RESOLUTION NUMBER 7741

WHEREAS, on or about May 20, 2024, the Mayor and City Council of the City of Beatrice adopted the "Employee Technology Usage Policy" to define the acceptable use of Technology at the City of Beatrice and to ensure the City complies with all legally mandated requirements; and

WHEREAS, the Mayor and City Council of the City of Beatrice desire to update the "Employee Technology Usage Policy".

NOW, THEREFORE, BE IT RESOLVED BY THE MAYOR AND CITY COUNCIL OF THE CITY OF BEATRICE, NEBRASKA:

SECTION 1. That the "Employee Technology Usage Policy", marked as Exhibit "A", attached hereto and incorporated herein by this reference, be and hereby is adopted.

SECTION 2. That Resolution Number 7310 and any and all resolutions or parts of resolutions in conflict herewith are hereby repealed.

RESOLUTION PASSED AND APPROVED this 16th day of March, 2026.

Attest:

Amanda Kuhlman, Deputy City Clerk

Robert Morgan, Mayor

Exhibit "A"

STAKE YOUR CLAIM

BEATRICE

CITY • BOARD OF PUBLIC WORKS

EMPLOYEE TECHNOLOGY USAGE POLICY

PURPOSE

The intent of the Employee Technology Usage Policy is to define the acceptable use of Technology at the City of Beatrice (City) and to ensure the City complies with all legally mandated requirements. It outlines the responsibilities of those who work for and on behalf of the City in contributing to the maintenance and protection of its information resources in a secure, stable, and cost-effective manner. This policy is consistent with the intent and requirements of the City's work policies and rules.

POLICY SCOPE

The Employee Technology Usage Policy defines the oversight, use and protection of the City's computing equipment, network, voice, electronic communications, and data repositories. This includes the acquisition, access and use of all software, hardware, and shared resources, whether connected to the network, configured off the network, or while in transit (mobile).

It applies to all those who work on behalf of the City, including but not limited to, employees, contractors, consultants, , supplementals, interns, volunteers and other workers including all personnel affiliated with third parties. This policy also applies to all equipment that is owned or leased by the City regardless of project and program funding sources.

ACQUISITION OF TECHNOLOGY RESOURCES

The Information Technology (IT) Department must evaluate and approve all software, hardware, removable devices, and related maintenance and support contracts, whether the selected products or solution will be on the network or off; used by one or many people; and for all program and project funding sources. In addition, acquisition of Technology resources should conform to existing purchasing policies and procedures as defined by the IT Department. Most City-owned Technology has a pre-determined lifecycle replacement period and must be surrendered for replacement on a 1:1 basis or retired, according to that schedule. Such Technology may not be redeployed or otherwise put back into use without approval from the IT Department.

ACCESS TO THE CITY'S TECHNOLOGY RESOURCES

- The IT Department must approve the setting up of new user accounts.
- Users are responsible to establish and maintain passwords consistent with the City's standards.
- User accounts and ALL passwords may not be shared with anyone other than the named owner and City IT employees. Examples include co-workers, subordinates, business associates, household members, etc.

Adopted March 16, 2026
Resolution Number 7741

- The individual logged onto the City network must be present while the logon credentials are being used to access Network resources, or must ensure that the account is locked or logged off and not being used by others when not present.
- IT Department must approve connection of ANY devices using the City's internal network.
- Information Technology must approve installation of all software, freeware and software that is obtained for evaluation purposes.
- Any software or files downloaded via the Internet into the City's network become the property of the City. Any such files or software may be used only in ways that are consistent with their licenses and/or copyrights.
- Direct secure (peer-to-peer) connections are provided only in unique circumstances, requiring prior approval from the IT Department.
- Information Technology must be consulted during the ***infancy*** stages of major projects pertaining to or including IT equipment and/or software.
- Connection or installation of personally owned hardware or software within the City-provided infrastructure (i.e. network, Internet, fax lines, telephone lines, and printers) is not allowed.
- All activity resulting from device, network or software application access is the responsibility of the person assigned the user account.

