BUFFALO COUNTY
Wisconsin

Buffalo County Resolution

Drafted By:
Lee Engfer
Presented Month/Year:
June 2023
Involved Committees:
Human Resources

County Department:
Administration
Fiscal Impact: YES / NO

AC Approved: YES / NO

RESOLUTION # 23-06-02

A RESOLUTION TO UPDATE PERSONNEL POLICY 401 – ELECTRONIC MEDIA AND SOCIAL MEDIA

WHEREAS, the current Buffalo County Handbook requires the Buffalo County Board of Supervisors to authorize by resolution any amendments to the Employee Handbook; and,

WHEREAS, the contracted IT partner, Itechra, has recommended updating technology related policies to bring them up to date; and,

WHEREAS, the Human Resource Committee has recommended changes to Policy 401 – Electronic and Social Media to rename the policy to "Technology, Email, and Network – Acceptable Use Policy" and to update the content of the policy to reflect standard acceptable usage of Buffalo County's network, devices, and email to protect the County and the residents from illegal or damaging actions while moving the Social Media portion to its own policy; and,

NOW, THEREFORE BE IT RESOLVED, that the Buffalo County Board of Supervisors hereby amends Policy 401 (now Technology, Email, and Network – Acceptable Use Policy) of the Buffalo County Handbook effective June 26th, 2023, to make these updates.

Adopted at a duly called and noticed meeting of the Buffalo County Board of Supervisors on the 26th day of June, 2023.

ATTEST:

County Clerk

County Board Chairperson

BUFFALO COUNTY
Wisconsin

Buffalo County Resolution

Respectfully Submitted:

Human Resources Committee:

Steven Nelson

Carol McDonough

Mary Anne McMillan Urell

Excused
Nathan Nelson

Michael Taylor

ANTICIPATED FINANCIAL IMPACT STATEMENT

None

BUFFALO COUNTY Wisconsin

Buffalo County Resolution

Exhibit A: Old Policy

POLICY 401 - ELECTRONIC MEDIA & SOCIAL MEDIA

Purpose: To address the fast-changing landscape of the internet and the way residents communicate and obtain information online, Buffalo County Departments may consider participating in social media formats to reach a broader audience. Buffalo County encourages the use of social media outlets to further the goals of the County and to meet the mission statement of the County.

Policy:

- It is the County's policy that information, in all its forms, written, spoken, recorded electronically, or printed, will be protected from accidental or intentional unauthorized modification, destruction, or disclosure.
- All electronic media must be protected from misuse, unauthorized manipulation, and destruction.
- It is further the policy of the County that employees may not use social media technology while at work or off of work to engage in or post communications or material that would violate any Personnel Policy, including, but not limited to, using technology to post communications or materials that are derogatory or offensive with respect to race, religion, gender, sexual orientation, national origin, disability, age, or any other legally protected class status.

General Guidelines:

- **Electronic Media**:
  - All county-provided electronic media systems are the County's property.
  - All messages and files composed, sent or received, or posted on these systems are and remain the property of the County. They are not the private property of any employee.
  - The use of our electronic media systems is reserved solely for the conduct of business, during work hours.
  - If employees wish to use these systems during breaks, lunch periods, or before and after regular working hours, they may do so but employees are specifically prohibited from using these services for any illegal, illicit, immoral or offensive purposes.
  - A post is "offensive" if it could reasonably be construed to intentionally harm someone's reputation, contribute to a hostile work environment on the basis of a protected classification, incite violence or similar inappropriate or unlawful conduct, or disparage members of the public/customers, co-workers/associates or suppliers.
  - The electronic media systems may not be used to solicit or proselytize for commercial ventures, religious or political causes, or other non-job-related solicitations.
  - The electronic media systems are not to be used to create any "offensive" or disruptive messages or documents (see definition of "offensive", above) or used in a manner that adversely affects your job performance or is disruptive to the job performance of co-workers.

