FILE REFERENCE NO: 20260229
ORDINANCE NO: 3506

AN ORDINANCE

AMENDING: Marietta City Code Chapter 4-4, Personnel Rules and Regulations

---

NOW, THEREFORE, BE IT HEREBY ORDAINED BY THE MAYOR AND COUNCIL OF THE CITY OF MARIETTA, GEORGIA, THAT:

Section 1: Section 4-4-11-010 - Internet and electronic mail acceptable use policy, shall read:

4-4-11-010 Internet and electronic mail acceptable use policy.

A. General Principles. This statement sets forth the policy of the City of Marietta (city) and Marietta Board of Lights and Water (BLW) with regard to access to and disclosure of electronic mail (e-mail), technology solutions/collaboration tools and other electronic records sent or received by employees, utilizing city/BLW-provided technology and online services.

This policy governs use of city/BLW information technology resources, including but not limited to: e-mail, collaboration platforms, internet access, cloud services, mobile devices, and network infrastructure.

Internet, technology solutions/collaboration tools and e-mail services are provided by the city/BLW to support open communications and exchange of information and the opportunity for collaborative government-related work. The city/BLW encourages the use of electronic communications by its agencies and employees. Although access to information and information technology is essential to the missions of government agencies and their users, use of internet, technology solutions/collaboration tools, and e-mail services is a revocable privilege. Conformance with acceptable use, as expressed in this policy statement is required. Departments of the city/BLW are expected to maintain and enforce this policy.

Internet, technology solutions/collaboration tools, and e-mail communications to and from city/BLW employees are presumed to be work-related. City/BLW computers and any data stored in them are the property of the city/BLW and may be accessed at any time by authorized officials of the city/BLW. Employees shall not expect privacy in the use of city/BLW computers. The city/BLW may, without notice, monitor internet, technology solutions/collaboration tools, and/or e-mail to ensure it is being used only for business purposes.

At a minimum, users of internet, technology solutions/collaboration tools, and e-mail services provided by the city/BLW are expected to:

1. Inform themselves of this acceptable use policy and acceptable and unacceptable uses on the internet, technology solutions/collaboration tools, and with e-mail used both internally to the city/BLW and externally to the world at large. The burden of responsibility is on the user to abide by the acceptable and unacceptable uses, or prior to use, inquire about uses not cited. Compliance with applicable acceptance use restrictions is mandatory.
2. Use city/BLW-provided internet, technology solutions/collaboration tools, and e-mail services for city/BLW government-related activities and not for personal business.
3. Abide by the legal protection provided by copyright and license to programs and data.
4. Know and follow the generally accepted etiquette of the internet. For example, use civil forms of communication when using e-mail, technology solutions/collaboration tools, and/or the internet.

5. Avoid uses of the network e-mail, technology solutions/collaboration tools, blogging, and/or the internet that reflect poorly on their department or on the city/BLW. Statements on e-mail, technology solutions/collaboration tools, and/or the internet should reflect the same language used in the presence of a department head or the city manager. City/BLW Conflict of Interest Code and other existing and evolving rules, regulations, and guidelines on ethical behavior of government employees and the appropriate use of government resources apply to the use of electronic communications systems supplied by the city/BLW.

6. Make each electronic communication truthful and accurate.

B. Specifically Acceptable Uses of the Internet, Technology Solutions/Collaboration Tools, and E-mail.

1. Communication and information exchange directly related to the mission, charter, or work tasks of the city/BLW department.

2. Communication and exchange for professional development, to maintain currency of training or education, or to discuss issues related to the user's city/BLW research or programs.

3. Use in applying for or administering grants or contracts for the city/BLW's research or programs.

4. Use for advisory, standards, research, analysis, and professional society activities related to the user's city/BLW work tasks and duties.

5. Announcements of new city/BLW regulations, ordinances, procedures, policies, rules, services, programs, information, or activities.

6. Any other government administrative communications not requiring a high level of security.

C. Specifically Unacceptable Uses of the Internet, Technology Solutions/Collaboration Tools and E-mail.

1. Use of the internet, technology solutions/collaboration tools, and/or e-mail for any purpose that violates a federal, state, or local law.

2. Use for any for-profit activities unless specific to the charter, mission, or duties of the city/BLW department.

3. Use for purposes not directly related to the mission, charter, or work tasks of the city/BLW department during normal business hours.

