



KELLY MADIGAN
Inspector General

STEVE QUISENBERRY
Deputy Inspector General

Office of the Inspector General

April 26, 2024

D'Andrea L. Walker
County Administrative Officer
400 Washington Avenue
Towson, Maryland 21204

Re: OIG Investigative Report – Case No. 24-010

The mission of the Office of the Inspector General (hereafter “the Office”) is to provide increased accountability and oversight in the operations of the Baltimore County government (hereafter “the County”) by identifying fraud, waste, and abuse, while also striving to find ways to promote efficiency, accountability, and integrity.

Between April 2021 and February 2024, the Office issued six reports concerning the misuse of the County’s electronic communications system by eight different employees (hereafter “the Subject Employees”). Three of the reports were issued to the public and three were issued internally to the County’s Administration. In each of the six investigations associated with those reports, the Office reviewed the County email accounts of the Subject Employees and in some cases, the files stored by the Subject Employees on the County’s computer drives.

As a result of the six investigations conducted by the Office, it was determined that all of the Subject Employees had misused their County email accounts, including three of the Subject Employees who had sent sensitive or confidential County data to a family member. Also, five of the Subject Employees had stored inappropriate content on the County’s computer drives. In addition, some of the Subject Employees had misused County software applications, including one of the Subject Employees who had used a service paid for by the County to conduct their own private business. Finally, two of the Subject Employees had attached personally-owned, unauthorized removable USB drives, which contained personal data, to their County computers. All of this conduct was in violation of the County’s electronic communications policy.

Because the misuse of the County’s computer system has been central to several of the Office’s investigations over the past few years, the Office has determined that the County’s existing information technology policies are either not effectively being communicated to County employees or the ramifications of such policy violations are not severe enough to deter the misconduct. As a result, there is a concern that the misuse of the County’s computer system will

continue, and that such ongoing conduct could jeopardize County data and the integrity of the County's information systems.

I. Applicable Policies

Listed below are the applicable subsections from Section 1.10 of the County's Personnel Manual titled "Electronic Communications Policy." A copy of Section 1.10 in its entirety is attached to the report as **Exhibit 1**. In addition, there are three Office of Information Technology (OIT) policies that are pertinent to the report. Relevant sections from the three OIT policies, which are titled "Acceptable Use of Computer Systems," "Work Product File Storage," and "Remote Access Security," are set forth below and attached in full as **Exhibit 2**, **Exhibit 3**, and **Exhibit 4** respectively.

Personnel Manual - Section 1.10.1 "Electronic Communications Sent or Received by Employees"

This Electronic Communications Policy applies to all County employees. This Policy governs all County employees' use of the County's electronic communications system, including but not limited to, electronic documents, transmissions, photographs, information, or messages sent or received by Baltimore County employees via any County computer, laptop, computer network, electronic mail system, Internet, telephone, voicemail system, scanner, fax machine, or any other County electronic communication device or system. This policy may be changed by the County at its discretion without prior notice.

Personnel Manual - Section 1.10.3 "County Business Purposes Only"

Employees shall only use the electronic communications systems for County business purposes only. **Personal use of the County's electronic communications systems, unless pre-approved by the employee's supervisor, is strictly prohibited.** Any employee's inappropriate use or misuse of the electronic communications systems for nonbusiness purposes may lead to disciplinary action, up to and including termination. **Inappropriate use or misuse includes but is not limited to** creation, display, receipt, downloading, or transmission of sexually explicit or discriminatory images, messages or cartoons or any transmission that contains ethnic slurs, racial epithets, harassment or otherwise offensive, defamatory or interruptive communications, **unapproved personal use**, or any use that violates any federal, state or local law. If any employee received or accesses any inappropriate information or communication, the employee should promptly notify his or her supervisor. If the employee knows the party that transmitted an inappropriate communication, the employee should promptly advise the other party to cease all such inappropriate communication. Unauthorized interception of communications by any unauthorized employee is strictly prohibited and is a violation of this Policy.

Personnel Manual - Section 1.10.5 "Use of Unlicensed Software"

The County is required to enter into license agreements for all software used on County information technology resources. County departments, agencies and employees shall be

familiar with the license agreements for their software and shall not misuse such software. County departments, agencies, and employees shall not install unlicensed software on County information technology resources. No software shall be downloaded from the Internet or installed on County information technology resources without the Office of Information Technology's prior written approval. All software used on County Information Technology resources shall be installed by the responsible LAN administrator or Office of Information Technology staff, in accordance with all County license agreements and procedures. **Employees who misuse software in violation of a license agreement or this Policy** or who install or use unlicensed software on County information technology resources **will be subject to disciplinary action, up to and including dismissal.**

OIT Policy - Acceptable Use of Computer Systems

Under the "Property" heading, item #3 states "[u]se shall be limited to official purposes in the capacity for which it was assigned."

Under the "Data Protection Responsibility" heading, it states "Baltimore County employees are entrusted with access to sensitive information, which requires special protection, and care when handling...Accidental or intentional disclosure of Confidential Controlled Information (CI) can result in [a] 'breach' event, which may result in fines, legal ramification for the employee and County, termination of employment, and loss of citizen confidence in Baltimore County. All Baltimore County employees are expected to exercise due care when they are in possession of Confidential (Controlled) Information (CI)."

Under the "Standards of Use" heading, item #9 states "[e]mployees may not attach personal equipment (computers, removable media, cell phone, and other peripheral devices) to the Baltimore County network or systems without approval."

Under the "Unacceptable Use" heading, items #7 and #13 list "[u]sing Baltimore County systems for personal business activities offering products or services" and "[c]onnecting non-County equipment into the Baltimore County network or system" respectively as unacceptable uses of the County's computer systems.

OIT Policy - Work Product File Storage

Under the "Policy" heading, item #8 states "[p]ersonal files shall not be placed on County network shares, County licensed cloud storage or other County systems."

OIT Policy - Remote Access Security

Under the "Policy" heading, item #16 states "County issued devices are for County business and shall not be used as an employee primary home computer for personal use."

II. Policies Provided to New Employees

Historically, the County's new employees were provided with an Employee Handbook during their onboarding. The Employee Handbook contained a variety of policies that employees needed to abide by, including the Electronic Communications Policy (see Exhibit 1). Upon receipt of the Handbook, employees were required to sign an Employee Handbook Receipt Form. A blank Employee Handbook Receipt Form is attached as **Exhibit 5**. Since during or about 2019, the County instituted a four-page Centralized Acknowledgement Form as part of their new employee orientation process. The Centralized Acknowledgement Form covers a variety of County-related policies, including the Electronic Communications Policy and the OIT Acceptable Use of Computer Systems Policy (hereafter "the Acceptable Use Policy"). A blank Centralized Acknowledgement Form is attached as **Exhibit 6**.¹ While the Centralized Acknowledgement Form does not set forth the full language of the Electronic Communications Policy or the Acceptable Use Policy, it does state that employees have "received, read, understand, and agree to comply with" each of those policies and that the acknowledgement will be part of the employee's personnel file. However, it is the Office's understanding that in reality, employees who are currently being onboarded into the County are not receiving a hard copy of the Employee Handbook or a copy of the Acceptable Use Policy. Rather, employees are expected to take the initiative to locate those documents on the County's internal website in order to review them.