- The electronic media systems may not be used to send (upload) or receive (download) copyrighted materials, trade secrets, proprietary financial information, employee/employee family medical information or similar materials without prior authorization. This guideline is not intended to restrict employees from discussing with others their wages or other terms and conditions of employment.
- The County reserves and intends to exercise the right to review, audit, intercept, access and disclose all internet activity and any messages or documents created, received or sent over the County's electronic media systems for any purpose.
- The confidentiality of any message cannot be assumed. Even when a message is erased, it is still possible to retrieve and read that message. Further, the use of passwords for security does not guarantee confidentiality. All passwords must be disclosed to the Department Manager or designee, or they are invalid and cannot be used.
- Employees may not modify, delete, or destroy any county document created by any electronic media unless specifically authorized to do so.

- **Social Media:**
  - Only on Your Own Time. Unless you have received advance permission from your supervisor or unless such activity is directly related to the performance of your job, you may not engage in social media activity on work time and in work areas (you may engage in social media activities during break times and pre/post work time.)
  - Post as Yourself. Make clear that you are expressing your personal views alone, not those of the County.
  - Be Respectful and Nice. Do not post communications or material that is disparaging of services, or employees; obscene, profane, vulgar, bullying, threatening, or maliciously false. This guideline is not intended to prevent employees from discussing with others their wages or other terms and conditions of employment.
  - Use Good Judgment. Because what you say online is accessible to the public, use good judgment in your communications.
  - Obey the Law. Do not post any material that violates the law, such as material that is obscene, profane, defamatory, threatening, harassing, or that violates the privacy rights of someone else. The posting of such material may subject you to criminal and civil liability.
  - Don't Expect Privacy. Because your social media communications are publicly available, you should not expect that your communications are private in any way. Once you post something online, it is completely out of your control and generally available to anyone in the world.
  - Ask for Guidance. If you have any questions about what is appropriate to include in social media communications, ask your manager or a member of the Administration Office.
  - Comply with Harassment/Discrimination and Other Policies. Employees may not use social media technology to engage in or post communications or material that would violate any other Personnel Policy, including, but not limited to, the Harassment and Discrimination Policy. This guideline is not intended to prevent employees from discussing with others their wages or other terms and conditions of employment.
  - Keep Secrets. You must not disclose "confidential information" which does not include discussions with third parties about your wages, hours and/or conditions of employment.

Reporting Deviations from Policy:

- All employees are encouraged to report any discovered or suspected unauthorized or improper usage of electronic media or social media with impact on the workplace.
- The County prohibits taking negative action against any employee for reporting a possible deviation from this policy or for cooperating in an investigation.
- Any employee who retaliates against another employee for reporting a possible deviation from this policy and/or for cooperating in an investigation will be subject to disciplinary action, up to and including discharge from employment.

Policy Violations: Employees who violate this policy may be subject to discipline, up to and including immediate termination of employment.

Policy 401 - Effective May 31, 2015

BUFFALO COUNTY Wisconsin

Buffalo County Resolution

Exhibit B: Agreement Sign Off

BUFFALO COUNTY Wisconsin

Technology Acceptable Use Agreement

Name	
Job Title	
Department	

This Technology Acceptable Use Agreement (the "Agreement") is established by Buffalo County to define the acceptable use of technology resources within the County.

Purpose: The purpose of this policy is to define acceptable usage of Buffalo County's network, computer devices, and email systems. This policy is to protect Buffalo County's employees, partners, and the residents from illegal or damaging actions by individuals, either knowingly or unknowingly. Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and application services are the property of Buffalo County. Effective security is a team effort involving the participation and support of every Buffalo County employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly. This policy covers accessing our network, passwords, security, prohibited use, and user responsibility.

Scope: This policy applies to all employees, contractors, and temporary staff who use, access, or interact with Buffalo County's technology resources, including, but not limited to, computers, laptops, tablets, mobile devices, software, hardware, networks, and internet access.

Technology Use: Buffalo County provides computer/laptop/other electronic devices and network access as a professional resource for employees to fulfill business needs and is not intended for personal use.