4. Use for private business, including commercial advertising.

5. Use for access to and distribution of:

   a. Patently offensive representations or descriptions of ultimate sexual acts, normal or perverted, actual or simulated or patently offensive representations or descriptions of masturbation, excretory functions, or lewd exhibition of the genitals;

   b. Material sent or received in violation of the Protection of Children Against Sexual Exploitation Act of 1977, as amended, 18 U.S.C. 2252.

6. Use for, access to and distribution of computer games and/or music that have no bearing on the department's mission. Employees may not use the internet to download games or other entertainment software. Employees may not download screen-savers, music files (e.g., MP3) or messaging software from the internet. This includes unauthorized messaging or collaboration platforms. Some games that help teach, illustrate, train, or simulate agency-related issues may be acceptable.

7. Use city/BLW-provided internet, technology solutions/collaboration tools, and/or e-mail services so as to interfere with or disrupt network users, services, or equipment.

8. Intentionally seek out information on, obtain copies of, or modify files and other data, which are confidential under federal, state, or local law, unless specifically authorized to do so once the legal conditions for release are satisfied.

9. No intentional copy is to be made of any software, electronic file, program, music, or data using city/BLW-provided internet, technology solutions/collaboration tools, and/or e-mail services without a prior, good faith determination that such copying is, in fact, permissible. Any efforts to obtain permission should be adequately documented. Copyrighted materials include text and pictures, video, and audio (to include music).

10. Intentionally seeking information on, obtaining copies of, or modifying files or data belonging to others without authorization of the file owner. Seeking passwords of others or the exchange of passwords is specifically prohibited.

11. Users intentionally representing themselves electronically as others, either on the city/BLW internal network or elsewhere on the internet unless specifically authorized to do so by those other users. Users shall not circumvent established policies defining eligibility for access to information or systems.

12. Intentionally developing programs designed to harass other users or infiltrate a computer or computing system and/or damage or alter the software components of same.

13. Use for fundraising or public relations activities not specifically related to city/BLW-approved activities. Approved city/BLW fundraising must be approved by the city manager.

14. Intentionally streaming non-business-related media on a network-connected PC during any time an employee is at work, not just during their work shift, i.e. this includes breaks, lunch, etc.

15. Intentionally misusing mobile devices and harming another person's reputation, harassing, defaming, or violating the city/BLW EEO policy.

16. Intentionally tampering with, and/or disabling, automatic vehicle location (AVL) devices in city/BLW vehicles.

17. Intentionally tampering with, and/or disabling, wireless access points installed on city/BLW networks. Only IT staff may install wireless access points on city/BLW networks.

City Code Section 44-20-040, Rule Z, requires disciplinary action for improper or inappropriate use of the city/BLW computer hardware or software or communications systems and, specifically, violations of this section of the Code of Ordinances.

D. Additional Guidelines.

1. Computer Viruses on Downloaded Software. Any software or hardware obtained from outside the city/BLW government shall be virus checked prior to use.

2. Use by Contractors. Contractors and other non-city/BLW employees may be granted access to city/BLW-provided internet services at the discretion of the city manager or their designee. Acceptable use by contractors and other non-city/BLW employees working for the city/BLW is the responsibility of the city/BLW contract administrator. The city/BLW contract administrator is expected to provide contractors who use city/BLW internet, technology solutions/collaboration tools, and/or e-mail services with this policy.

3. Passwords and User Access Controls. Use passwords associated with a city/BLW information system only on that system. When setting up an account at a different information system that will be accessed using the internet, choose a password that is different from ones used on city/BLW information systems. Do not use the same password for both local and remote internet-accessed systems. If the password used at the remote, internet-accessed remote site were to be compromised, the different password used locally would still be secure. Passwords should not be so obvious so that others could easily guess them, and user access controls shall

be determined by the director of information technology based on industry accepted best practices.

4. Logoff (Exiting). Always make a reasonable attempt to complete the logoff or other termination procedure when finished using a remote, internet-accessed system or resource. This will help prevent potential breaches of security.

5. E-mail and Technology Solutions/Collaboration Tools Security. Unencrypted electronic mail and digital messages sent or received outside any department and on the internet cannot be expected to be secure.

6. Disclaimers. Users shall avoid being drawn into discussions where disclaimers like "this represents my personal opinion and not that of my department of the city/BLW" need to be used. When you are using internet, technology solutions/collaboration tools, and or e-mail services provided by the city/BLW, users shall remember that they are representing the city/BLW and shall act accordingly.

