GRATIOT COUNTY BOARD OF COMMISSIONERS

RESOLUTION TO APPROVE INFORMATION TECHNOLOGY POLICY

RESOLUTION NUMBER 26-441
ADOPTED JULY 21, 2026

WHEREAS authority to establish rules and regulations in reference to the management of the interest and business concerns of the county is vested with the Board of Commissioners (MCL 46.11(m)); and

WHEREAS the Board wishes to establish a policy to set forth requirements for the acceptable, secure, and responsible use of information technology resources; and

WHEREAS the proposed policy is intended to protect County systems, data, employees, public records, and technology infrastructure; establish expectations for appropriate use; support compliance with applicable laws, regulations, retention requirements, and cybersecurity standards; and

WHEREAS the proposed policy defines the County's rights regarding access to, monitoring, review, preservation, disclosure, and removal of information created, received, transmitted, stored, or accessed through County IT resources.

THEREFORE, BE IT RESOLVED, that the Gratiot County Board of Commissioners hereby adopts the attached Information Technology Policy.

BE IT FURTHER RESOLVED that this policy supersedes all previous Information Technology policies and/or past practices which are hereby rescinded.

BE IT FURTHER RESOLVED that this policy shall have immediate effect.

The resolution set forth was offered by Commissioner _____ and supported by Commissioner_____.

A vote was thereupon taken on the foregoing resolution and the voter for such resolution was as follows:

AYES: _____

NAYS:_____

A majority of the members-elect having approved such resolution deems the resolution APPROVED.

STATE OF MICHIGAN)
)ss
COUNTY OF GRATIOT)

I certify that the foregoing is a true and accurate copy of the resolution adopted by the Gratiot County Board of Commissioners, that such resolution was duly adopted at a regular meeting held on the 21st day of July 2026, and that notice of such meeting was given as required by law.

_____

Angie Thompson, Gratiot County Clerk

General and Administrative Policy No. 1214

Information Technology

Approved: _____

Resolution No. _____

1. **PURPOSE:** The purpose of this policy is to establish requirements for the acceptable, secure, and responsible use of Gratiot County information technology resources. This policy governs the use of County-owned and County-authorized technology resources, including but not limited to computers, networks, Internet access, cloud services, remote access services, mobile devices, telecommunications systems, software, electronic records, and future technologies. This policy is intended to protect County systems, data, employees, public records, and technology infrastructure; establish expectations for appropriate use; support compliance with applicable laws, regulations, retention requirements, and cybersecurity standards; and define the County's rights regarding access to, monitoring, review, preservation, disclosure, and removal of information created, received, transmitted, stored, or accessed through County IT resources. This policy does not constitute a contract. The County reserves the right to modify, suspend, or revoke access to IT resources, and to amend this policy at any time, subject to applicable approval requirements.

2. **AUTHORITY:** Authority to establish rules and regulations in reference to the management of the interest and business concerns of the county is vested with the Gratiot County Board of Commissioners (MCL 46.11(m)).

3. **APPLICATION:** This policy applies to all users of Gratiot County IT resources, including but not limited to employees, elected officials, appointed officials, department heads, agencies, volunteers, court staff, contractors, vendors, temporary workers, and any other individual or entity authorized to access, use, manage, support, or connect to County IT resources. Nothing in this policy is intended to restrict the lawful discretion or statutory duties of elected officials, who retain independent constitutional authority. The County may regulate the use of County owned technology systems but may not impose disciplinary sanctions on elected officials. Judicial officers and courts may adopt additional or superseding evidentiary handling procedures consistent with state law and the Michigan Code of Judicial Conduct.

4. **RESPONSIBILITY:** The County Administrator and Information Technology Director, or their respective designees, shall be responsible for implementation and administration of this policy.

5. **DEFINITIONS:**

   5.1 ***"Administrator"*** means the Gratiot County Administrator or designee.

   5.2 ***"Agency"*** refers to any organization, unit, office, department, court, board, commission, or activity that utilizes Gratiot County IT resources.

5.3 ***"Authorized User"*** means any employee, elected official, appointed official, department head, volunteer, court staff member, contractor, vendor, temporary worker, or other individual who has been granted permission to access or use County IT resources.

5.4 ***"County Data"*** means any information, record, file, communication, image, video, audio recording, credential, report, database entry, electronic message, metadata, or other data created, received, transmitted, accessed, processed, or stored while conducting County business or using County IT resources.

5.5 ***"County-Owned Device"*** means any computer, mobile device, tablet, cellular device, server, storage device, peripheral, network device, or other technology equipment purchased, leased, issued, managed, or maintained by or on behalf of Gratiot County.

5.6 ***"Electronic Communication"*** means any communication created, sent, received, transmitted, stored, or accessed electronically, including but not limited to e-mail, text messages, instant messages, voicemail, video communications, chat messages, collaboration platform messages, social media messages used for County business, and communications transmitted through County systems or personal devices used for County business.

