.03 Shared cellular phone

Whenever frequency of use does not justify individual assignment, the sharing of county-owned cellular phones is encouraged to reduce costs.

Section 5.04 Individual assignment and self management

When sharing of county-owned cellular phones does not meet operational needs, an employee may be individually assigned cellular phone equipment.

Section 5.05 Employee acknowledgement of receipt of cellular phone

Employees will acknowledge the receipt and acceptance of the conditions for the shared use or individual assignment of a county-owned cellular phone using acknowledgement of receipt cellular phone services and equipment form developed for this purpose. The agency is responsible for keeping the receipt form on file for the duration of the individual assignment of a cellular phone to an employee. When the employee leaves his/her position or is no longer an authorized user, the county cellular equipment must be returned to the employee's supervisor or other designated official.

Section 5.06 Public information

Some call detail (e.g., time, date, duration, cost incurred) of calls appearing on the county cellular phone billing account is public information. Other call detail, such as the number called, may not be public information.

Section 5.07 Use of county cell phones for personal use

The use of county-owned cellular phone equipment and service is intended for county business. Personal use of county-owned cellular phone should be limited to essential personal calls.

- (a) Essential personal calls. Essential personal calls are defined as calls of minimal duration and frequency that are urgent in nature and cannot be made at another time or from a different telephone. Examples of essential personal calls are calls to arrange for care of a child or other family emergency, to alert a family member of an unexpected delay due to a change in work schedule, or to arrange for transportation or service in the event of car trouble.
- (b) Non-essential personal use of a county cellular phone in violation of this policy or agency work rules may result in revocation of the cellular phone assignment and possible disciplinary action against the employee. In addition, employees may be responsible for any charges incurred that are non-essential or excessive use of county cellular phone.

Section 5.08 Safety and Use

For safety reasons, use of a cell phone while driving motor vehicle or operating heavy equipment should be kept to a minimum. Employees should pull off the road or use a hands-free device to conduct business using a cell phone. In all cases, employees shall follow local and State regulations regarding the use of cell phones while operating a motor vehicle.

Section 5.09 Report of lost or stolen device

Employees are required to report a lost or stolen cellular phone immediately. Cellular phone service will be suspended on the device.

Article VI. Reporting misuse, failure to comply and harassment

- (a) Any allegations of misuse should be promptly reported to the Todd County MIS Department, as well as the appropriate Department Head.
- (b) Violations of Todd County's information systems policy will be handled in accordance with the information systems use policy and the Todd County personnel policy.
- (c) Todd County is committed to creating and maintaining a workplace that is free from political, sexual, religious, or other types of harassment. Use of any Todd County information systems to harass others is strictly prohibited. Employees shall not create, send or download any documents, graphics or data that would constitute harassment as defined in the Todd County policy on harassment.