- You may access, use, or share Buffalo County Information and/or Information Systems only to the extent it is authorized and necessary to fulfill your assigned job duties.
- Buffalo County information stored on electronic and computing devices must be protected through legal or technical means that information is protected.
- You have a responsibility to promptly report the damage, theft, loss, or unauthorized disclosure of Buffalo County information and/or Information Systems.
- For security and network maintenance purposes, the County reserves the right to monitor, access, and review all activities conducted using its technology resources, including email, internet usage, and stored data, with or without notice, to ensure compliance with this policy and applicable laws.

Email Use:

- All use of email must be consistent with Buffalo County policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.
- Buffalo County email accounts should be used for Buffalo County business-related purposes; non-Buffalo County related uses are prohibited.
- The Buffalo County email system should not be used to harass or make threats, nor be offensive or disruptive in nature; should not include language or images related to race, gender, age, sexual orientation, unless specifically related to your job duties; pornography, religious or political beliefs, national origin, or disability, unless specifically related to your job duties; should not present personal views as the county's own; should not engage in commercial activity unrelated to the county; should not unlawfully distribute copyrighted material; and should not share confidential material, trade secrets, or proprietary information outside of the county, unless specifically related to your job duties. Employees

who receive any emails with this content from any Buffalo County employee should report the matter to their supervisor/Department Head/Administration Department immediately.

- Users are prohibited from automatically forwarding Buffalo County email to a third-party email system. Individual messages which are forwarded by the user must not contain Buffalo County confidential or above information, unless specifically related to your job duties.
- Use of Buffalo County resources for personal emails is not acceptable.
- Sending chain letters or joke emails from a Buffalo County email accounts is prohibited.
- Buffalo County may monitor messages without prior notice.
- All messages sent or received are and remain the property of the County. They are not the private property of any employee.

Network Access: Any user (remote or internal) accessing Buffalo County network and/or devices must be authenticated using a unique user ID and Password. Other methods of authentication may be used but must be approved by the Buffalo County Information Technology (IT) Department.

The unique user ID assigned to each individual is used for access and control to data and systems. All logging and tracking requirements for privacy, auditing, security, and monitoring are recorded based on this unique user ID. Users will be held responsible for all actions taken under their user ID as recorded by our network and systems. It is strictly forbidden that your user ID and password be used by others.

Obtaining User Id and Password: In order to issue a user id and password, the Buffalo County IT Department must receive the following:

- Notification from the Department Head indicating the account need the appropriate ticket system. Any needed applications and data access must be submitted through a ticket by the Department Head.
- The user must read and sign this policy, acknowledging acceptance thereof.
- Users needing access to data owned by another department will only be granted access upon written approval from his/her Department Head and the data's owner.

Passwords:

- Passwords must conform to the following:
  - Must be at least eight (8) characters long.
  - Must contain at least one alphabetic and one non-alphabetic character. Non-alphabetic characters include numbers (0-9) and punctuation.
  - Must contain at least one lower case and one upper case alphabetic character.
  - Must not be similar to passwords that they had previously employed.
  - Must be difficult to guess. Do not use derivatives of user-IDs, and common character sequences such as "123456" must not be employed. Likewise, personal details such as spouse's name, automobile license plate, social security number, and birthday must not be used unless accompanied by additional unrelated characters. User-chosen passwords must also not be any part of speech. For example, proper names, geographical locations, common acronyms, and slang must not be employed.
- Each user of Buffalo County computer systems will be given six attempts to enter a correct password. If a user has incorrectly entered a password six consecutive times, the user ID will be locked out for 15 minutes.
- All users will be automatically forced to change their passwords upon receipt of an IT issued password and at least once every forty-five (45) days.
- Users must never write down or otherwise record their password.
- Users must never reveal their user id or account password to others or allow the use of their account by others.

- All passwords must be promptly changed if they are suspected of being disclosed or known to have been disclosed to unauthorized parties.
- Users may request a password reset by e-mail, phone or in person. For non-employees your password will not be given verbally but will be sent to your registered email address.
- Every work account should have a different, unique password.
- Whenever possible, also enable the use of multi-factor authentication.