REMOTE ACCESS TO CITY SYSTEMS

Remote access to certain City systems, applications, and data is maintained for selected employees. City remote access systems require a high level of application and user maintenance as well as monitoring. In addition, they significantly increase the security risks associated with outside access to applications and data. Remote access systems are therefore restricted only to those City employees who show a demonstrated necessity to access data or applications while away from City facilities and ONLY for City business. Remote access will not be granted for convenience. Users who do not regularly utilize remote access systems may be removed as Remote Access Users. Use of remote access for other than official business will result in immediate removal as a remote user and, if appropriate, disciplinary action.

a. **Authorization Required**
   Prior to use by any City employee, the appropriate City employee must submit a written request to the IT Department identifying the user and stating what business necessity exists requiring the potential user to utilize remote access. Permission will be based on demonstrated need and subject to the criteria listed below.

INTERNET USAGE

- Use of the Internet should be consistent with City policies and work rules. Incidental personal use of City resources is allowed as defined in the paragraph Incidental Personal Use. Visiting, referencing, downloading and/or storing materials that are inappropriate in a work environment is prohibited unless such activity is specifically related to your employment with the City. Examples include but are not limited to data from sexually explicit sites, and those associated with violence, hate crimes or illegal activities.
- Content and images posted on the City's website, file transfer protocols (FTP), Cloud, or Social Media sites should be consistent with the City's policies and practices and should conform to professional standards in tone and format.

- Monitoring and Reporting of Internet Use - It is the responsibility of Department Heads to monitor and audit Internet web use within their department. Because there is the potential for employee abuse of the system, the City may monitor and record user access to Internet sites. No user should have the expectation of privacy as to his/her Internet usage.
- All information that is posted, copied or shared, either on the City's servers and desktops or on the City's website or Social Media sites, must be done so in accordance with the laws that govern copyrighted materials including, but not limited to, photographs, magazines, books, copyrighted music, the installation of any copyrighted software for which the City or end user does not have an active license, or the installation of "pirated" software.
- Web usage that significantly impacts network bandwidth may be restricted. Individuals should utilize only the City's tools and recommended best practices to manage their connections when viewing, downloading, sharing and printing information to ensure that these shared resources are not negatively impacted.

MOBILE DEVICES

All mobile devices, whether City-owned or personal, that have access to systems and applications are governed by this policy. Applications, including cloud storage software used by staff on their own personal devices may also be subject to this policy. The following general procedures and protocols apply to the use of mobile devices:

- All City-owned mobile computing devices must be protected with a password required at the time the device is powered on.
- Personal mobile computing devices that require network connectivity must conform to City standards for use and configuration.
- Mobile Device Management (MDM) will be used to enforce common security standards and configurations on City-owned devices.
- City-owned mobile devices will have location services enabled at all times.
- Unattended mobile computing devices shall be physically secured .
- Lost and stolen devices will be locked and location services will be used to locate the device. If the device cannot be located, it will be wiped of all information.

Information Technology shall implement procedures and measures to strictly limit access to sensitive data moving to and from mobile computing devices since these devices generally pose a higher risk for incidents than non-portable devices.

CELL PHONE USE

Please refer to the City's Cell Phone Policy for guidelines.

E-MAIL COMMUNICATIONS

- The electronic mail system is intended for business purposes. Electronic mail communications constitute public records and the City has the right to access or monitor messages for work- related purposes, security, or to respond to public record requests. All messages should be composed with the expectation that they are public. Refrain from using your City email address for anything other than official business.
- Users shall have no expectation of privacy in email messages, whether they are business related or an allowed personal use as provided herein. Use of electronic mail shall be considered consent to City

Officials, managers, and other employees to inspect, use, or disclose any electronic mail or other electronic communications and/or data.