7. Retention. Only essential e-mail and/or instant messages shall be saved. It is the responsibility of the Director of IT or their designee, in conformance with the city's retention policy, to establish retention criteria in compliance with federal and state law for essential e-mail and other electronic records within his/her department.

8. Open Records Act. All public departments are subject to the Open Records Act. All records, including computer-based or generated information fall under this Act. Therefore, users of the city/BLW information systems should treat computer-based information as they would written communications. All information on the city/BLW computer system is confidential. Such information may not be shared with other users internally or externally except through the procedures outlined in the Georgia Open Records Act. Department heads will be responsible for determining what information is appropriate for dissemination via e-mail, instant messaging, and other forms of electronic dissemination.

9. Permanence. Users shall exercise the same care in drafting e-mail and digital records and communications that would be applied to any other written communication. E-mail is more permanent than paper communications. Anything said in e-mail and digital records may be discovered by an opponent in litigation.

10. Enforcement. All provisions of this policy are deemed rules of the city/BLW and violation of any could result in disciplinary action up to and including termination under the City Code (Section 4-4-20-040).

E. Procedures. The department head, or their delegated representative is responsible for their employees' compliance with the provisions of this policy and for investigating noncompliance. When an instance of noncompliance with this policy is discovered or suspected, the agency shall proceed in accord with departmental and city/BLW personnel policies. Complaints about inappropriate or offensive e-mail, digital records, and/or other forms of electronic communication should be promptly reported to the immediate supervisor. Such reports shall be taken seriously by the supervisor and carefully investigated. Suspension of service to users may occur when deemed necessary to maintain the operation and integrity of the city/BLW network. User accounts and network access may be withdrawn without notice if a user violates the acceptable use policy. Disciplinary action up to and including termination of employment may be imposed depending on the severity of the violation. Criminal or civil action against users may be initiated when laws are violated.

4-4-11-020 Use of licensed software.

In compliance with federal copyright laws, the city/BLW will not participate in or condone the illegal duplication of licensed software and/or digital media. Such activity is strictly prohibited on city/BLW premises and/or machinery. The city/BLW does not own the copyright to any software or its

related documentation and, unless authorized by the software developer, does not have the right to reproduce it for use on more than one computer.

With regard to use on local area networks or on multiple machines, city/BLW employees shall use the software only in accordance with the license agreement. City/BLW employees are required to report any misuse of software or related documentation within the city/BLW to their department head or the IT director. City/BLW employees, who make, acquire, or use unauthorized copies of computer software and/or digital media on devices accessing city/BLW network machinery shall be subject to disciplinary action up to and including termination of employment.

4-4-11-030 Information security policy.

A. Purpose. This document is designed to provide the city/BLW minimum security policies for protection of city/BLW assets inclusive of information, computers and networks.

B. Information Custodianship. Information, such as data, electronic mail, documents and software, are city/BLW assets. Information technology systems include any device (i) procured or maintained by city/BLW staff; and (ii) used to interact, store, or access City of Marietta data or electronic services. This includes, but is not limited to, computers, mobile devices, phones, access key pads or cards, radios, etc. By placing information on city/BLW information technology systems, employees grant the city/BLW the right to edit, delete, copy, republish, and/or distribute such information. The city/BLW at all times retains the right to access, search, and monitor all directories, electronic mail messages, instant messages, voice mail messages, internet sites visited by employees, chat groups and newsgroups, material downloaded or uploaded by users of the internet, or any other electronic or telephonic transmissions contained in or used in conjunction with the city/BLW's computer, electronic mail, instant messaging, and voice systems and equipment with no prior notice. This right applies both during employees' employment by the city/BLW and after its cessation for any reason or no reason, including whether the cessation was voluntary or involuntary. In determining the value of an asset, consideration shall be given not only to the sensitivity of the information, but also to the consequences of unauthorized disclosure, modification, destruction, or unavailability of the information. The value of these assets will determine the level of controls needed to provide adequate safeguards, backup and access controls. However, ownership, custodial responsibility and rights to these assets are herein established.

1. Records. A "record" includes any information kept, held, filed, produced or reproduced by, with or for a department in any form or media including, but not limited to, reports, statements, examinations, memoranda, opinions, folders, files, books, manuals, pamphlets, forms, papers, designs, drawings, maps, images, photos, letters, microfilms, computer tapes or discs, rules, regulations or codes.

2. Property of a Department. All records, software, and hardware that are part of a department's information system are considered property of the city/BLW and shall be used for city/BLW business purposes only.