Security: Buffalo County will implement physical and technical safeguards to ensure the integrity of the county hardware, systems, and data.

Users will be granted access to information on a "need-to-know" basis. That is, users will only receive access to the minimum applications and privileges required to perform their jobs.

It is the responsibility of the user to practice the following security measures:

- Do not allow others access through your user ID and password. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
- Secure workstations (screen lock or logout) prior to leaving area to prevent unauthorized access.
- You must lock the screen or log off when the device is unattended.
- Log out of all applications when not in use.
- Complying with all applicable password policies and procedures.
- Never install unauthorized software on any workstation/laptop/device.
- Know the level of security associated to network drives and system directories when storing data.
    - Personal Access – can only be seen by user (currently \\BCC-DC2\Users and \\BCC-DC2\Users2)
    - Department Access – can be accessed only by users associated to the Department
- Do not store sensitive information on workstation/laptops, instead store all sensitive information, including protected health information (PHI) in a network directory.
- Ensure that monitors are positioned away from public view.
- Do not store sensitive data on portable storage devices such as CD, DVD, and USB.
- Never use portable storage devices (CD, DVD, USB, etc) from unknown or suspicious sources.
- Never download files from unknown or suspicious sources
- Must never disable or interfere with the anti-virus software unless given explicit permission from Buffalo County IT Department
- Must never disable or interfere with the firewall unless given explicit permission from Buffalo County IT Department
- Ensure proprietary software per your department is up to date.
- Ensure workstations are left on but logged off in order to facilitate after-hours updates.
- Ensure workstations and laptops are restarted at least weekly, in order to facilitate after-hours updates.
- Exit running applications and close open documents at the end of the day or when away from the device for an extended period.
- If a user has any questions or suspicions regarding emails or files, they must contact the IT Department immediately.

Prohibited: The following activities are strictly prohibited:

- To engage in any activity that is illegal under local, state, federal or international law while using Buffalo County-owned resources.
- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Buffalo County.

- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music.
- Pornography, Child Pornography, Nudity, or other Sexually Explicit Material; not specifically related to your job duties.
- Deliberately create, propagate, or distribute malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Logging into a device with an account that the user is not expressly authorized to access.
- Disrupt network communications. This includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, port scanning or security scanning and forged routing information.
- Port scanning or security scanning is expressly prohibited.
- Executing any form of network monitoring which will intercept data.
- Circumventing user authentication or security on any network, workstation, device or system.
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's session.
- Export or Copy information about, or lists of, Buffalo County employees to parties outside Buffalo County. Exceptions would be for compliance of Open Records Requests laws.
- Copy or Export county-owned software, intellectual property.
- Copy, export and distribute data not specifically related to your job duties.
- Using any Instant Messaging (IM) software communications service that enables you to create a kind of private chat room with another individual in order to communicate in real time over the Internet from any device.

Remote Access: Refer to Policy 403 Virtual Private Network (VPN).

Social Media and Online Conduct: Refer to Policy 403 Social Media.

Policy Violations: Violations of this policy may result in disciplinary action, up to and including termination of employment or contract, as well as legal penalties,

Agreement
This Technology Acceptable Use Agreement shall be maintained by the Buffalo County Administrative Coordinator. A copy of this Agreement and any addendums or amendments shall be provided to the employee. This agreement will remain in effect for the duration of user's employment with Buffalo County or until a revised agreement is issued.

Employee: By signing, the user states they have read, understood, and agree to the terms and conditions of this Agreement:

User Signature		Date Signed	

BUFFALO COUNTY Wisconsin

Buffalo County Resolution

Exhibit C-New Policy

POLICY 401 – TECHNOLOGY, EMAIL, AND NETWORK - ACCEPTABLE USE POLICY

Purpose: The purpose of this policy is to define acceptable usage of Buffalo County's network, computer devices, and email systems. This policy is to protect Buffalo County's employees, partners, and the residents from illegal or damaging actions by individuals, either knowingly or unknowingly. Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and application services are the property of Buffalo County. Effective security is a team effort involving the participation and support of every Buffalo County employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly. This policy covers accessing our network, passwords, security, prohibited use, and user responsibility.