III. Relevant Reports Issued by the Office

Case #21-003

In **April 2021**, the Office issued an internal report² to the County Administration detailing an investigation into a County employee who had been regularly misusing their County email account. Some of the inappropriate email communications sent by the employee contained profanity, disparaging remarks about individuals, to include children and co-workers, sensitive health-related information concerning individuals not related to the subject employee, and County-related internal business dealings that potentially were not meant to be shared with individuals outside of the County.

Case #22-008

In **April 2022**, the Office issued an Investigative Report to the public concerning a member of County Council violating the County's Electronic Communications Policy by co-mingling campaign solicitations with their County email address. The investigation showed that between approximately April 2021 and January 2022, the Councilmember caused at least 40 emails containing campaign solicitations to be sent to constituents through a third-party email marketing service. The Councilmember used one of their County email addresses in the "from" line for all

¹ Six of the Subject Employees signed the Employee Handbook Receipt Form or the Centralized Acknowledgement Form.

² The Office currently refers to internal reports as Executive Management Referrals. For purposes of this report, any communications sent to the County Administration that was not meant for public release will be referred to as an internal report.

40 of the emails. On two occasions, constituents replied to the emails indicating they intended to make donations to the Councilmember's campaign. Those replies traveled over the County's email servers. Because the Councilmember's email address, which is the property of the County, was used in the "from" line of the emails in question, those emails were violations of the County's Electronic Communications Policy. Further, because the Councilmember's email address was in the "from" line, any replies to those emails containing campaign-related materials were sent over the County's servers, thereby, causing additional violations of the Policy. When questioned about the emails, the Councilmember told the Office that the inclusion of any campaign solicitations in any emails involving the Councilmember's County email address was done inadvertently.

Case #22-004

In **May 2022**, the Office issued an Investigative Report to the public detailing how a County employee, an attorney who was providing legal services on behalf of the County, was operating a private law practice using County resources. Specifically, at times, the employee was using the County computer system and related equipment to prepare, store, and transmit documents associated with their private law practice. In addition, the Office discovered that on one occasion, the employee had shared the details of a sensitive human resource matter with their spouse via the County email system. The Office made a recommendation that the County develop a plan to increase awareness among employees that they have a duty not to misuse County resources, including the computer system and its related elements as detailed in the Electronic Communications Policy.

Case #22-003

In **September 2022**, the Office issued an Investigative Report to the public concerning a County employee, a licensed real estate appraiser who worked on property-related matters for the County, who was operating a private real estate appraisal business using County resources. The Office's investigation substantiated that between approximately 2017 and 2021, the employee had used the County computer system, its related equipment, and a service paid for by the County, to facilitate the operation of their private business in violation of the County's Electronic Communications Policy. As a result of this investigation, the Office again recommended that the County develop a plan to increase awareness among employees that they have a duty to not misuse County resources, including the computer system and its related elements.

Case #23-007

In **January 2023**, the Office issued an internal report to the County Administration regarding a County employee who between April 2022 and July 2022, violated the County's security policies on multiple occasions by transmitting sensitive County documents from their County email account to personal and work email accounts associated with their spouse. Not only did the employee expose sensitive County data to their spouse, they potentially exposed that information to others who may have had access to their spouse's work email communications. The Office recommended that the Administration continue to reinforce to its employees, through on-line trainings and other forms of instruction, the policies pertaining to the proper usage of the County's electronic communications system and the need to protect sensitive County data from

unauthorized data leaks. Additionally, it was recommended that the Administration consider other proactive measures such as having supervisors re-enforce these policies to their employees during annual performance reviews.

Case #23-017

In **February 2024**, the Office issued an internal report to the County Administration concerning how a high-level County official and two of their subordinates had misused the County computer system to prepare and store non-County related documents. Further, all three individuals had misused their County email accounts to transmit personal data to one another as well as to others outside of the County. In addition, the investigation uncovered that two of the three employees had attached personally owned, unauthorized USB drives to their respective County-issued computers. The Office recommended that the County Administration remind all employees of their obligation to abide by the County's information technology policies, to include ensuring that County computers, drives, and email accounts are used solely for County-related business. Also, the Office recommended that employees be reminded that only authorized devices should be plugged into the County computer system. Finally, the Office recommended that employees be reminded of the ramifications of not abiding by these policies and how violations of such policies could affect their future employment with the County.

IV. Conclusion

Over approximately the past three years, the Office has produced six reports to the County Administration, three of which were made available to the public, detailing different types of misuse of the County's computer system by the Subject Employees. Pursuant to those reports, the Office has made several recommendations related to raising employee awareness of the County's information technology policies as well as each employee's obligation to abide by those policies. Despite those recommendations, the misuse appears to be ongoing, as noted in the summary of the February 2024 internal report for Case #23-017. The Office is not suggesting this is a systemic problem in the County. However, the misuse of the County's computer system has appeared often enough in the Office's investigations that it warranted the Office compiling its findings over the past three years into this report. This was done in an effort to amplify the Office's concerns and to recommend additional safeguards that could be put into place to protect the integrity of the County's computer system and to ensure that every County employee has a clear understanding of the policies that govern the use of that system. With that said, the Office recommends the following:


- The Employee Handbook should be updated to include all policies that concern employee conduct, including all relevant OIT policies. Currently, only the Electronic Communications Policy is included in the Employee Handbook. At a minimum, the Acceptable Use Policy, which is currently not being provided to employees in hard copy form and is only referenced in the Centralized Acknowledgement Form, should be added to the Employee Handbook in its entirety.

- All employees should be given a hard copy of the Employee Handbook when they are onboarded. As noted earlier in the report, this is currently not being done. Instead, employees are expected to locate an electronic version of the Employee Handbook on the County’s internal network. While this may be a relatively simple task for some of the County’s employees, there are other employees who either do not have ready-access to a computer or they do not possess the requisite skills to navigate the County’s internal network to locate such a document. While the Office realizes there would be a cost associated with printing the Handbooks, the Office believes this cost would be outweighed by the benefits gained as a result of employees’ adhering more consistently to the County’s policies.
- During the onboarding process, new employees should be given an overview of the Employee Handbook, with emphasis given to highlighting some of the more significant policies, such as those pertaining to the use of the County’s computer systems.
- The Centralized Acknowledgement Form, which lists a multitude of policies, should be replaced by a single acknowledgement form that is tied to the Employee Handbook. Once signed by the employee, the single acknowledgement form should be made part of the employee’s official personnel record. The following is suggested language for the single acknowledgement form “I acknowledge that I have received a copy of the Employee Handbook, which contains **all** of the relevant policies that govern my employment with the County. I agree to familiarize myself with these policies and to abide by them. I understand that it is my responsibility to seek clarification should I have any questions about these policies. I also recognize that should I violate any of these policies, I may be subject to disciplinary action to include termination.”
- OIT should update and strengthen the Acceptable Use Policy. The Office makes the following recommendations to accomplish this:³
 - The section titled “Unacceptable Use” should be renamed “Prohibited Activities”
 - The list of “Prohibited Activities” should be expanded to include:
 - Any activity that involves creating, copying, storing, uploading, downloading, accessing, sharing, or transmitting data that could be construed as: sexually explicit, obscene, racist, discriminatory, religious, political, or otherwise offensive
 - The use of the computer system to participate in non-profit activities or volunteer work unless such activities are expressly authorized by the County

³ As part of the investigation, the Office reviewed the information technology policies for some of the surrounding jurisdictions and the State of Maryland. The recommendations set forth by the Office are based on that review.