- Use of Non-City Email Accounts - Non-City email accounts (like MSN, Yahoo!, Gmail, Hotmail, etc.) may not be used to conduct City business. Likewise, a non-City email account may not be forwarded to a City email account.
- Transmission of Confidential Information - Confidential material must be encrypted before transmission.
- E-mail communications will conform to the same professional standards as with written and verbal business correspondence. A professional tone should prevail and content will be consistent with and representative of the City's policies and practices.
- Use of personal email (like MSN, Yahoo!, Gmail, Hotmail, etc.) is prohibited on City-owned Technology.

INTELLECTUAL PROPERTY, PRIVACY AND MONITORING

There is no right to privacy in the course of using the City's Technology resources, whether conducting City business or for incidental personal use. The City owns all data stored on its network and peripheral devices and reserves the right to inspect and monitor any and all such use at any time (examples include e-mail, voicemail, Internet usage, computers, laptops, cell phones, etc.). The City may conduct requested audits in order to ensure compliance with its policies and requirements, to respond to public disclosure requests, investigate suspicious activities or security threats, or to fulfill legally mandated requirements (i.e. software license rules, Payment Card Industry (PCI) regulations, and the Health Insurance Portability and Accountability Act (HIPAA) requirements), Criminal Justice Information Services (CJIS).

INCIDENTAL PERSONAL USE

The City's Technology resources using an Internet web browser are City property and intended for use to conduct City business by its authorized employees, contractors, consultants, , supplementals, interns, volunteers and other workers including all personnel affiliated with third parties; hereafter referred to as the user. Limited personal use is permitted as long as it does not result in a cost to the City, does not interfere with the responsibilities and fulfillment of job duties, is brief in duration and frequency, does not distract from the conduct of City business and does not compromise the security or integrity of City information or software. As noted previously, there is no right to privacy in the course of using the City's Technology resources, whether for City business or incidental personal use.

a. **Permissible Use**
   Personal use of City-owned devices while on duty shall be kept to a minimum. Downloading personal email to the City's system or attaching a personal email box is prohibited.

b. **Prohibited Uses**
   A prohibited use is any use related to the conduct of an outside business; a use for the purposes of supporting, promoting, or soliciting for any non-City sponsored outside organization or group; soliciting funds for any purpose; or religious activity, campaign or political use; commercial use; posting to or buying from online auction or sales sites; use to conduct illegal activities; any entertainment uses; and/or uses which result in the City being placed on electronic mailing lists related to prohibited uses. ,. The IT Director and City Administrator have the authority to make an exception on a case-by-case basis.

SECURITY, STORAGE, AND PROTECTION

Effective security requires the participation and support of every user in the organization. The City employs enterprise tools to manage, monitor and protect the organization from internal and external security threats and data loss. In addition to these measures, it is the responsibility of individuals to remain vigilant in their awareness and protection of the City's resources, including equipment and data they have access to and while in their possession. Specific due diligence requirements are outlined below:

- City devices and computer equipment must be logged out or "locked" when unattended. This also includes a screen lock on City-owned mobile devices.
- All users must log off of their pc and leave it powered on at the end of their shift to enable off- shift maintenance and security updates.
- Intruding or attempting to intrude into any gap in the system or network security is prohibited. Sharing of information with others that facilitates their unauthorized access to the City's data, network or devices, or their exploitation of a security gap is also prohibited.
- It is the responsibility of each individual to prevent unauthorized and indiscriminate access to "personal information" (see Definitions) that could pose the threat of identity theft, thus risking a person's privacy, financial security and other interests.
- As noted above, user accounts and passwords may not be shared. The individual logged onto the City network must be present while logon credentials are being used to access Network resources
- In general it is not permissible to download "personal information" to any removable/portable device, including laptop computers, unless access to that information is within the scope of your job, your manager has approved the copy of information to a portable device and the data or device is encrypted. Please see the City's Personal Information Security policy for further information.
- Transmitting confidential data in part or full via e-mail or other unencrypted medium is prohibited.
- Leaving personal, sensitive or confidential information exposed to view while unattended, either on paper or on screen, is prohibited.
- Whenever possible, laptop and desktop hard drives and removable devices should only contain copies of source files, not the original file.
- Individuals must report to the City any equipment, software or data that is lost, damaged or stolen at their first available opportunity. Reports will be made to a supervisor, manager, or director. Unrecoverable equipment may incur additional replacement costs.
- Lost equipment, especially that containing sensitive or confidential information as defined here, including building access cards, must be reported immediately to the I.T. Staff.
- Stolen computers, laptops, thumb drives, smart phones, etc. must be reported immediately to the Police Department at 402-228-4080 **AND** to the IT Department.
- Storage of any copyrighted material on a network server or local hard drive including, but not limited to, photographs from magazines, books or other copyrighted sources, copyrighted music, the installation of any copyrighted software for which the City or end user does not have an active license, or the installation of "pirated" software is strictly prohibited.