Scope: This policy applies to all employees, contractors, and temporary staff who use, access, or interact with Buffalo County's technology resources, including, but not limited to, computers, laptops, tablets, mobile devices, software, hardware, networks, and internet access.

Technology Use: Buffalo County provides computer/laptop/other electronic devices and network access as a professional resource for employees to fulfill business needs and is not intended for personal use.

- You may access, use, or share Buffalo County Information and/or Information Systems only to the extent it is authorized and necessary to fulfill your assigned job duties.
- Buffalo County information stored on electronic and computing devices must be protected through legal or technical means that information is protected.
- You have a responsibility to promptly report the damage, theft, loss, or unauthorized disclosure of Buffalo County information and/or Information Systems.
- For security and network maintenance purposes, the County reserves the right to monitor, access, and review all activities conducted using its technology resources, including email, internet usage, and stared data, with or without notice, to ensure compliance with this policy and applicable laws.

Email Use:

- All use of email must be consistent with Buffalo County policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.
- Buffalo County email accounts should be used for Buffalo County business-related purposes; non-Buffalo County related uses are prohibited.
- The Buffalo County email system should not be used to harass or make threats, nor be offensive or disruptive in nature; should not include language or images related to race, gender, age, sexual orientation, unless specifically related to your job duties; pornography, religious or political beliefs, national origin, or disability, unless specifically related to your job duties; should not present personal views as the county's own; should not engage in commercial activity unrelated to the county; should not unlawfully distribute copyrighted material; and should not share confidential material, trade secrets, or proprietary information outside of the county, unless

specifically related to your job duties. Employees who receive any emails with this content from any Buffalo County employee should report the matter to their supervisor/Department Head/Administration Department immediately.

- Users are prohibited from automatically forwarding Buffalo County email to a third-party email system. Individual messages which are forwarded by the user must not contain Buffalo County confidential or above information, unless specifically related to your job duties.
- Use of Buffalo County resources for personal emails is not acceptable.
- Sending chain letters or joke emails from a Buffalo County email accounts is prohibited.
- Buffalo County may monitor messages without prior notice.
- All messages sent or received are and remain the property of the County. They are not the private property of any employee.

Network Access: Any user (remote or internal) accessing Buffalo County network and/or devices must be authenticated using a unique user ID and Password. Other methods of authentication may be used but must be approved by the Buffalo County Information Technology (IT) Department.

The unique user ID assigned to each individual is used for access and control to data and systems. All logging and tracking requirements for privacy, auditing, security, and monitoring are recorded based on this unique user ID. Users will be held responsible for all actions taken under their user ID as recorded by our network and systems. It is strictly forbidden that your user ID and password be used by others.

Obtaining User Id and Password: In order to issue a user id and password, the Buffalo County IT Department must receive the following:

- Notification from the Department Head indicating the account need the appropriate ticket system. Any needed applications and data access must be submitted through a ticket by the Department Head.
- The user must read and sign this policy, acknowledging acceptance thereof.
- Users needing access to data owned by another department will only be granted access upon written approval from his/her Department Head and the data's owner.

Passwords:

- Passwords must conform to the following:
  - Must be at least eight (8) characters long.
  - Must contain at least one alphabetic and one non-alphabetic character. Non-alphabetic characters include numbers (0-9) and punctuation.
  - Must contain at least one lower case and one upper case alphabetic character.
  - Must not be similar to passwords that they had previously employed.
  - Must be difficult to guess. Do not use derivatives of user-IDs, and common character sequences such as "123456" must not be employed. Likewise, personal details such as spouse's name, automobile license plate, social security number, and birthday must not be used unless accompanied by additional unrelated characters. User-chosen passwords

must also not be any part of speech. For example, proper names, geographical locations, common acronyms, and slang must not be employed.