- Online gambling activities
 - The mining of crypto-currency
 - Personal use that goes beyond minor, incidental, or that would otherwise be deemed inappropriate
- Section 1.10.3 of the County’s Electronic Communication Policy titled “County Business Purposes Only” should be updated to include specific language to describe misuse to include: inappropriately accessing, sharing, or transmitting non-public County information to family members, associates, or any other individual that does not have the authority to view such materials.
 - On an annual basis, all employees should be reminded of their obligation to abide by the County’s OIT policies and the ramifications of not adhering to those policies. This could be accomplished by incorporating the reminder into annual performance reviews and through annual required training. Such training could be in the form of the KnowBe4 trainings that County employees are already required to take on an annual basis. The training should be tailored such that it covers the information technology policies that are specific to the County. The Office does not believe an annual reminder delivered via a Countywide email communication would be sufficient as not all County employees have access to email and even if they did, it is likely that a number of the employees would simply delete the message without reading it.
 - Each time the Office issues a public report, it should be distributed to all employees via the County email system. The distribution of these reports would increase the probability that employees see these reports and are made aware of the types of activities that are deemed violations of the County’s policies and procedures.

This matter is being referred to you for an official response. Please respond in writing by May 26, 2024, indicating what action has been taken or what action you intend to take regarding this matter. Should you have any questions, please do not hesitate to contact me.

Sincerely,

Kelly Madigan
Inspector General
Office of the Inspector General

cc: John A. Olszewski, Jr., County Executive
Dori Henry, Chief of Staff
James R. Benjamin, Jr., County Attorney
Chris Martin, Acting Director, Office of Information Technology
Renee Coleman, Director, Office of Human Resources

Section 1.10 Electronic Communications Policy

Section 1.10.1 Electronic Communications Sent or Received by Employees

This Electronic Communications Policy applies to all County employees. This Policy governs all County employees' use of the County's electronic communications system, including but not limited to, electronic documents, transmissions, photographs, information, or messages sent or received by Baltimore County employees via any County computer, laptop, computer network, electronic mail system, Internet, telephone, voicemail system, scanner, fax machine, or any other County electronic communication device or system. This policy may be changed by the County at its discretion without prior notice.

Section 1.10.2 No Expectation of Privacy

No County employee should have any expectation of privacy regarding his or her use of the County's electronic communications systems. All electronic communications sent or received by Baltimore County employees are the property of Baltimore County. Baltimore County reserves the right to monitor, access, view, read, maintain, and disclose all such electronic communications at any time without notice. Employees understand and agree that the existence of passwords does not mean their communications are private or confidential.

Section 1.10.3 County Business Purposes Only

Employees shall only use the electronic communications systems for County business purposes only. Personal use of the County's electronic communications systems, unless pre-approved by the employee's supervisor, is strictly prohibited. Any employee's inappropriate use or misuse of the electronic communications systems for nonbusiness purposes may lead to disciplinary action, up to and including termination. Inappropriate use or misuse includes but is not limited to creation, display, receipt, downloading, or transmission of sexually explicit or discriminatory images, messages or cartoons or any transmission that contains ethnic slurs, racial epithets, harassment or otherwise offensive, defamatory or interruptive communications, unapproved personal use, or any use that violates any federal, state or local law. If any employee received or accesses any inappropriate information or communication, the employee should promptly notify his or her supervisor. If the employee knows the party that transmitted an inappropriate communication, the employee should promptly advise the other party to cease all such inappropriate communication. Unauthorized interception of communications by any unauthorized employee is strictly prohibited and is a violation of this Policy

Section 1.10.4 Copyright Protected Information

Employees shall not use, download, copy, or send any information, documentation, photos, or material designated as protected by copyright or any other forms, of intellectual property protections without proper prior written authorization.

Section 1.10.5 Use of Unlicensed Software

The County is required to enter into license agreements for all software used on County information technology resources. County departments, agencies and employees shall be familiar with the license agreements for their software and shall not misuse such software. County departments, agencies, and employees shall not install unlicensed software on County information technology resources. No software shall be downloaded from the Internet or installed on County information technology resources without the Office of Information Technology's prior written approval. All software used on County Information Technology resources shall be installed by the responsible LAN administrator or Office of Information Technology staff, in accordance with all County license agreements and procedures. Employees who misuse software in violation of a license agreement or this Policy or who install or use unlicensed software on County information technology resources will be subject to disciplinary action, up to and including dismissal.

Acceptable Use of Computer Systems Policy

Purpose

The purpose of this policy is to outline the acceptable use of computer systems at Baltimore County. These rules are in place to protect employees, Baltimore County, and citizen data. Inappropriate use exposes Baltimore County to risks from malware, legal issues, and can lead to the compromise of systems, networks, and services. These minimum requirements may be augmented at any time to reflect changes in technology.

Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers of Baltimore County, including all personnel affiliated with third parties. This policy applies to all equipment and software that is owned or leased by Baltimore County.

Privacy and Ownership

1. While Baltimore County's administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the County systems remains the property of Baltimore County.
2. For security and network maintenance purposes, authorized individuals within Baltimore County may monitor equipment, systems, and network traffic at any time.
3. Baltimore County reserves the right to audit networks, systems, and accounts on a periodic basis to ensure compliance with this policy.

Property

1. Employees shall be responsible for the safekeeping of County property/equipment entrusted to them.
2. County property/equipment shall only be used by those to whom it is assigned.
3. Use shall be limited to official purposes in the capacity for which it was assigned.
4. An employee's intentional or negligent abuse or misuse of County property/equipment may lead to appropriate disciplinary action.
5. Two documented incidents of negligent property abuse within any two calendar years will be investigated and may result in wage garnishment to recoup replacement costs of property.

Data Protection Responsibility

Baltimore County employees are entrusted with access to sensitive information, which requires special protection, and care when handling. Information that requires protection is referred to as Confidential (Controlled) Information (CI) by Baltimore County (ex. first name, last name, in conjunction with a Social Security Number, date of birth etc.). Accidental or intentional disclosure of Confidential Controlled Information (CI) can result in "breach" event, which may result in fines, legal ramification for the employee and County, termination of employment, and loss of citizen confidence in Baltimore County. All Baltimore County employees are expected to exercise due care when they are in possession of Confidential (Controlled) Information (CI).