ACCESS TO SENSITIVE CARDHOLDER DATA

- Do not store cardholder data (e.g., full PAN, CVV, magnetic stripe data) unless explicitly authorized.
- Never write down, email, text, or instant-message cardholder data.
- Only use approved systems and applications to process payments.
- Access to payment systems is limited to authorized users with a business need.
- Use only City-approved devices and software for payment-related activities.
- Never respond to requests for cardholder data via email or phone unless verified.
- Avoid using public or unsecured Wi-Fi when handling sensitive data.
- Violations may result in disciplinary action, up to and including termination, and possible legal consequences.

REPORTING AND ADMINISTRATION

Anyone who observes or suspects a violation of these policies and requirements, or a potential gap in security or protection of the City's assets or data, should immediately report these to their Department Head. Violations may result in disciplinary actions up to and including termination of employment. Requests for exceptions to any of the Technology Usage Policy definitions must be submitted in writing from Department Heads to the IT Director. Exceptions require the approval of both the requesting department's director and the IT Director. Approvals must be documented in writing and limited in duration to provide for periodic re-evaluation.

EMPLOYEE TECHNOLOGY USAGE POLICY
ACKNOWLEDGEMENT FORM

I have received a copy of the *Employee Technology Usage Policy* and have read and understand my responsibilities as a user of the City's Technology resources.

I understand this policy is subject to change without notice and agree to abide by it and all subsequent changes.

I also understand that violation of the policy may result in disciplinary action, including termination.

I also understand that this document will be kept in my personnel file.

_____
Employee Name (Print)

_____
Employee Signature

_____
Date

Adopted March 16, 2026
Resolution Number 7741

Redline

STAKE YOUR CLAIM

BEATRICE

CITY • BOARD OF PUBLIC WORKS

EMPLOYEE TECHNOLOGY USAGE POLICY

PURPOSE

The intent of the Employee Technology Usage Policy is to define the acceptable use of Technology at the City of Beatrice (City) and to ensure the City complies with all legally mandated requirements. It outlines the responsibilities of those who work for and on behalf of the City in contributing to the maintenance and protection of its information resources in a secure, stable, and cost-effective manner. This policy is consistent with the intent and requirements of the City's work policies and rules.

POLICY SCOPE

The Employee Technology Usage Policy defines the oversight, use and protection of the City's computing equipment, network, voice, electronic communications, and data repositories. This includes the acquisition, access and use of all software, hardware, and shared resources, whether connected to the network, configured off the network, or while in transit (mobile).

It applies to all those who work on behalf of the City, including but not limited to, employees, contractors, consultants, , supplementals, interns, volunteers and other workers including all personnel affiliated with third parties. This policy also applies to all equipment that is owned or leased by the City regardless of project and program funding sources.

ACQUISITION OF TECHNOLOGY RESOURCES

The Information Technology (IT) Department must evaluate and approve all software, hardware, removable devices, and related maintenance and support contracts, whether the selected products or solution will be on the network or off; used by one or many people; and for all program and project funding sources. In addition, acquisition of Technology resources should conform to existing purchasing policies and procedures as defined by the IT Department. Most City-owned Technology has a pre-determined lifecycle replacement period and must be surrendered for replacement on a 1:1 basis or retired, according to that schedule. Such Technology may not be redeployed or otherwise put back into use without approval from the IT Department.