5.7 ***"Information technology (IT) resources"*** means all County-owned, County-managed, County-authorized, or County-connected technology systems and services, including but not limited to computers, servers, networks, Internet access, e-mail systems, telephones, cellular devices, tablets, software, cloud services, remote access services, telecommunications systems, electronic storage, databases, cybersecurity systems, video and voice communication systems, and future technologies.

5.8 ***"Mobile Device"*** means a portable computing or communication device, including but not limited to a smartphone, tablet, cellular-enabled device, hotspot, or similar device.

5.9 ***"Multi-Factor Authentication"*** or ***"MFA"*** means an authentication method that requires a user to verify identity using two or more factors, such as something the user knows, something the user has, or something the user is.

5.10 ***"Personally-Owned Device"*** means any device not owned or leased by the County that is used to conduct County business, access County systems, store County data, transmit County communications, or connect to County networks or services.

5.11 ***"Remote Access"*** means access to County IT resources from outside a County facility or from a non-County network, including but not limited to VPN, remote desktop, cloud-based access, vendor access, administrative access, and other approved remote connection methods.

5.12 ***"User"*** means any individual who accesses, uses, manages, supports, administers, or connects to County IT resources.

6. POLICY:

6.1 General Use and County Ownership of Information. IT resources are provided to support the efficient, secure, and effective operation of Gratiot County government.

6.1.1 Authorized Users shall use IT resources in a responsible, lawful, professional, and secure manner, and primarily for County-related business purposes.

6.1.2 All County Data is the property of Gratiot County, regardless of where it is created, received, transmitted, accessed, processed, or stored. This includes County Data located on County-owned devices, personally owned devices used for County business, County networks, cloud services, e-mail systems, collaboration platforms, telecommunications systems, removable media, backup systems, and any other County-authorized or County-connected technology resource.

6.1.3 Incidental personal use of County IT resources may be permitted when it is limited, reasonable, does not interfere with County business, does not result in additional cost or risk to the County, does not violate this policy or any other County policy, and does not compromise County systems, data, or operations.

6.1.4 Personal information created, received, transmitted, accessed, or stored using County IT resources may be accessed, reviewed, disclosed, or removed in the same manner as other information on County systems. Users are responsible for protecting County IT resources and County Data from unauthorized access, disclosure, modification, loss, or misuse. Users shall comply with all applicable laws, regulations, retention requirements, security requirements, administrative procedures, and County policies when using IT resources or handling County Data.

6.2 Electronic Records, E-Mail, and Retention. Electronic communications and electronic records created, received, transmitted, accessed, or stored while conducting County business are County records and shall be managed in accordance with applicable records retention requirements, County procedures, and legal preservation obligations.

6.2.1 E-mail messages, text messages, chat messages, voicemail, electronic documents, attachments, metadata, transactional information, and other electronic communications may constitute County records when they are created or received as part of conducting County business. The retention period for an electronic record is determined by the content and purpose of the record, not by the technology used to create, transmit, or store it. Users are responsible for managing electronic records in accordance with applicable County procedures, approved records retention and disposal schedules, litigation holds, FOIA requirements, and instructions from the County Administrator, FOIA Coordinator, Legal Counsel, Department Head, or Information Technology Director.

6.2.2 Users shall not delete, alter, conceal, destroy, or remove electronic records when those records are subject to a pending FOIA request, litigation hold, audit, investigation, public records request, court order, or other preservation requirement.

6.2.3 The Information Technology Department may assist with preservation, search, retrieval, backup, migration, and access to electronic records; however, IT system backups are intended primarily for disaster recovery and continuity of operations and should not be treated as the primary method of records retention. Department Heads and elected officials are responsible for ensuring that records created or received by their departments, including records of former employees, are retained and managed in accordance with applicable retention requirements.

6.2.4 Users who conduct County business using personally owned devices, personal accounts, or non-County systems may be required to preserve, search, produce, transfer, or delete County records from those systems as directed by the County, subject to applicable law.

6.3 Authentication, Passwords, and MFA.

6.3.1 Users are responsible for protecting all usernames, passwords, passcodes, security tokens, multi-factor authentication prompts, certificates, and other authentication methods assigned to or used by them.

6.3.2 Users shall not share passwords, passcodes, MFA codes, security tokens, authentication applications, or account access with any other person unless specifically authorized by the Information Technology Director or designee for an approved business or technical purpose.

6.3.3 Users are accountable for activity conducted under their assigned accounts or credentials. Users shall immediately report suspected password compromise, unauthorized account access, unexpected MFA prompts, lost or stolen authentication devices, or other suspected credential misuse to the Information Technology Department.

6.3.4 The County may require MFA for access to County systems, including but not limited to Microsoft 365, remote access, VPN, administrative accounts, privileged systems, cloud services, law enforcement or criminal justice systems, financial systems, and Windows or device sign-in. MFA requirements may vary based on role, system sensitivity, data accessed, legal or regulatory requirements, risk level, and available technology.

6.3.5 When MFA is required, users must enroll in and use County-approved authentication methods. County-approved MFA methods may include authenticator applications, hardware tokens, security keys, passkeys, biometric verification, phone-based verification, or other methods approved by the Information Technology Department.