Standards of Use

1. All employees are required to complete monthly information security training. Failure to complete training will result in your account being disabled.

2. Only the authorized user is allowed to use their assigned respective account(s). Sharing accounts is prohibited.
3. Login credentials (passwords, pass-phrases, pin codes) will be protected as Confidential (Controlled) Information (CI). Passwords will consist of at least eight (8) characters with a combination of uppercase, lowercase letters, numbers, and special characters. Sharing of accounts or passwords is not authorized. Passwords will not consist of birthdays, phone numbers, or commonly known user information (like children's name). Passwords may not consist of Confidential (Controlled) Information (CI) either in part or whole.
4. Passwords will be changed every quarter (90 days).
5. All Baltimore County employees using County computer equipment are required to log off their computer at the end of their workday and leave the computer powered on. Computers are required to be left powered on to allow maintenance to be performed during off hours. Computers shall be restarted at least once a week to allow patches to be applied and maintenance tasks to complete.
6. Employees will not store, transport, or download digital Confidential (Controlled) Information (CI) to personal equipment of any type. Confidential (Controlled) Information (CI) must only be accessed on Government Furnished Equipment (GFE) that has the proper security controls in place.
7. Employees will not remove portable computers or removable media from government premises without encryption. When transporting portable computers or removable media to any remote location it is the user's responsibility to ensure that the device is encrypted prior to transporting the device. Lost or stolen devices will be reported to the Help Desk immediately.
8. Employees will report the electronic release or loss of Confidential (Controlled) Information (CI) immediately upon discovery. The release or loss of CI to unauthorized individuals may result in a breach event, which may need to be reported to the appropriate authorities.
9. Employees may not attach personal equipment (computers, removable media, cell phone, and other peripheral devices) to the Baltimore County network or systems without approval.
10. Employees shall promptly report to their supervisor and Service Desk (x8200), any loss, damage, or unserviceable condition of any County-issued property/equipment assigned for their use.
11. Employees shall not post messages to public forums (social media sites, newsgroups, websites) in any official capacity for Baltimore County unless specifically authorized based on job responsibility.

Unacceptable Use

The following activities are, in general prohibited. Under no circumstances is an employee of Baltimore County authorized to engage in an activity that is illegal under local, state, or federal law while utilizing Baltimore County resources. The list below is by no means exhaustive, but provide a framework of activities that fall into the category of unacceptable use.

1. Violation of the rights of any person or company protected by copyright trade secret, patent or other intellectual property right.
2. The installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Baltimore County.
3. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Baltimore County does not have an active license is strictly prohibited.
4. Providing information about, or lists of, Baltimore County employees to parties outside of Baltimore County without authorization.
5. Introduction of malicious programs into the Baltimore County network or system (e.g., malware, viruses, worms, hacker tools, etc.).

6. Using a Baltimore County system to procure or disseminate material that is in violation of sexual harassment or hostile workplace laws. Please refer to the Workplace Violence and Sexual Harassment Policies from Human Resources. Any form of harassment via e-mail, text messaging, telephone, paging, whether through language, frequency, or size of messages.
7. Using Baltimore County systems for personal business activities offering products or services.
8. Intentionally accessing data for which the employee is not the intended recipient or logging into a system or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties.
9. Causing network communications disruptions, which interfere or deny service to any user. "Disruption" includes, but is not limited to ping floods, packet spoofing, Denial of Service (DoS), DNS cache poisoning, forged routing, port scanning, etc.
10. Performing network monitoring to intercept data not intended for the employee, unless this activity is part of the employee's normal job responsibilities.
11. Circumventing authentication or security of any system, network, or account.
12. Copying Baltimore County data to a non-County device (or removable media) and removal from County property unless management has approved this for a specific business purpose.
13. Connecting non-County equipment into the Baltimore County network or system.
14. Certain network protocols (telnet, FTP, rlogin) and applications (P2P, Instant Messaging) are prohibited within the County network and may not be used, unless they are sanctioned by OIT for specific business purposes.
15. Altering the configuration of any County-issued system without OIT approval.

Enforcement

Any employee found to have violated this policy is subject to disciplinary action, up to and including termination of employment.

Work Product File Storage Policy

Baltimore County employees must ensure that any work products produced for the County are stored in a way that preserves the confidentiality, integrity, and availability (CIA) of that information. Work product is any document or information created for the benefit of the County. This includes work product which was produced on non-County provided equipment if the work was done specifically for the County. To preserve the CIA of work product Baltimore County Government requires that work product be stored in locations that allow the OIT the ability to backup work product files which will allow for the recovery of work product files in the event of an incident or disaster recovery scenario. While all information produced or transmitted on County systems are the property of Baltimore County Government, personal files are not considered work product. Personal files should not be stored to network shares, County licensed cloud storage, mobile device, or other County systems and will not be recovered in the event of an incident or disaster recovery scenario.

Scope

This policy applies to all Baltimore County employees and contractor's that produce work product for Baltimore County Government.

Policy

1. All work product shall be stored to a County network share or approved cloud storage location licensed by Baltimore County Government.
2. All work product created on non-County owned systems shall be transferred to County shares or approved cloud storage location licensed by Baltimore County Government to prevent loss of data.
3. Work product shall not be stored in locations that do not allow OIT to backup those files. For example, on the local hard drive of a computer (i.e. C: drive, "My Documents," local "Desktop").
4. Confidential (Controlled) information shall be stored in appropriate access "Restricted Folders."
5. Confidential (Controlled) information shall not be created or processed on non-County owned systems.
6. Confidential (Controlled) information shall not be stored on unencrypted desktops, unencrypted removable media, or unencrypted laptop computers.
7. If Confidential (Controlled) or any work product is collected or produced on a system (i.e. encrypted County issued laptop) while working remotely, the information shall be transferred to the appropriate network share at the next opportunity.
8. Personal files shall not be placed on County network shares, County licensed cloud storage or other County systems.

Guidance

Home Folders (H: Drive)

- The content of an individual's home directory is protected by file system permissions, and by default is only accessible to that individual.

- An individual's home directory is intended to contain that individual's work product related files that are not intended to be shared with others; to include text documents, music, pictures or videos related to County business.
- An individual's home directory shall not to be used to store Confidential (Controlled) information.
- The home directory can be organized further with the use of sub-directories.
- It is important to note that each individual is assigned a limited amount of storage space for their home folder. If the quota is exceeded, the individual will receive an email notification advising them to clean up or delete files from their home folder as appropriate. This quota will be enforced and the burden is on the individual to maintain their folder below the quota limit.
- All home folders are backed up on the County's enterprise backup system.