ACCESS TO THE CITY'S TECHNOLOGY RESOURCES

- The IT Department must approve the setting up of new user accounts.
- Users are responsible to establish and maintain passwords consistent with the City's standards.
- User accounts and ALL passwords may not be shared with anyone other than the named owner and City IT employees. Examples include co-workers, subordinates, business associates, household members, etc.

Adopted _____, 2026
Resolution Number ____

- The individual logged onto the City network must be present while the logon credentials are being used to access Network resources, or must ensure that the account is locked or logged off and not being used by others when not present.
- IT Department must approve connection of ANY devices using the City's internal network.
- Information Technology must approve installation of all software, freeware and software that is obtained for evaluation purposes.
- Any software or files downloaded via the Internet into the City's network become the property of the City. Any such files or software may be used only in ways that are consistent with their licenses and/or copyrights.
- Direct secure (peer-to-peer) connections are provided only in unique circumstances, requiring prior approval from the IT Department.
- Information Technology must be consulted during the ***infancy*** stages of major projects pertaining to or including IT equipment and/or software.
- Connection or installation of personally owned hardware or software within the City-provided infrastructure (i.e. network, Internet, fax lines, telephone lines, and printers) is not allowed.
- All activity resulting from device, network or software application access is the responsibility of the person assigned the user account.

REMOTE ACCESS TO CITY SYSTEMS

Remote access to certain City systems, applications, and data is maintained for selected employees. City remote access systems require a high level of application and user maintenance as well as monitoring. In addition, they significantly increase the security risks associated with outside access to applications and data. Remote access systems are therefore restricted only to those City employees who show a demonstrated necessity to access data or applications while away from City facilities and ONLY for City business. Remote access will not be granted for convenience. Users who do not regularly utilize remote access systems may be removed as Remote Access Users. Use of remote access for other than official business will result in immediate removal as a remote user and, if appropriate, disciplinary action.

a. **Authorization Required**
   Prior to use by any City employee, the appropriate City employee must submit a written request to the IT Department identifying the user and stating what business necessity exists requiring the potential user to utilize remote access. Permission will be based on demonstrated need and subject to the criteria listed below.

INTERNET USAGE

- Use of the Internet should be consistent with City policies and work rules. Incidental personal use of City resources is allowed as defined in the paragraph Incidental Personal Use. Visiting, referencing, downloading and/or storing materials that are inappropriate in a work environment is prohibited unless such activity is specifically related to your employment with the City. Examples include but are not limited to data from sexually explicit sites, and those associated with violence, hate crimes or illegal activities.
- Content and images posted on the City's website, file transfer protocols (FTP), Cloud, or Social Media sites should be consistent with the City's policies and practices and should conform to professional standards in tone and format.

- Monitoring and Reporting of Internet Use - It is the responsibility of Department Heads to monitor and audit Internet web use within their department. Because there is the potential for employee abuse of the system, the City may monitor and record user access to Internet sites. No user should have the expectation of privacy as to his/her Internet usage.
- All information that is posted, copied or shared, either on the City's servers and desktops or on the City's website or Social Media sites, must be done so in accordance with the laws that govern copyrighted materials including, but not limited to, photographs, magazines, books, copyrighted music, the installation of any copyrighted software for which the City or end user does not have an active license, or the installation of "pirated" software.
- Web usage that significantly impacts network bandwidth may be restricted. Individuals should utilize only the City's tools and recommended best practices to manage their connections when viewing, downloading, sharing and printing information to ensure that these shared resources are not negatively impacted.