6.3.6 The County may permit or require an MFA application, passkey, security key, or similar authentication method to be installed, registered, or used on a personally owned device when needed to access County systems. Use of a personally owned device for MFA does not, by itself, authorize the County to access personal content

on the device; however, the user is responsible for maintaining the device in a secure condition and for promptly reporting loss, theft, compromise, or replacement of the device.

6.3.7 Users shall not approve MFA prompts, provide MFA codes, or complete authentication requests unless they are actively attempting to sign in to the applicable County system. Unexpected MFA prompts must be denied and reported to the Information Technology Department.

6.4 Remote Access and Vendor Access.

6.4.1 Remote access to County IT resources is a privilege granted only for approved County business purposes. Remote access may include VPN, remote desktop, cloud-based access, administrative access, vendor access, or any other approved method of connecting to County systems from outside a County facility or from a non-County network.

6.4.2 Remote access must be approved by the user's Department Head or elected official and the Information Technology Director or designee. Remote access for vendors, contractors, non-employees, or other third parties must also be approved by the County Administrator or designee unless otherwise authorized by contract, law, or approved administrative procedure.

6.4.3 Remote access shall be granted only when there is a legitimate business need, such as continuity of operations, emergency response, after-hours support, mobility necessary to perform assigned duties, vendor support, or other County-approved operational need.

6.4.4 Users shall use only County-approved remote access methods, software, devices, authentication methods, and connection procedures. Users shall not establish, install, configure, or use unauthorized remote access tools, remote-control software, VPN services, tunnels, file-sharing services, or other methods that bypass County security controls.

6.4.5 Remote access users must comply with all County IT policies, security requirements, records retention requirements, confidentiality obligations, and instructions from the Information Technology Department. Remote access may be subject to monitoring, logging, session restrictions, MFA requirements, device compliance requirements, time limitations, and other security controls.

6.4.6 Vendor, contractor, and third-party remote access shall be limited to the systems, services, data, and time periods necessary to perform the approved work. The County may require vendor access to be supervised, time-limited, logged, disabled by default, or enabled only upon request.

6.4.7 The Information Technology Department may deny, suspend, revoke, restrict, or terminate remote access at any time when access is no longer needed, approval is

withdrawn, policy requirements are not met, suspicious activity is detected, or continued access presents a security, operational, legal, or compliance risk.

6.4.8 Unauthorized remote access, sharing remote access credentials, allowing another person to use an approved remote access session, or using remote access for non-County purposes is prohibited and may result in revocation of access, disciplinary action, contract remedies, and/or legal action.

6.5 Mobile Devices and Personally Owned Devices.

6.5.1 Mobile devices, including cellular phones, smartphones, tablets, hotspots, and similar devices, may be used for County business only when authorized by the County and when used in compliance with this policy and applicable administrative procedures.

6.5.2 A County-owned mobile device may be assigned when the responsibilities of the position require routine County business outside normal working hours, after-hours response, emergency response, on-call availability, mobility necessary to perform assigned duties, access to County systems or data, or when assignment is otherwise in the best interest of the County.

6.5.3 A personally owned device may be used for County business only when authorized by the employee's Department Head or elected official, the County Administrator or designee where required, and the Information Technology Director or designee. Authorization may be modified, restricted, or revoked at any time.

6.5.4 Use of a personally owned device for County business does not convert the device into County property. However, County Data created, received, transmitted, accessed, or stored on the device remains County property and may be subject to public records laws, FOIA, litigation discovery, court order, retention requirements, audit, investigation, or other legal disclosure obligations.

6.5.5 Users of County-owned devices and users of personally owned devices authorized for County business shall comply with all County security requirements, including but not limited to passcode, encryption, operating system, application, MFA, mobile device management, remote lock, remote wipe, and reporting requirements established by the Information Technology Department.

6.5.6 Users shall not bypass, disable, remove, or interfere with County-required security settings, management software, monitoring tools, device restrictions, or data protection controls on any device used to access County systems or County Data.

6.5.7 Users shall report lost, stolen, replaced, compromised, or unauthorized-accessed mobile devices used for County business in accordance with the reporting requirements of this policy and applicable administrative procedures.

6.5.8 The County may remotely lock, disable, disconnect, remove County access from, or remotely wipe a County-owned device or a personally owned device used for County

business when necessary to protect County systems or County Data, respond to loss or theft, preserve records, comply with legal obligations, or address a suspected security incident. A remote wipe may remove personal data from the device. Users are responsible for backing up personal data separately and acknowledge that the County is not liable for loss of personal data resulting from authorized security or remedial action.

6.5.9 Users shall not use unapproved cloud backup, synchronization, messaging, file storage, or application services to store, transmit, or back up County Data unless approved by the Information Technology Department.

6.5.10 Users shall cooperate with the County in preserving, retrieving, transferring, or deleting County Data from any County-owned or personally owned device used for County business, subject to applicable law. This cooperation may include producing County-related records, providing access to County business content, or following instructions to remove County accounts and data.