Shared Folders (S: Drive)

- The contents of the County shared folder (S:\County\Shared) is not restricted and is available to all County personnel and as such should be used with caution.
- Shared folders are intended to contain all non-Confidential (Controlled) files that may be used by more than just the creator; to include text documents, music, pictures or videos related to County business.
- Shared folders should NOT contain any software installable, executables, databases, or Confidential (Controlled) files.
- The contents of other shared folders are only restricted by department or division assigned to that shared space.
- Any file placed in a shared location will inherit equal rights by all the individuals in that shared location.
- All shared data will be backed up on the County's enterprise backup system.

Restricted Folders

- Restricted folders are shared to a specific group or subset of individuals with a verified need to access a category of Confidential (Controlled) information (i.e. health records, police files).
- Restricted folders are intended to contain Confidential (Controlled) files that may be used by more than just the creator; to include text documents, music, pictures or videos related to County business.
- Restricted folders should **not** contain any installable software, executables, or databases.
- Restricted folders are not intended to be used as a means to protect files from changes or deletion.
- The contents of restricted folders are controlled by file permissions assigned to the folder that contains the files, not the files themselves.
- Any files placed within a restricted folder will inherit the same rights as the folder itself. These rights can be different for different individuals.
- All restricted data will be backed up on the county's enterprise backup system.

Cloud Storage

- Confidential (Controlled) information is not authorized in cloud storage (see definition 1 below).
- The only approved cloud storage is Microsoft OneDrive as approved and licensed by Baltimore County Government.
- Storing work product on non-County Microsoft OneDrive (personal Office 365 accounts or other cloud storage platforms) is prohibited)
- An individual's personal OneDrive is intended to contain that individual's work product related files and may be shared with other individuals using Discretionary Access Control (DAC) (see definition 2 below).
- DAC puts the responsibility of sharing files with the individual. The individual is responsible for all files shared using cloud storage. Each user is assigned a limited amount of storage space in OneDrive. This quota will be enforced and the burden is on the individual to maintain their folder below the quota limit.
- Cloud storage allows users to recover data with recovery features and versioning.

Enforcement

Authorized OIT staff shall audit computer systems and network shares to validate compliance to this policy. Any employee found to have violated this policy is subject to disciplinary action, up to and including termination of employment.

Revision and Review

- Created October 10, 2015
- Revised March 26, 2018
- Revised March 10, 2020

Definitions

1. **Cloud Storage**—A network of connected data servers collectively used to share and access files across devices.
2. **Discretionary Access Control (DAC)**—A means of restricting access to objects based on the identity of subjects/groups they belong. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission on to any other subject.

Remote Access Security Policy - Employee

Overview

The meaning of remote access has changed with the advent of the Cloud. Remote access to County systems now encompasses more than the traditional meaning and includes any Cloud system that County employees may access. The term "County System(s)" hereafter shall refer to any network, system located in County facilities or Cloud hosted application which has been procured to house and manage Baltimore County data in the furtherance of our mission to support the citizens of Baltimore County. Remotely is defined as any access to County Systems from a non-County facility. The security of County Systems is essential and mandatory. Each County employee given the privilege of accessing County Systems remotely shall not compromise any County System, and shall only access County Systems for County business purposes in accordance with this Security Policy.

Scope

This policy applies to all Baltimore County employees granted the privilege of accessing any County System remotely.

Policy

1. All County employees must submit a Remote Access Request Form upon start of employment.
2. Access to County Systems may only be made through a secure remote connection.
3. Each employee understands and agrees that it is their responsibility to manage their remote access accounts, and must take the necessary and reasonable precautions to protect their account, and remote access device(s). An employee must inform The Office of Information Technology (OIT) immediately by calling the Service Desk at 410-887-8200 if they determine their account has been tampered with, information was disclosed inadvertently or intentionally to others, or if the employee transfers departments, leaves the employment of the County; or if for any reason the employee no longer requires remote access.
4. An employee must call the Service Desk at 410-887-8200 for issues with their County devices.
5. Request to reset password remotely will require identity proofing by verifying specific personal information. Employees with Administrative privileges may need to present themselves in person for password resets.
6. OIT is responsible for providing employees access and maintaining availability of remote resources.
7. Sharing of remote access accounts is not permitted. Each employee must obtain an individual account to use remote access.
8. Each employee must continue to follow all OIT policies while connected to County Systems remotely.
9. Employees shall not modify or circumvent remote access configuration settings as configured and managed by OIT.

10. All activity associated with remote access connectivity will be logged and audit trails will be reviewed regularly.
11. The County reserves the right to suspend an employee's access to the County Systems for any reason.
12. Utilizing the remote access solution to bulk transfer files or Confidential (Controlled) information to a remote system is prohibited.
13. Employees utilizing personal equipment to connect to County resources remotely may be denied access if the device utilized does not meet minimum standards such as an active up-to-date antivirus product or other minimum requirement as determined by OIT.
14. Employees will follow all requirements outlined in the work from home agreement.
15. An employee shall only connect to County Systems through remote access services for County business. The employee shall not connect to County Systems for any other purpose or reason, and shall promptly terminate their connection to the County System when County business is complete.
16. County issued devices are for County business and shall not be used as an employee primary home computer for personal use.
17. County issued devices may not be taken outside of the Continental United States for remote access. Please see the Travel Policy for further details.
18. Remote access to County Systems from outside the Continental United States is prohibited without Agency/Office/Department Director and OIT Director approval. Please see the Travel Policy for guidance.
19. An employee who establishes access to a County System remotely shall not walk away and leave their computer unattended. If the employee must walk away from their computer, they must either lock their computer or log out and reconnect at a later time.
20. The remote access solution(s) have a built in 30-minute idle time out. If there is no activity on your session for 30 minutes, the employee will automatically be logged out of County Systems.
21. Non-emergency personnel that do not utilize remote access services routinely (three months) will be blocked by OIT and a new request in accordance with this Security Policy must be submitted to OIT for approval by the Director of OIT.

Enforcement

1. Violation of this Security Policy may result in the removal of remote access. Any County employee who violates this Security Policy may be subject to disciplinary action, up to and including termination of employment.
2. The undersigned acknowledges having received a copy of and reading this Security Policy. By signing below, the undersigned hereby evidences their receipt, knowledge, understanding, and acceptance of this Security Policy and all of their duties and responsibilities associated with receipt of remote access to County Systems. The undersigned understands the consequences of their noncompliance with this Security Policy and that they may be responsible for actual damages and subject to disciplinary actions.

Signature

Sign and attach the [Remote Access Security Employee Policy](#) (PDF) when submitting requests for remote access in accordance with this policy.

Please download, sign and submit the [Remote Access Security Policy – Remote Employee](#) document to verify you have read and understand this policy.

Revision History

- Revised August 8, 2017
- Revised September 7, 2017
- Revised June 28, 2023



Employee Handbook Receipt Form

I have received a copy of the Employee Handbook which outlines the benefits, policies, and employees responsibilities for Baltimore County government. I will familiarize myself with the information in this handbook, seek verification or clarification when necessary, and comply with the policies, procedures and requirements for benefits pertaining to the County and agency in which I am employed.