MOBILE DEVICES

All mobile devices, whether City-owned or personal, that have access to systems and applications are governed by this policy. Applications, including cloud storage software used by staff on their own personal devices may also be subject to this policy. The following general procedures and protocols apply to the use of mobile devices:

- All City-owned mobile computing devices must be protected with a password required at the time the device is powered on.
- Personal mobile computing devices that require network connectivity must conform to City standards for use and configuration.
- Mobile Device Management (MDM) will be used to enforce common security standards and configurations on City-owned devices.
- City-owned mobile devices will have location services enabled at all times.
- Unattended mobile computing devices shall be physically secured .
- Lost and stolen devices will be locked and location services will be used to locate the device. If the device cannot be located, it will be wiped of all information.

Information Technology shall implement procedures and measures to strictly limit access to sensitive data moving to and from mobile computing devices since these devices generally pose a higher risk for incidents than non-portable devices.

CELL PHONE USE

Please refer to the City's Cell Phone Policy for guidelines.

E-MAIL COMMUNICATIONS

- The electronic mail system is intended for business purposes. Electronic mail communications constitute public records and the City has the right to access or monitor messages for work- related purposes, security, or to respond to public record requests. All messages should be composed with the expectation that they are public. Refrain from using your City email address for anything other than official business.
- Users shall have no expectation of privacy in email messages, whether they are business related or an allowed personal use as provided herein. Use of electronic mail shall be considered consent to City

Officials, managers, and other employees to inspect, use, or disclose any electronic mail or other electronic communications and/or data.

- Use of Non-City Email Accounts - Non-City email accounts (like MSN, Yahoo!, Gmail, Hotmail, etc.) may not be used to conduct City business. Likewise, a non-City email account may not be forwarded to a City email account.
- Transmission of Confidential Information - Confidential material must be encrypted before transmission.
- E-mail communications will conform to the same professional standards as with written and verbal business correspondence. A professional tone should prevail and content will be consistent with and representative of the City's policies and practices.
- Use of personal email (like MSN, Yahoo!, Gmail, Hotmail, etc.) is prohibited on City-owned Technology.

INTELLECTUAL PROPERTY, PRIVACY AND MONITORING

There is no right to privacy in the course of using the City's Technology resources, whether conducting City business or for incidental personal use. The City owns all data stored on its network and peripheral devices and reserves the right to inspect and monitor any and all such use at any time (examples include e-mail, voicemail, Internet usage, computers, laptops, cell phones, etc.). The City may conduct requested audits in order to ensure compliance with its policies and requirements, to respond to public disclosure requests, investigate suspicious activities or security threats, or to fulfill legally mandated requirements (i.e. software license rules, Payment Card Industry (PCI) regulations, and the Health Insurance Portability and Accountability Act (HIPAA) requirements), Criminal Justice Information Services (CJIS).

INCIDENTAL PERSONAL USE

The City's Technology resources using an Internet web browser are City property and intended for use to conduct City business by its authorized employees, contractors, consultants, , supplementals, interns, volunteers and other workers including all personnel affiliated with third parties; hereafter referred to as the user. Limited personal use is permitted as long as it does not result in a cost to the City, does not interfere with the responsibilities and fulfillment of job duties, is brief in duration and frequency, does not distract from the conduct of City business and does not compromise the security or integrity of City information or software. As noted previously, there is no right to privacy in the course of using the City's Technology resources, whether for City business or incidental personal use.

a. Permissible Use

Personal use of City-owned devices while on duty shall be kept to a minimum. Downloading personal email to the City's system or attaching a personal email box is prohibited.

b. Prohibited Uses

A prohibited use is any use related to the conduct of an outside business; a use for the purposes of supporting, promoting, or soliciting for any non-City sponsored outside organization or group; soliciting funds for any purpose; or religious activity, campaign or political use; commercial use; posting to or buying from online auction or sales sites; use to conduct illegal activities; any entertainment uses; and/or uses which result in the City being placed on electronic mailing lists related to prohibited uses. ,. The IT Director and City Administrator have the authority to make an exception on a case-by-case basis.