6.5.11 The Information Technology Department may provide support for County-owned devices and for County business access or security configuration on personally owned devices. The County is not responsible for supporting personal applications, personal accounts, personal data, personal device hardware, personal cellular service, or other non-County use of personally owned devices.

6.5.12 Users shall comply with applicable laws while using mobile devices, including laws relating to distracted driving. Texting, emailing, or other unsafe use of a mobile device while driving on County business or while operating a County vehicle is prohibited.

6.5.13 Staff making use of Personally Owned Mobile Devices for county employment are eligible for a reimbursement of an amount per month determined by the County Administrator and Information Technology Director. In order to be eligible for reimbursement staff must allow the Information Technology Department to install Mobile Device Management software to their device to ensure that security policies are being adhered to and must fill out the appropriate Reimbursement Form. The user's Department Head or Elected Official must sign off on the Form as budget administrator to approve the use of County funds for reimbursement.

6.6 Software, Cloud Services, and Approved Applications.

6.6.1 Users shall use only County-approved software, applications, systems, cloud services, browser extensions, mobile applications, storage services, remote access tools, and communication platforms when conducting County business or handling County Data.

6.6.2 Users shall not install, download, configure, access, or use unauthorized software, applications, browser extensions, cloud services, remote-control tools, file-sharing services, artificial intelligence tools, synchronization services, backup services,

messaging platforms, or other technology services for County business unless approved by the Information Technology Department.

6.6.3 Users shall not use personal cloud storage, personal e-mail accounts, personal messaging accounts, consumer file-sharing services, or unapproved applications to create, store, transmit, back up, synchronize, or process County Data unless specifically authorized by the Information Technology Director or designee.

6.6.4 Software and services used for County business must comply with applicable licensing, cybersecurity, records retention, privacy, confidentiality, public records, accessibility, and contractual requirements. Users shall not copy, install, distribute, or use software in violation of copyright law, license terms, or County procedures.

6.6.5 The Information Technology Department may restrict, remove, disable, block, or require modification of any software, application, browser extension, cloud service, account connection, device configuration, or technology service that is unauthorized, unsupported, insecure, unnecessary, improperly licensed, no longer needed, or inconsistent with County policy.

6.6.6 Software purchases, subscriptions, renewals, application integrations, and cloud services intended for County business must be reviewed and approved through applicable County purchasing and IT review procedures before acquisition or use. Approval may include review for security, compatibility, licensing, supportability, records retention, legal terms, data ownership, and budget impact.

6.6.7 Users shall not intentionally or carelessly introduce malware, unauthorized scripts, unauthorized automation, or other malicious or disruptive code into County systems. Users shall exercise caution when opening attachments, clicking links, downloading files, approving integrations, granting application permissions, or connecting third-party services to County accounts.

6.6.8 Games, entertainment software, cryptocurrency mining tools, unauthorized scanning tools, hacking tools, peer-to-peer file-sharing tools, or other non-business software shall not be installed, accessed, or used on County IT resources unless specifically authorized for a legitimate County business, investigative, training, or legal purpose.

6.6.9 Users shall conserve County IT resources and shall not use systems, storage, printing, bandwidth, processing capacity, or cloud resources in a wasteful, excessive, disruptive, or unauthorized manner.

6.6.10 Software licensed by or to Gratiot County shall be used only in accordance with applicable license terms, contracts, and County procedures.

6.7 Generative Artificial Intelligence. Generative artificial intelligence ("AI") tools include applications, websites, browser features, software features, chatbots, assistants, automated drafting tools, transcription tools, summarization tools, image-generation tools, code-generation tools, and other systems that create, summarize, analyze, transform, or predict text,

images, audio, video, software code, or other content. AI can create new content and ideas based on prompts, using machine learning models trained on large datasets

6.7.1 Users may use County-approved AI tools for legitimate County business purposes when such use complies with this policy, applicable law, records retention requirements, confidentiality obligations, cybersecurity requirements, and any administrative procedures issued by the County.

6.7.2 Users shall not enter, upload, paste, summarize, transmit, or otherwise disclose nonpublic County Data into any AI tool unless the tool has been reviewed and approved by the Information Technology Department and, where appropriate, Legal Counsel, the County Administrator, or the applicable Department Head or elected official.

6.7.3 Prohibited AI input includes, but is not limited to, security credentials, passwords, MFA codes, criminal justice information, law enforcement sensitive information, protected health information, personnel records, attorney-client privileged information, confidential financial information, personally identifiable information, confidential vendor information, nonpublic security information, or other restricted, confidential, exempt, regulated, or legally protected information.

6.7.4 Users are responsible for reviewing AI-generated content for accuracy, completeness, bias, appropriateness, confidentiality, and compliance with County policy before relying on, sharing, publishing, or using the content for County business. AI-generated content shall not be treated as authoritative without appropriate human review.

6.7.5 AI tools shall not be used to make final employment, disciplinary, law enforcement, benefit, eligibility, procurement, legal, financial, or other official County decisions without appropriate human review and approval by an authorized County official.