3. Designation of Responsibility. Department heads, or their designee, have the responsibility to ensure that all city/BLW information resources, regardless of medium, are used, maintained, disclosed and disposed of according to law, regulation or policy.

4. Copyright and Licensing of Vendor Hardware and Software. Departments shall adhere to copyright laws and licensing agreements.

5. Records Retention and Destruction. City/BLW information shall be retained and/or destroyed in accordance with records retention schedules developed in cooperation with the State Archives and Records Administration (SARA) and policies and procedures established by the city/BLW, unless required otherwise by applicable laws.

6. State and Federal Access, Privacy and Confidentiality Laws. All information, regardless of the medium in which it is maintained or communicated, is subject to pertinent state and federal

laws governing access, the protection of privacy and prohibitions against unauthorized disclosure.

7. Access Categories—Classification of Information. Information classification provides a means for separating information into categories with different protective requirements. The city/BLW determines, in advance, the extent to which information shall be disclosed to specified users. Determinations shall be made based on the nature of the information and the duties of city/BLW employees. The following general categories of information serve to provide guidance in identifying appropriate users or recipients:

    a. "Public information" is information accessible under Freedom of Information Law and the Georgia Open Records Act and is available to any person, notwithstanding one's status or interest within the limitations as provided in those laws.

    b. "Restricted information" pertains to information that is not public information but can be disclosed to or used by city/BLW representatives to carry out their duties, so long as there is no legal bar to disclosure.

    c. "Confidential information" including protected health information (PHI) and Personal Identifiable Information (PII) is information that is protected by law. Access to confidential information is prohibited unless permitted by an exception in law.

C. Physical Access Security. The department head shall put into place appropriate safeguards to limit physical access to any information technology systems.

1. Secure Locations. Information technology systems and associated devices shall be stored in a location that protects them from unauthorized physical access. Physical access to such equipment potentially provides access to information stored therein.

2. Location Selection. Physical locations for all information technology systems shall be selected to protect against equipment and information loss by flood, fire, and other disasters, natural or manmade.

3. Review of New Connections to Outside Sources. Proposed access to or from a network external to the city/BLW shall be reviewed and approved by the department head or designee prior to establishment of the connection. Final approval shall be obtained from the director of IT.

4. Review of Installation. Installation, upgrades, changes and/or repairs of information technology systems (hardware, software, firmware) are to be reviewed by the IT department for potential physical security risks.

5. Platform-Specific Physical Security. Platform-specific physical security shall be established, implemented and periodically reviewed and revised as necessary to address physical vulnerabilities of that platform.

6. City/BLW Laptop, Notebook, Tablets, Cell Phone, and Portable Computer Devices. Portable computing devices shall not be left unattended at any time unless the device has been secured. When traveling, portable computers shall remain with the employee's carry-on hand luggage.

D. Information Security. The security officer (IT director or designee) is responsible for the security of all electronic information resources. Specific procedures will be developed and disseminated by the security officer to conform to the following policies. These procedures will be reviewed frequently to reflect changes in personnel and technology.

E. Information Security Administration Functions. The security officer will formally delegate responsibility for information security matters. Multiple individuals across organizational lines may be involved as long as there is a clear separation of duties and responsibilities which provide effective checks, balances and accountability.

F. Logon Security. Access to city/BLW information systems requires identification and authentication through approved methods, including Multi-Factor Authentication (MFA) for all accounts. This

includes direct logon, remote access, privileged accounts, cloud services, and mobile applications. Passwordless authentication methods (biometric, hardware tokens, passkeys) may be approved by the Director of IT or designee. Any exceptions require written approval from the IT Director with annual review..

G. Remote Access to City/BLW Information. Remote external access to city/BLW networks containing restricted or confidential information requires Multi-Factor Authentication (MFA) and connection through approved secure access methods (VPN, zero-trust network access, or approved remote access platforms). The IT Director must approve any remote access method prior to deployment, with periodic security assessments..

1. Employees accessing or possessing city/BLW data are responsible for ensuring that City/BLW data is not accessed, viewed, or overheard by unauthorized individuals.

H. External Network Access to City/BLW Information. External network access to a city/BLW network that contains restricted or confidential information including PHI requires at least a hardware or software firewall on the platform, network, or device accessing the city/BLW network. Firewalls provide network security similar to the installation of a perimeter security system on a building by blocking or permitting traffic.

I. Transaction Controls and Database Security. Transactions entered into the City/BLW production databases shall be checked for accuracy and authenticity. Database management systems (DBMS) shall implement security and authorization subsystems adequate to protect against unauthorized access and modification.