SECURITY, STORAGE, AND PROTECTION

Effective security requires the participation and support of every user in the organization. The City employs enterprise tools to manage, monitor and protect the organization from internal and external security threats and data loss. In addition to these measures, it is the responsibility of individuals to remain vigilant in their awareness and protection of the City's resources, including equipment and data they have access to and while in their possession. Specific due diligence requirements are outlined below:

- City devices and computer equipment must be logged out or "locked" when unattended. This also includes a screen lock on City-owned mobile devices.
- All users must log off of their pc and leave it powered on at the end of their shift to enable off- shift maintenance and security updates.
- Intruding or attempting to intrude into any gap in the system or network security is prohibited. Sharing of information with others that facilitates their unauthorized access to the City's data, network or devices, or their exploitation of a security gap is also prohibited.
- It is the responsibility of each individual to prevent unauthorized and indiscriminate access to "personal information" (see Definitions) that could pose the threat of identity theft, thus risking a person's privacy, financial security and other interests.
- As noted above, user accounts and passwords may not be shared. The individual logged onto the City network must be present while logon credentials are being used to access Network resources
- In general it is not permissible to download "personal information" to any removable/portable device, including laptop computers, unless access to that information is within the scope of your job, your manager has approved the copy of information to a portable device and the data or device is encrypted. Please see the City's Personal Information Security policy for further information.
- Transmitting confidential data in part or full via e-mail or other unencrypted medium is prohibited.
- Leaving personal, sensitive or confidential information exposed to view while unattended, either on paper or on screen, is prohibited.
- Whenever possible, laptop and desktop hard drives and removable devices should only contain copies of source files, not the original file.
- Individuals must report to the City any equipment, software or data that is lost, damaged or stolen at their first available opportunity. Reports will be made to a supervisor, manager, or director. Unrecoverable equipment may incur additional replacement costs.
- Lost equipment, especially that containing sensitive or confidential information as defined here, including building access cards, must be reported immediately to the I.T. Staff.
- Stolen computers, laptops, thumb drives, smart phones, etc. must be reported immediately to the Police Department at 402-228-4080 **AND** to the IT Department.
- Storage of any copyrighted material on a network server or local hard drive including, but not limited to, photographs from magazines, books or other copyrighted sources, copyrighted music, the installation of any copyrighted software for which the City or end user does not have an active license, or the installation of "pirated" software is strictly prohibited.

ACCESS TO SENSITIVE CARDHOLDER DATA

- Do not store cardholder data (e.g., full PAN, CVV, magnetic stripe data) unless explicitly authorized.
- Never write down, email, text, or instant-message cardholder data.
- Only use approved systems and applications to process payments.
- Access to payment systems is limited to authorized users with a business need.
- Use only City-approved devices and software for payment-related activities.
- Never respond to requests for cardholder data via email or phone unless verified.
- Avoid using public or unsecured Wi-Fi when handling sensitive data.
- Violations may result in disciplinary action, up to and including termination, and possible legal consequences.

REPORTING AND ADMINISTRATION

Anyone who observes or suspects a violation of these policies and requirements, or a potential gap in security or protection of the City's assets or data, should immediately report these to their Department Head. Violations may result in disciplinary actions up to and including termination of employment. Requests for exceptions to any of the Technology Usage Policy definitions must be submitted in writing from Department Heads to the IT Director. Exceptions require the approval of both the requesting department's director and the IT Director. Approvals must be documented in writing and limited in duration to provide for periodic re-evaluation.

EMPLOYEE TECHNOLOGY USAGE POLICY
ACKNOWLEDGEMENT FORM

I have received a copy of the *Employee Technology Usage Policy* and have read and understand my responsibilities as a user of the City's Technology resources.

I understand this policy is subject to change without notice and agree to abide by it and all subsequent changes.

I also understand that violation of the policy may result in disciplinary action, including termination.

I also understand that this document will be kept in my personnel file.

_____
Employee Name (Print)

_____
Employee Signature

_____
Date

Adopted _____, 2026
Resolution Number ____