6.7.6 Users shall not use AI tools to impersonate another person, misrepresent County authority, create deceptive content, generate malicious code, bypass security controls, conduct unauthorized surveillance, or produce content that violates County policy or applicable law.

6.7.7 AI prompts, outputs, summaries, transcripts, or related records created or used for County business shall be managed in accordance with this policy, applicable retention requirements, and legal preservation obligations.

6.7.8 The Information Technology Department may block, restrict, approve, monitor, or revoke access to AI tools based on cybersecurity, privacy, legal, operational, licensing, or records-management considerations.

6.7.9 Users are responsible for exercising appropriate judgment when relying on information obtained from Internet sources, artificial intelligence tools, or other external sources and should verify information before using it for official County business.

6.7.10 AI tools will be used only in a manner consistent with applicable federal law, Michigan law, County policy, and County security standards. Applicable requirements may include, as relevant, Michigan FOIA and records retention obligations, privacy and security requirements governing PII, PHI, and CJIS, civil rights and employment laws, and contractual or regulatory restrictions applicable to specific data types or functions. Where any law, regulation, contract, or security requirement imposes a stricter standard than this policy, the stricter standard shall govern. Users shall coordinate with the Information Technology Department and County legal counsel, as applicable, in connection with approval, procurement, deployment, and incident response.

6.8 Data Classification, Confidentiality, and Minimum Necessary Access.

6.8.1 Users shall access, use, transmit, disclose, and store County Data only as necessary to perform authorized County duties or approved County business.

6.8.2 County Data may include public, internal, confidential, restricted, regulated, privileged, or legally protected information. Users are responsible for handling County Data according to its sensitivity, applicable law, County policy, records retention requirements, confidentiality obligations, and instructions from the County Administrator, Department Head, elected official, Legal Counsel, FOIA Coordinator, or Information Technology Director.

6.8.3 Confidential, restricted, regulated, privileged, or legally protected County Data shall not be accessed, disclosed, transmitted, copied, removed, photographed, downloaded, synchronized, stored, or shared except for authorized County business and through County-approved systems or methods.

6.8.4 Users shall not access County Data, systems, files, mailboxes, records, applications, or accounts unless they have a legitimate business need and have been authorized to do so. Access to County Data shall be limited to the minimum necessary access required for the user's assigned duties, role, approved project, or authorized support function.

6.8.5 Users shall not access or use County Data for any purpose unrelated to authorized County business.

6.8.6 Users who receive, discover, or access County Data in error shall not further access, use, copy, disclose, or distribute the information and shall promptly report the issue to the Information Technology Department.

6.8.7 Users shall promptly report suspected unauthorized access, disclosure, loss, theft, compromise, or misuse of County Data to the Information Technology Department and their Department Head or elected official.

6.8.8 Users shall not disclose personal, confidential, or nonpublic information about employees, officials, residents, clients, vendors, or other individuals except as authorized for legitimate County business and in accordance with applicable law, County policy, and approved procedures.

6.8.9 The County may restrict, audit, monitor, modify, suspend, or revoke access to County Data or IT resources when necessary to protect County operations, comply with legal requirements, investigate potential misuse, or enforce this policy.

6.9 Information Security and Incident Reporting.

6.9.1 Users are responsible for helping protect County IT resources and County Data from unauthorized access, disclosure, modification, loss, theft, misuse, malware, ransomware, phishing, social engineering, and other cybersecurity threats.

6.9.2 Users shall follow County security procedures, training, system prompts, warnings, and instructions issued by the Information Technology Department. Users shall not bypass, disable, remove, interfere with, or attempt to defeat County security controls, including but not limited to antivirus, endpoint protection, firewalls, web filtering, e-mail security, encryption, logging, mobile device management, MFA, access controls, software restrictions, or monitoring tools.

6.9.3 Users shall promptly report suspected or actual security incidents to the Information Technology Department and their Department Head or elected official, even if they are unsure whether an actual compromise occurred. Reportable incidents include, but are not limited to, suspected phishing, malware, ransomware, lost or stolen devices, unauthorized access, accidental disclosure of County Data, suspicious MFA prompts, compromised passwords, misdirected e-mail containing sensitive information, unusual system behavior, or suspected misuse of County IT resources.

6.9.4 Users shall not attempt to investigate, remediate, delete, forward, conceal, or alter evidence of a suspected security incident unless directed by the Information Technology Department, Legal Counsel, or another authorized County official. Users shall preserve relevant messages, files, logs, devices, and other information when instructed.

6.9.5 The Information Technology Department may take reasonable and necessary action to protect County systems and data, including but not limited to disconnecting devices, disabling accounts, resetting credentials, revoking access, blocking applications or websites, quarantining e-mail, preserving logs, remotely locking or wiping devices, or taking other remedial action.

6.9.6 Unauthorized access, attempted unauthorized access, misuse of County systems, intentional introduction of malicious code, disruption of County systems, unauthorized scanning, unauthorized monitoring, or attempts to evade security controls are prohibited and may result in disciplinary action, revocation of access, contract remedies, and/or legal action.