Employee signature

Employee name (please print)

Date



Office of Human Resources

New Employee Orientation | Centralized Acknowledgement Form

ACKNOWLEDGEMENT OF EMPLOYEE HANDBOOK

I have received a copy of the Employee Handbook which outlines the benefits, policies, and employees responsibilities for Baltimore County government. I will familiarize myself with the information in this handbook, seek verification or clarification when necessary, and comply with the policies, procedures and requirements for benefits pertaining to the County and agency in which I am employed. I am aware that a copy of this Acknowledgment will become part of my personnel file.

-EMPLOYEE INITIALS _____

disciplinary action may include counseling, written warning, transfer, demotion, discharge, or any other action deemed appropriate by Baltimore County. Baltimore County will aggressively take appropriate action to prevent repeated acts of harassment. I also am aware that a copy of this Acknowledgment will become part of my agency personnel file.

ACKNOWLEDGEMENT OF WORKPLACE VIOLENCE POLICY

Baltimore County is an equal opportunity employer and does not discriminate against employees or job applicants on the basis of race, color, religion, sex, age, national origin, physical or mental disability, gender identity, marital status, sexual orientation or genetic information except where a bona fide occupational qualification applies. Baltimore County will recruit, hire, train and promote persons in all job classifications, without regard to race, color, religion, sex, age, national origin, physical or mental disability, gender identity or marital status, sexual orientation or genetic information except where a bona fide occupational qualification applies. Baltimore County has administered, and will continue to administer, all aspects of employment -- including, but not limited to, compensation, benefits, transfers, layoffs, return from layoff, sponsored training, educational tuition assistance, and social and recreation programs without regard to race, color, religion, sex, age, national origin, physical or mental disability, gender identity or marital status, sexual orientation or genetic information except where a bona fide occupational qualification applies.

I am aware that a copy of this Acknowledgment will become part of my personnel file.

-EMPLOYEE INITIALS _____

It is the policy of Baltimore County to provide a work environment that is free from violence, threats of violence, harassment, intimidation and other abusive behavior. Such behavior will not be tolerated in the workplace. Individuals who violate this policy may be removed from the workplace and are subject to disciplinary action, including dismissal, criminal prosecution, or both. Workplace violence may include oral or written statements, gestures, or expressions that communicate a direct or implied threat of harm. In addition, the use or possession of any dangerous weapon (i.e., gun, sword, bow and arrow, knife, etc.) is prohibited on County property, in County vehicles, and in private vehicles used for County business or entering County property, **unless authorized by the County.**

I acknowledge that I have received, read, understand, and agree to comply with the County's Workplace Violence Policy. I am aware violations of this policy will result in termination. Employees who become aware of any violent or threatening behavior that has caused an injury or poses an imminent threat of harm should immediately call 911 and notify supervision. All other threatening, intimidating, or abusive behavior should be reported to supervision or the Office of Human Resources (OHR) at 410-887-3122. I also am aware that a copy of this Acknowledgment will become part of my agency personnel file.

ACKNOWLEDGEMENT OF SEXUAL HARASSMENT POLICY

Sexual harassment is a violation of federal, state and local law and will not be tolerated by Baltimore County. Sexual harassment has no legitimate business purpose, and therefore should not occur in the work environment. Sexual harassment adversely affects not only the person to whom it is directed, but also hurts employee morale overall. Preventing sexual harassment is a team effort and therefore, the cooperation of all employees is necessary to eliminate sexual harassment. All employees are expected to conduct themselves in a professional and businesslike manner, and report incidents of harassment they observe promptly as provided in the full details of the policy. Any employee of Baltimore County found to be in violation of this sexual harassment policy will be subject to disciplinary action. Similarly, Baltimore County will take appropriate disciplinary action against anyone who attempts to retaliate against employees who complain about alleged harassment, or against any individual who participates in an investigation of alleged sexual harassment.

I acknowledge that I have received, read, understand, and agree to comply with the County's Sexual Harassment Policy. I am aware

-EMPLOYEE INITIALS _____

ACKNOWLEDGEMENT OF SUBSTANCE ABUSE POLICY

It is the intent of Baltimore County to maintain a work place that is free of drugs and alcohol. All employees are expected to obey all laws regarding the use of illegal drugs or alcohol. Baltimore County government prohibits the possession, unlawful manufacturing, distribution of illegal drugs or the abuse of alcohol or prescription drugs while on Baltimore County premises during work hours.

I acknowledge that I have received, read, understand, and agree to comply with the County's Substance Abuse Policy. I am aware any employee violating this policy will be subject to appropriate discipline, including termination. Baltimore County government will, however, give the same consideration to persons with chemical dependency as it does employees having other illnesses. Although seeking assistance for chemical dependency will not, in and of itself, result in disciplinary action. Poor performance, poor attendance or behavioral problems will result in disciplinary actions - including termination. I also am aware that a copy of this Acknowledgment will become part of my personnel file.



Office of Human Resources

New Employee Orientation | Centralized Acknowledgement Form

-EMPLOYEE INITIALS _____

ACKNOWLEDGEMENT OF SMOKE FREE POLICY

Smoking is prohibited in all government buildings in Baltimore County. Smoking is also prohibited in all County vehicles.

I acknowledge that I have read, understand, and agree to comply with the County's Smoke-Free Policy. I am aware that a copy of this Acknowledgment will become part of my personnel file.

-EMPLOYEE INITIALS _____

ACKNOWLEDGEMENT OF ACCEPTABLE USE POLICY

The purpose of this policy is to outline the acceptable use of computer systems at Baltimore County. These rules are in place to protect employees, Baltimore County, and citizen data. Inappropriate use exposes Baltimore County to risks from malware, legal issues, and can lead to the compromise of systems, networks, and services. These minimum requirements may be augmented at any time to reflect changes in technology.

I acknowledge that I have received, read, understand, and agree to comply with the County's Acceptable Use Policy. I am aware any employee found to have violated this policy is subject to disciplinary action, up to and including termination of employment. I also am aware that a copy of this Acknowledgment will become part of my personnel file.

Revision date: June 2019

-EMPLOYEE INITIALS _____

This Electronic Communications Policy applies to all County employees. This Policy governs all County employees use of the County's electronic communications system, including but not limited to, electronic documents, transmissions, photographs, information, or messages sent or received by Baltimore County employees via any County computer, laptop, computer network, electronic mail system, internet, telephone, voicemail system, scanner, fax machine, or any other County electronic communication device or system. This policy may be changed by the County at its discretion without prior notice.

I acknowledge that I have received, read, understand, and agree to comply with the County's Electronic Communications System. I am aware employees who misuse software in violation of a license agreement or this Policy or who install or use unlicensed software on County information technology resources will be subject to disciplinary action, up to and including dismissal. I also am aware that a copy of this Acknowledgment will become part of my personnel file.