J. Downloading Software. The security officer or their designee, upon request of a department head, will determine whether downloading of software from an external site will be permitted.

K. City/BLW Owned IT Components. City/BLW hardware shall be reviewed and cleansed (sanitized) before being reassigned or discarded. The security officer or their designee shall work with IT department staff to ensure compliance with this policy. Department heads shall maintain adequate documentation of hardware/software taken off city/BLW premises by employees.

L. Electronic Communications. When transmitting confidential information, such as protected health information (PHI) or personal identifiable information (PII), on an external network (outside the firewall), city/BLW shall employ a secure technology rendering the information unusable to an unauthorized or intercepting third party.

M. Malicious Software. All city/BLW computers shall be equipped with up-to-date end-point protection software. The IT department will ensure that all network attached PCs are protected from malicious software and viruses.

N. City/BLW Security Management. Accountability and appropriate separation of duties and responsibilities are essential elements of security administration. Departments shall develop security awareness among all staff.

1. Security Training. All employees, agents and others who access city/BLW computer systems shall be provided with sufficient training and/or supporting reference materials to allow them to properly protect city/BLW information.

2. Employment Changes. Department heads or their designees shall report changes in employment status of their staff to the security officer and/or systems administrator in the IT department.

3. Audit Trails. The department head shall maintain audit trail records of individuals accessing city/BLW records sufficient to meet the requirements of the law, the city/BLW internal controls and audit requirements, and as necessary, disaster recovery requirements.

O. Information Recovery. All business applications shall have backup and recovery procedures that are documented, maintained and the backup media stored off site. The city/BLW shall test these procedures on an annual basis.

P. Data Exchange Agreements; Third Party Agreements. All agreements with third parties such as vendors, other government agencies, or contractors shall include requirements to adhere to city/BLW information security policies.

Q. Vendor/Contractor Agreements. All vendor agreements shall contain a requirement that any city/BLW information obtained as a result of such an agreement shall be the property of the city/BLW and shall not be utilized, including, but not limited to, secondary release or disclosure, without written authorization of the city/BLW.

R. Employee/Agent Responsibilities. As a condition of continued employment, all employees/agents by signature of the city/BLW's personnel policies and procedures, as may be amended, indicate that they have read and understand the city/BLW's policies and procedures regarding information security, and agree to comply in all respects to those policies and procedures.

1. Password Protection. Employees/agents shall not post or share their assigned passwords or other authentication credentials or tokens and shall develop secure passwords according to IT department security guidelines.

2. Use of Automatic Logons. Employees/agents shall not facilitate any logon procedure with local programming such as keyboard programming or scripting.

3. Unattended Computers. Unattended computers shall be logged off or protected in such a way as to protect the computer and network from unauthorized access.

S. Reporting Suspicious Events. Any observations of suspicious activity shall be reported to the appropriate department head and/or the Director of IT.

1. Suspicious activity can include: signs of unauthorized equipment usage during evenings and weekends, phone requests from unidentifiable callers for access to PHI, fraudulent or suspected phishing e-mail requests, unidentifiable files found on file servers, and unusual activity recorded in log files.

T. Shadow IT. Employees, contractors, and agents shall not, without prior written approval from the IT Director or designee:

1. Install or use unapproved software, applications, browser extensions, or plug-ins on City/BLW devices;

2. Create or utilize external cloud services, online collaboration tools, file-sharing platforms, or data storage solutions for City/BLW business;

3. Procure, connect, or operate unapproved hardware devices, including network equipment, storage devices, or internet-connected devices, on City/BLW networks;

4. Transmit, store, or process City/BLW data using non-approved systems or services.

Section 2: It is hereby declared to be the intention of this Ordinance that its sections, paragraphs, sentences, clauses and phrases are severable, and if any section, paragraph, sentence, clause or phrase of this Ordinance is declared to be unconstitutional or invalid, it shall not affect any of the remaining sections, paragraphs, sentences, clauses or phrases of this Ordinance.

Section 3: All Ordinances or parts of Ordinances in conflict with this Ordinance are hereby repealed.

Section 4: This Ordinance shall become effective upon the signature or without the signature of the Mayor, subject to Georgia laws 1983, page 4119.

DATE: _____ **APPROVED:** _____

R. Steve Tumlin, Mayor

ATTEST: _____

Stephanie Guy, City Clerk

Approved as to form: _____

Douglas R. Haynie, City Attorney