6.10 Acceptable and Prohibited Use.

6.10.1 Users shall not use County IT resources or County Data to:

a. Violate federal, state, or local law, County policy, court rule, contractual obligation, licensing requirement or administrative procedure.
b. Harass, threaten, intimidate, discriminate against, embarrass, or target another person or organization.
c. Create, access, view, store, solicit, transmit, or distribute obscene, pornographic, sexually explicit, offensive, discriminatory, hateful, or harassing material, except as may be required by authorized law enforcement, prosecutorial, legal, investigative, or other official County duties.
d. Support or oppose political candidates, political parties, or ballot measures in a manner prohibited by law or County policy.
e. Conduct private business, commercial solicitation, unauthorized fundraising, unauthorized advertising, or personal financial gain.
f. Send chain letters, junk mail, spam, mass messages, unauthorized solicitations, or other disruptive communications.
g. Misrepresent identity, impersonate another person, use another person's account, conceal the origin of a communication, or make unauthorized statements on behalf of Gratiot County.
h. Access, copy, disclose, alter, delete, damage, destroy, or remove County Data, systems, files, records, software, or communications without authorization.
i. Attempt to gain unauthorized access to County systems, non-County systems, user accounts, data, networks, applications, or security controls.
j. Introduce malware, ransomware, spyware, unauthorized scripts, unauthorized automation, or other malicious or disruptive code.
k. Interfere with, degrade, disrupt, overload, scan, probe, monitor, or test County systems or networks without authorization.
l. Bypass, disable, evade, weaken, or interfere with security controls, monitoring systems, filtering tools, access controls, logging, MFA, encryption, endpoint protection, or mobile device management.
m. Install, download, store, copy, distribute, or use unauthorized software, copyrighted material, pirated content, or unlicensed applications.
n. Store, transmit, or process County Data using unapproved personal accounts, personal cloud services, removable media, messaging platforms, AI tools, or file-sharing systems.
o. Waste County IT resources, including excessive personal use, unnecessary printing, excessive storage use, excessive bandwidth use, or use that interferes with County operations.
p. Use County IT resources in any manner that creates an unreasonable security, operational, legal, financial, reputational, or compliance risk to the County.
q. Leave open active sessions, unlocked devices, open files, applications, or systems unattended in a manner that could allow unauthorized access to County IT resources or County Data.

6.11 Monitoring, Access, and Administrative Control

6.11.1 Users should have no expectation of privacy when using County IT resources or when creating, receiving, transmitting, accessing, processing, or storing County Data. Personal use of County IT resources, where permitted, may be monitored, accessed, reviewed, disclosed, preserved, deleted, or otherwise managed in the same manner as County business use.

6.11.2 The County may access, monitor, inspect, preserve, retrieve, copy, review, disclose, restrict, remove, or delete information, communications, files, logs, records, accounts, devices, applications, systems, or other IT resources for legitimate County purposes, including but not limited to security, system administration, troubleshooting, compliance, records retention, FOIA, litigation, audit, investigation, continuity of operations, personnel administration, legal obligations, or enforcement of County policy.

6.11.3 The Information Technology Department may monitor, manage, prioritize, restrict, disable, disconnect, quarantine, reconfigure, update, patch, wipe, or remove County IT resources or County access to protect County systems, maintain system integrity, respond to security incidents, preserve records, support operations, comply with legal obligations, or enforce this policy.

6.11.4 The County may monitor network traffic, system activity, device activity, account activity, e-mail and messaging activity, cloud service activity, remote access activity, Internet activity, application activity, logs, and other use of County IT resources, subject to applicable law.

6.11.5 Users shall cooperate with authorized County efforts to access, preserve, retrieve, transfer, secure, or remove County Data from County-owned devices, personally owned devices used for County business, County systems, cloud services, removable media, backups, or other locations where County Data may reside.

6.11.6 Users shall not interfere with, disable, bypass, conceal, alter, delete, or obstruct County monitoring, logging, access, records-preservation, security, administrative, or management controls.

6.12 Public Records, FOIA, Litigation Holds, and Legal Preservation.

6.12.1 County Data, electronic communications, electronic records, metadata, files, messages, attachments, logs, and other information created, received, transmitted, accessed, or stored while conducting County business may be public records and may be subject to the Michigan Freedom of Information Act, records retention requirements, litigation discovery, court order, subpoena, audit, investigation, or other legal disclosure or preservation requirements.

6.12.2 Users shall preserve, produce, transfer, or assist in retrieving County records when directed by the County Administrator, FOIA Coordinator, Legal Counsel,

Department Head, elected official, Information Technology Director, or other authorized County official.

6.12.3 Users shall not delete, alter, conceal, destroy, overwrite, remove, or otherwise make unavailable any County Data or County records that are subject to a FOIA request, litigation hold, court order, subpoena, audit, investigation, records request, or other preservation requirement.

6.12.4 Department Heads and elected officials are responsible for notifying the Information Technology Department and other appropriate County officials when records under their control may require preservation, retrieval, or production due to a FOIA request, litigation hold, employee separation, investigation, audit, or other legal or administrative need.