-EMPLOYEE INITIALS _____

ACKNOWLEDGEMENT OF SAFETY AND HEALTH POLICY

The safety and health of employees and the public we serve are the primary concern of every aspect of the operation of Baltimore County Government. This administration is committed to providing a safe work environment and to comply with all applicable occupational health and safety laws and guidelines. The Safety and Health Policy is aimed at identifying, correcting and preventing safety and health hazards in the work environment. The success of this policy depends on the support and cooperation of every employee and supervisor.

I acknowledge that I have received, read, understand, and agree to comply with the County's Safety and Health Policy. I am aware failure to comply may result in removal from job and/or disciplinary action up to and including termination. I also am aware that a copy of this Acknowledgment will become part of my personnel file.

-EMPLOYEE INITIALS _____

ACKNOWLEDGEMENT OF HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) PRIVACY POLICY

HIPAA mandates standards that ensure the security and integrity of protected health information (PHI) that is maintained and/or transmitted electronically. It is the policy of Baltimore County to comply fully with all State of Maryland and Federal Regulations. County employees who come into contact with PHI will be trained on procedures to safeguard and process the information they handle. Employees who fail to comply with this policy are subject to disciplinary action, including dismissal, as well as civil and criminal penalties. County employees are required to cooperate with internal or external audit inquiries.

I acknowledge that I have received and read the County's HIPAA Privacy Policy. I am aware that a copy of this Acknowledgment will become part of my personnel file.

-EMPLOYEE INITIALS _____

ACKNOWLEDGEMENT OF DISABILITY POLICY

It is the policy of Baltimore County to provide equal employment opportunity for all qualified individuals, including those with disabilities as defined by Federal and State law (including disability caused or contributed to by pregnancy). The County seeks to ensure access to employment opportunities based on merit and will provide safe and reasonable accommodation to enable qualified individuals to perform the essential functions of a job. In all cases, any modifications to working conditions are required to comply with Baltimore County workplace safety and health policies and procedures.

I acknowledge that I have received and read the County's Disability Policy. I am aware that a copy of this Acknowledgment will become part of my personnel file.

-EMPLOYEE INITIALS _____



Office of Human Resources

New Employee Orientation | Centralized Acknowledgement Form

ACKNOWLEDGEMENT OF ABSENCE CONTROL POLICY

It is critical to the success of Baltimore County Government that employees report to work promptly every scheduled work day to perform their assigned tasks. By accepting employment with 16 Baltimore County, employees are indicating that they will take appropriate action to manage their personal affairs, maintain good health standards and take precautions against accidents. Unfortunately, when an employee fails to make the necessary arrangements to ensure their regular attendance at work, morale among co-workers suffers, the cost of operating County Government escalates and there may be significant delays in the delivery of services to the citizens of Baltimore County. In order to help minimize the amount of time County employees have unplanned absences from work, an Absence Control Policy has been developed.

I acknowledge that I have received, read, understand, and agree to comply with the County's Absence Control Policy. I am aware after the appropriate corrective action has taken place, any continued violation of this policy is subject to disciplinary action, up to and including termination of employment. I also am aware that a copy of this Acknowledgment will become part of my personnel file.

-EMPLOYEE INITIALS _____

ACKNOWLEDGEMENT OF INCLEMENT WEATHER POLICY

In the interest of the welfare and safety of its employees, the County may curtail some operations because of bad weather. If so, employees may be dismissed from work early or, under severe conditions, may be excused for an entire day's work with no deduction from pay or accrued leave. If the employee's job is in one of the vital services or if the employee's agency especially needs the employee during bad weather conditions, the employee may be designated as emergency/essential and asked to stay on the job or report to work while other fellow workers are excused. The employee will be informed if he/she is designated as 'emergency/essential'. The designation of 'emergency/essential' is not grievable by the employees so designated.

I acknowledge that I have received and read the County's Inclement Weather Policy. I am aware that a copy of this Acknowledgment will become part of my personnel file.

-EMPLOYEE INITIALS _____

ACKNOWLEDGEMENT OF POLITICAL ACTIVITY POLICY

No employee of the County may be prohibited from, discriminated against or favored for participating in politics or political campaigns. However, no official or employee may participate in political activity while on the job during working hours. No County employee or officer shall be obligated to contribute in any way to an election campaign or political party.

I acknowledge that I have read, understand, and agree to comply with the County's Political Activity Policy. I am aware that a copy of this Acknowledgment will become part of my personnel file.

-EMPLOYEE INITIALS _____

POLICIES BELOW ARE AS APPLICABLE

ACKNOWLEDGEMENT OF CELL PHONE USAGE POLICY

It is the policy of Baltimore County to emphasize its commitment to the safe operation of all motor vehicles used by its employees while on County business. Therefore, the usage of cell phones, except when using a hands free device, while driving on County business is prohibited. If you receive a cell phone call while driving on County business, allow it to go to voicemail and when safe pull to the side of the road and stop to return the call. If you need to make a cell phone call, you are required to stop the vehicle you are driving to make the call.

I acknowledge that I have received, read, understand, and agree to comply with the Cell Phone Usage Policy. I am aware violation of this policy is subject to disciplinary action, up to and including termination of employment. I also am aware that a copy of this Acknowledgment will become part of my personnel file.

-EMPLOYEE INITIALS _____

ACKNOWLEDGEMENT OF COMMERCIAL DRIVER'S LICENSE POLICY

The United States Federal Transit Administration and Department of Transportation Regulation 49CFR Parts 40 and 382 mandates drug and alcohol testing of all operators of Commercial Motor Vehicles (CMV) who are required to possess a Commercial Driver's License (CDL). This same policy applies to employees in safety sensitive positions. Safety-sensitive positions include jobs such as inspecting, dispatching and follow-up. The drugs screened are those listed in the DOT regulations. The pre-employment drug and alcohol testing requirement applies to both new employees and current employees who transfer to positions requiring a CDL, and/or safety sensitive positions. Baltimore County employees in safety sensitive positions will be subject to random testing under this policy. Employees will be notified on the day of the random testing to report to a designated medical services provider at an appointed time.

I acknowledge that I have received and read the County's Commercial Driver's License Policy. I am aware that a copy of this Acknowledgment will become part of my personnel file.

-EMPLOYEE INITIALS _____

ACKNOWLEDGEMENT OF VEHICLE MANAGEMENT SYSTEM POLICY

The County has installed Global Positioning System (GPS) tracking equipment in all County-owned vehicles. The purpose of the equipment is to improve overall efficiency and reduce vehicle operating costs by ensuring that County vehicles are operated within established guidelines. This policy is adopted and designed to establish standards concerning the operation of County vehicles and the use of GPS to ensure that County employees are working in a safe and secure environment. This policy applies to all County employees operating a County vehicle at any time and for any purpose. This policy does not apply to police vehicles and fire equipment (but does apply to Fire Marshal vehicles). All County vehicles will be monitored for compliance with these standards. Department Heads or their designees are responsible for monitoring the GPS data. All work requests for a given individual must match the vehicle tracking information for a given day.