- Each user of Buffalo County computer systems will be given six attempts to enter a correct password. If a user has incorrectly entered a password six consecutive times, the user ID will be locked out for 15 minutes.
- All users will be automatically forced to change their passwords upon receipt of an IT issued password and at least once every forty-five (45) days.
- Users must never write down or otherwise record their password.
- Users must never reveal their user id or account password to others or allow the use of their account by others.
- All passwords must be promptly changed if they are suspected of being disclosed or known to have been disclosed to unauthorized parties.
- Users may request a password reset by e-mail, phone or in person. For non-employees your password will not be given verbally but will be sent to your registered email address.
- Every work account should have a different, unique password.
- Whenever possible, also enable the use of multi-factor authentication.

Security: Buffalo County will implement physical and technical safeguards to ensure the integrity of the county hardware, systems, and data.

Users will be granted access to information on a "need-to-know" basis. That is, users will only receive access to the minimum applications and privileges required to perform their jobs.

It is the responsibility of the user to practice the following security measures:

- Do not allow others access through your user ID and password. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
- Secure workstations (screen lock or logout) prior to leaving area to prevent unauthorized access.
- You must lock the screen or log off when the device is unattended.
- Log out of all applications when not in use.
- Complying with all applicable password policies and procedures.
- Never install unauthorized software on any workstation/laptop/device.
- Know the level of security associated to network drives and system directories when storing data.
    - Personal Access – can only be seen by user (currently \\BCC-DC2\Users and \\BCC-DC2\Users2)
    - Department Access – can be accessed only by users associated to the Department
- Do not store sensitive information on workstation/laptops, instead store all sensitive information, including protected health information (PHI) in a network directory.
- Ensure that monitors are positioned away from public view.
- Do not store sensitive data on portable storage devices such as CD, DVD, and USB.
- Never use portable storage devices (CD, DVD, USB, etc) from unknown or suspicious sources.
- Never download files from unknown or suspicious sources
- Must never disable or interfere with the anti-virus software unless given explicit permission from Buffalo County IT Department

- Must never disable or interfere with the firewall unless given explicit permission from Buffalo County IT Department
- Ensure proprietary software per your department is up to date.
- Ensure workstations are left on but logged off in order to facilitate after-hours updates.
- Ensure workstations and laptops are restarted at least weekly, in order to facilitate after-hours updates.
- Exit running applications and close open documents at the end of the day or when away from the device for an extended period.
- If a user has any questions or suspicions regarding emails or files, they must contact the IT Department immediately.

Prohibited: The following activities are strictly prohibited:

- To engage in any activity that is illegal under local, state, federal or international law while using Buffalo County-owned resources.
- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Buffalo County.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music.
- Pornography, Child Pornography, Nudity, or other Sexually Explicit Material; not specifically related to your job duties.
- Deliberately create, propagate, or distribute malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Logging into a device with an account that the user is not expressly authorized to access.
- Disrupt network communications. This includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, port scanning or security scanning and forged routing information.
- Port scanning or security scanning is expressly prohibited.
- Executing any form of network monitoring which will intercept data.
- Circumventing user authentication or security on any network, workstation, device or system.
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's session.
- Export or Copy information about, or lists of, Buffalo County employees to parties outside Buffalo County. Exceptions would be for compliance of Open Records Requests laws.
- Copy or Export county-owned software, intellectual property.
- Copy, export and distribute data not specifically related to your job duties.
- Using any Instant Messaging (IM) software communications service that enables you to create a kind of private chat room with another individual in order to communicate in real time over the Internet from any device.

Remote Access: Refer to Policy 404 Virtual Private Network (VPN).

Social Media and Online Conduct: Refer to Policy 403 Social Media.

Policy Violations: Violations of this policy may result in disciplinary action, up to and including termination of employment or contract, as well as legal penalties, where applicable.

Policy 401 - Effective May 31, 2015; Revised June 26, 2023