6.12.5 The FOIA Coordinator, Legal Counsel, County Administrator, Department Heads, elected officials, and the Information Technology Department shall coordinate as needed to identify, preserve, search, retrieve, and produce electronic records in accordance with applicable law and County procedures.

6.12.6 The Information Technology Department may preserve accounts, mailboxes, devices, files, logs, backups, cloud data, or other electronic information when needed to comply with legal, records-management, security, or administrative obligations.

6.12.7 Former employees' County records, including e-mail, files, messages, and other electronic records, shall be retained, transferred, preserved, or disposed of in accordance with applicable retention schedules, legal holds, County procedures, and instructions from authorized County officials.

6.13 Access Authorization, Changes, and Termination.

6.13.1 Access to County IT resources shall be granted, modified, reviewed, suspended, or terminated based on the user's role, job duties, authorized business need, employment status, contract status, legal requirements, security requirements, and approval from appropriate County officials.

6.13.2 Users shall be granted only the access necessary to perform authorized County duties or approved County business. Access may be limited by system, department, role, data type, location, device, time period, authentication method, or other security or operational requirement.

6.13.3 Human Resources is responsible for promptly notifying the Information Technology Department when access is needed, changed, or no longer required. This includes new hires, transfers, promotions, role changes, leaves of absence, separations, retirements, terminations, contract completion, and changes in business need. Department Heads and / or Elected Officials are responsible for notifying Information Technology department when vendor access is needed, changed or no longer required.

6.13.4 The Information Technology Department may require written approval, ticket submission, access request forms, identity verification, MFA enrollment, cybersecurity training, confidentiality acknowledgments, or other documentation before granting or modifying access.

6.13.5 Access for vendors, contractors, temporary workers, volunteers, or other non-employees shall be limited to the systems, data, and time period necessary for the approved purpose. Such access may be disabled by default, time-limited, reviewed periodically, or terminated when no longer required.

6.13.6 Users shall not retain, use, or attempt to use County access after authorization has expired, employment has ended, duties have changed, approval has been revoked, or the approved business need no longer exists.

6.13.7 Upon separation, transfer, reassignment, contract completion, or revocation of access, users shall return County-owned equipment, discontinue use of County accounts and credentials, cooperate with the transfer or preservation of County Data, and follow instructions from the County regarding removal of County access or County Data from personally owned devices.

6.13.8 The Information Technology Department may suspend, restrict, or revoke access when required for security, legal, operational, administrative, disciplinary, or compliance reasons, or when continued access presents a risk to County systems, County Data, or County operations.

6.14 Equipment, Physical Security, and Return of County Property.

6.14.1 County-owned IT resources, including but not limited to computers, mobile devices, tablets, monitors, peripherals, storage devices, network equipment, telecommunications equipment, access devices, software, licenses, and related accessories, are County property and shall be used, protected, returned, transferred, disposed of, and managed in accordance with County policy and Information Technology Department procedures.

6.14.2 Users assigned County-owned IT resources are responsible for using reasonable care to protect such resources from loss, theft, damage, unauthorized access, misuse, or unauthorized transfer. Users shall not loan, transfer, sell, dispose of, donate, relocate, or reassign County-owned IT resources without authorization from the Information Technology Department or other designated County official.

6.14.3 Users shall promptly report lost, stolen, damaged, missing, compromised, or unauthorized-accessed County IT resources to their Department Head or elected official and the Information Technology Department. Reports should be made as soon as practicable and no later than 72 hours after discovery.

6.14.4 County-owned IT resources shall be returned upon request, separation from employment, transfer, reassignment, contract completion, revocation of access, or when the equipment is no longer needed for the approved County purpose.

6.14.5 Departments and users shall cooperate with the Information Technology Department regarding inventory, assignment, reassignment, recovery, repair, replacement, secure storage, disposal, or return of County IT resources.

6.14.6 County IT resources shall be disposed of, recycled, transferred, or sold only through approved County procedures. The Information Technology Department may remove, preserve, transfer, wipe, destroy, or otherwise secure County Data before equipment is reassigned, returned, disposed of, recycled, or sold.

6.15 Telecommunications, Voice, Video, and Messaging Systems. County telecommunications, voice, video, voicemail, messaging, conferencing, collaboration, and related communication systems shall be used in a lawful, professional, secure, and responsible manner for authorized County business. This section applies to County telephone systems, voicemail, cellular calling, SMS/text messaging used for County business, video conferencing, softphones, chat, collaboration platforms, meeting platforms, call recording systems, conferencing systems, and similar communication services, whether accessed from County-owned devices, personally owned devices authorized for County business, or other County-approved systems.

6.15.1 Users shall not use County communication systems or County-authorized communication accounts to harass, threaten, misrepresent identity, conduct unauthorized personal business, send unauthorized mass communications, disclose confidential information, bypass records-retention requirements, or conduct activity prohibited by this policy.

6.15.2 Users shall use County-approved communication systems for County business when available. Personal accounts, personal phone numbers, consumer messaging applications, or unapproved conferencing tools shall not be used for County business when doing so would create a records-retention, security, confidentiality, public-records, or operational concern.