Office of Human Resources

New Employee Orientation | Centralized Acknowledgement Form

I acknowledge that I have received and read the County's Vehicle Management System Policy. I am aware exceeding the established threshold set for these standards will be considered violation of this policy and may subject the violator to disciplinary action at management discretion. I also am aware that a copy of this Acknowledgment will become part of my personnel file.

-EMPLOYEE INITIALS _____

ACKNOWLEDGEMENT OF TELEWORK POLICY

The Telework Policy applies to all eligible employees (non-probationary) who have valid executed telework agreements. Telework is a management option, not an employee right. It is a privilege extended to employees as a voluntary option with the clear understanding that not every job and every employee may be adaptable for remote work. It is, instead, an option that management uses whenever it determines that it is most appropriate for the situation and circumstances. This is a voluntary program both for the County and the employee and this privilege can be terminated by the employee or the County Administration with or without cause.

I acknowledge that I have received and read the County's Telework Policy. I am aware failure to meet any of the following guidelines will result in the termination of the teleworking privilege and/or other appropriate actions. I also am aware that a copy of this Acknowledgment will become part of my personnel file.

-EMPLOYEE INITIALS _____

ACKNOWLEDGEMENT OF LACTATION POLICY

In recognition of the health benefits of breastfeeding for infants and their mothers, this policy provides reasonable break time during the workday to express milk and requires agencies to provide an appropriate room for this purpose. This policy is designed in compliance with the Fair Labor Standards Act (FLSA), 29 U.S.C. § 207 (r). For up to one (1) year after the birth of a child, an employee will be permitted to take reasonable breaks during the workday to express breast milk. Agencies must provide a reasonable amount of break time to express milk. Although the frequency and length of such breaks may vary, a breastfeeding employee will typically require between two and three breaks in an eight-hour period. Such breaks often last anywhere from fifteen to thirty minutes with additional time needed for set-up and clean-up. This policy strictly prohibits any form of retaliation (or threats of retaliation) for requesting or receiving an accommodation under this policy. Any retaliation will result in disciplinary action, up to and including discharge from employment. Concerns about retaliation should be promptly reported to the Office of Human Resources (OHR) agency representative.

I acknowledge that I have received and read the County's Lactation Policy. I am aware Baltimore County is not responsible for the integrity or security of breast milk stored on County property. I also am aware that a copy of this Acknowledgment will become part of my personnel file.

-EMPLOYEE INITIALS _____

| SIGNATURES | | |
|---------------------------|-------------------|--------------------|
| <i>Danielle Duppins</i> | Danielle Duppins | |
| SIGNATURE OF OHR ISSUER | PRINT NAME | DATE SIGNED |
| EMPLOYEE SIGNATURE | PRINT NAME | DATE SIGNED |



JOHN A. OLSZEWSKI, JR.
County Executive

D'ANDREA L. WALKER
County Administrative Officer

June 26, 2024

Ms. Kelly Madigan
Inspector General
Office of the Inspector General
Baltimore County Government
400 Washington Avenue
Towson, Maryland 21204

RE: IG Investigative Report 24-010

Dear Ms. Madigan:

Thank you for providing an opportunity to respond to the Investigative Report, Case No. 24-010 regarding the misuse of County electronic communication systems. The Administration has carefully reviewed the report findings and recommendations.

This Administration takes the misuse of County electronic communications seriously. We continuously work on reviewing, updating, and clarifying policies. As stated in our policies, we implement administrator discipline in response to the misuse of these policies, including up to termination where appropriate. As stated in your report, we concur that this not a systemic problem in the County. We offer the following response to your recommendations and statements.

Statement: ...the Office has determined that the County's existing information technology policies are either not effectively being communicated to County employee's or the ramification of such policy violations are not severe enough to deter the misconduct.

Response: The administration refutes this statement and argues the County effectively communicates our policies, and that ramifications of technology policy violations are appropriately severe. Out of the six employees' reports were conducted on, five are no longer employed by the County.

| OIG Report | Date of Report | Employment Status |
|-----------------|----------------|---|
| Case No. 21-003 | April 2021 | Resigned in-lieu of termination. Not eligible for rehire. |
| Case No. 22-008 | April 2022 | Report about Councilmember. Not subject to Executive Branch employment oversight. |
| Case No. 22-004 | May 2022 | Resigned. Not eligible for rehire. |
| Case No. 22-003 | September 2022 | Resigned in-lieu of termination. Not eligible for rehire. |

| | | |
|-----------------|---------------|--|
| Case No. 23-007 | January 2023 | Still employed. Received verbal counseling. |
| Case No. 23-017 | February 2024 | One employee terminated. Two employees received other disciplinary action. |

Statement: ...it is the Office's understanding that in reality, employees who are currently being onboarded into the County are not receiving a hard copy of the Employee Handbook or a copy of the Acceptable Use Policy.

Response: The Office is correct in these assumptions. Employees do not receive a hardcopy of the handbook. However, they do receive a copy of the policies once they sign agreeing to abide by the policies during their new employee orientation and sign in. They are also given instructions on how to access these policies via BCnet. The Administration is currently working on implementing best practices on how employees are able to access these policies and signed acknowledgements through Workday.

Statement: ...The Office is not suggesting this is a systemic problem in the County.

Response: We concur and agree this is not a systemic problem within the County. Nonetheless, we will develop a business process that requires employees to acknowledge and sign all centralized policies on an annual basis to address this issue.

Recommendation: The Employee Handbook should be updated to include all policies that concern employee conduct, including all relevant OIT policies.

Response: We are currently updating the Employee Handbook and will provide a link for employees to have access to it electronically.

Recommendation: During the onboarding process, new employees should be given an overview of the Employee Handbook, with emphasis given to highlighting some of the more significant policies, such as those pertaining to the use of the County's computer system.

Response: The Administration already engages in this process but we do not provide a hardcopy of the Employee Handbook.

Recommendation: The Centralized Acknowledgement Form, which lists a multitude of policies, should be replaced by a single acknowledgement form that is tied to the Employee Handbook.

Response: We are currently updating the acknowledgement to include the most up to date OIT policies. These updates will be completed within the next 90 days.

Recommendation: OIT should update and strengthen the Acceptable Use Policy...

Response: OIT is currently reviewing the Acceptable Use Policy and will make updates as necessary.

Recommendation: On an annual basis, all employees should be reminded of their obligation to abide by County's OIT policies and the ramifications of not adhering to those policies.

Response: We are working on a process for employees to review policies in Workday. This process will also provide receipt of their review and acknowledgement tracked in Workday. The goal is to have this implemented by the beginning of the new calendar year (January 2025).

Thank you for the opportunity to respond. Please let me know if you have questions or need further information.

Sincerely,



D'Andrea L. Walker
County Administrative Officer

cc: John A. Olszewski, Jr. County Executive
Dori Henry, Chief of Staff
James R. Benjamin, Jr., County Attorney
Christopher Martin, Interim Director, Office of Information Technology
Renee Coleman, Director, Office of Human Resources