6.15.3 County business communications, including voicemail, call records, chat messages, meeting recordings, transcripts, text messages, video conference records, and related metadata, shall be managed in accordance with this policy, applicable records retention requirements, and legal preservation obligations.

6.15.4 Users shall not record calls, meetings, video conferences, or conversations unless authorized by law, County policy, court rule, department procedure, or all required approvals. Meeting recordings, transcripts, and call recordings created for County business shall be stored, shared, retained, and disposed of in accordance with County requirements.

6.15.5 The Information Technology Department may manage, restrict, disable, preserve, retrieve, or remove access to County communication systems and related data when necessary for security, records retention, troubleshooting, continuity of operations, legal obligations, or enforcement of this policy.

6.16 Cybersecurity Training, User Awareness, and Policy Acknowledgment.

6.16.1 Users may be required to acknowledge receipt of this policy, complete cybersecurity awareness training, role-based security training, phishing simulations, confidentiality acknowledgments, system-specific access agreements, or other training or documentation as a condition of receiving or maintaining access to County IT resources. Access may be delayed, denied, modified, suspended, or revoked when required by County policy, security requirements, operational need, legal obligation, employment status, contract status, business necessity, or failure to complete required training or documentation.

6.16.2 Users are responsible for understanding and complying with this policy, related administrative procedures, security training, system prompts, warnings, and instructions issued by the Information Technology Department or other authorized County officials.

6.16.3 Users shall exercise reasonable care when using County IT resources, including recognizing and reporting phishing attempts, suspicious links, suspicious attachments, unexpected MFA prompts, social engineering attempts, suspected malware, unauthorized access, and other potential security threats.

6.16.4 Failure to complete required training, policy acknowledgment, or access documentation may result in delay, denial, suspension, modification, or revocation of access to County IT resources.

6.16.5 The Information Technology Department, in coordination with the County Administrator, Department Heads, elected officials, Human Resources, Legal Counsel, or other appropriate officials, may establish training requirements, acknowledgment procedures, and user awareness programs to support compliance with this policy.

6.17 Exceptions and Waivers.

6.17.1 Exceptions or waivers to this policy may be approved only by the County Administrator or designee, in consultation with the Information Technology Director, Legal Counsel, Department Head, elected official, Human Resources, or other appropriate officials when applicable.

6.17.2 Exceptions may be granted only when there is a legitimate County business, legal, operational, technical, public safety, accessibility, or compliance need, and when appropriate safeguards are implemented to reduce risk to County systems, County Data, and County operations.

6.17.3 Exceptions may be limited by duration, user, department, system, device, location, data type, compensating control, or other condition. The County may modify, suspend, or revoke an exception at any time when the exception is no longer needed, conditions are not met, risk changes, or continued use is not in the County's interest.

6.17.4 Users shall not treat convenience, preference, past practice, lack of awareness, or technical difficulty as authorization to bypass this policy. Any user who believes an exception is necessary shall request approval through the applicable administrative procedure before taking action that would otherwise violate this policy.

6.17.5 The County Administrator and Information Technology Director, or their respective designees, may develop, revise, and implement administrative procedures, forms, standards, technical controls, user guidance, and security requirements necessary to administer and enforce this policy.

6.18 Enforcement.

6.18.1 Violation of this policy, related administrative procedures, security requirements, or lawful instructions from authorized County officials may result in corrective action, suspension or revocation of IT access, removal of software or services, remote lock or wipe of devices, disciplinary action up to and including termination, contract remedies, referral to law enforcement, civil action, and/or other action permitted by law or County policy. For employees covered by collective bargaining agreements, disciplinary procedures will follow the applicable agreement. For elected officials and employees of elected officials and Courts, discipline is subject to the discretion of the elected official or the Court subject to Michigan State law and any applicable collective bargaining agreement or employer policy.

6.18.2 The County may take immediate action to protect County IT resources, County Data, public records, confidential information, cybersecurity, legal obligations, or continuity of operations, including disabling accounts, restricting access, disconnecting devices, blocking applications or websites, preserving records, quarantining communications, resetting credentials, or removing access to systems or data.

6.18.3 Users may be held responsible for activity conducted under their assigned accounts, credentials, devices, or access privileges, unless the activity resulted from circumstances beyond the user's reasonable control and was promptly reported as required by this policy.

6.18.4 Enforcement decisions may consider the nature, severity, intent, risk, impact, recurrence, legal requirements, cooperation, and corrective action associated with the violation.

7. ADMINISTRATIVE PROCEDURES: The County Administrator and Information Technology Director shall be responsible for the development, revision, and implementation of any associated administrative procedures not already stated in this policy.

8. **<u>ADMINISTRATOR AND LEGAL COUNSEL REVIEW</u>:** The County Administrator shall approve all new and amended policies as to substance. County Counsel shall approve all new and amended policies as to legal content. These approvals shall accompany draft policies and amended policies submitted to the Board of Commissioners for consideration.