

ORDINANCE NO.: 7545

**AN ORDINANCE**

**AMENDING** the City of Marietta/BLW Personnel Rules and Regulations to clarify certain sections of the code.

---

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

**Section 1:** That Article 4-4-11, "Computer and Communication System Usage", shall be amended to read as follows:

**ARTICLE 4-4-11 Computer and Communication System Usage**

**4-4-11-010 Internet and Electronic Mail Acceptable Use Policy**

**C. Specifically Unacceptable Uses of the Internet, Instant Messaging (IM) And E-mail.**

18. 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.

**D. Additional Guidelines.**

8. Retention. Only essential E-mail and/or instant messages shall be saved. The IT department will delete E-mail transactions greater than 60 days old. It is the responsibility of the department head to establish retention criteria in compliance with federal and state law for essential E-mail and other electronic records within his/her department.

**4-4-11-020 Use of Microcomputer Software.**

In compliance with federal copyright laws, the city/BLW will not participate in or condone the illegal duplication of licensed microcomputer software and/or music. 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 music on city/BLW premises or machinery shall be subject to disciplinary action up to and including termination of employment.

#### **4-4-11-030 Information Security Policy.**

**C. Physical Access Security:** The department head shall put into place appropriate safeguards to limit physical access to any radio, computer, or computer-related device.

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 radios; computer equipment, or computer-related devices (hardware, software, firmware) are to be reviewed by the IT department for potential physical security risks.

**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.

**K. City/BLW Owned IT Components:** City/BLW hardware shall be reviewed and cleansed (sanitized) before being reassigned or discarded. The security officer 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.

**M. Virus Protection:** All city/BLW computers shall be equipped with up to date virus protection software. The IT department will ensure that all network attached PCs are virus protected.

**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.

New hires and promotional employees should be placed in the pay range at the appropriate level at the time of hire or promotion commensurate with their qualifications.

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.

**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 personal passwords, and shall develop secure passwords according to IT department security guidelines.

**Section 2:** That Article 4-12-2, "**Employee Health Insurance and Protected Health Information**", shall be amended to read as follows:

## **4-12-2-025 Employee Health Insurance and Protected Health Information**

### **H. Plan Sponsor Responsibility:**

#### **1. Administration.**

a. The benefits manager will serve as the privacy officer for the city/BLW. The privacy officer shall be responsible for the privacy program and shall regularly review the implementation of this policy and relevant privacy practices to assure that the confidentiality of individually identifiable health information is protected. If the employee has any questions regarding these policies, contact the privacy officer whose office is located in the human resources department.

b. The privacy officer is designated as the person to whom complaints should be brought. Contact the human resources department to reach the privacy officer or to obtain additional information about the plan's notice of privacy practices.

c. When performing plan administration functions on behalf of the plan, only the following employees or classes of employees will be given access to PHI to accomplish the intended purpose of the use, disclosure or request: Benefits manager, payroll manager, IT director, finance director and staff designated by the benefits manager, payroll manager, finance director and IT director.

2. Safeguards. The plan will comply with the security standards of the Act and have implemented technology and security policies to protect the personal data that is under the plan's control from unauthorized access, improper use or disclosure, alteration, and unlawful or accidental destruction. The IT director will serve as the security officer. The security officer and privacy officer have the responsibility of monitoring the program and maintaining appropriate administrative, technical and physical safeguards to protect the privacy of protected health information. The safeguards implemented include but are not limited to:

**Section 3:** That Article 4-4-16, “**Family and Medical Leave of Absence Without Pay**”, shall be amended to read as follows:

### **Article 4-4-16-090, Family and Medical Leave of Absence Without Pay**

The provisions of this section are regulated by the Family and Medical Leave Act of 1993 (P.L. 103-3) and pertinent Department of Labor regulations as they may be promulgated. The city/BLW specifically reserves the right to add to, change or abolish the provisions of this section, in whole or in part, based upon pertinent action by any appropriate legislative, judicial or regulatory authority.

**A. Eligibility and Reasons Granted.** The provisions of this section apply only to those employees who have been employed for at least 12 months (such 12 months of employment does not have to be consecutive) and who have provided at least 1,250 hours of service during the 12 months before any leave is requested. In determining the hours worked, paid leave, such as vacation, sick or compensatory leave is not included.

The city manager or a department head will grant up to a total of 12 workweeks of Family and Medical Leave Act (hereinafter FMLA) leave to any eligible employee during any 12-month period for one or more of the reasons listed below. The 12-month period for purposes of this section shall be measured forward from the beginning date of an employee's first approved FMLA leave..Employees are required to first use any accrued vacation, sick, holiday or

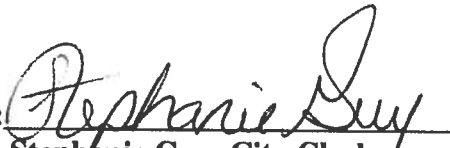
compensatory leave for all or any part of this 12-week period. When an employee uses paid leave in lieu of unpaid FMLA leave, the city/BLW will only provide sufficient unpaid leave to total 12 work weeks in the designated 12-month period of time in accordance with FMLA regulations.

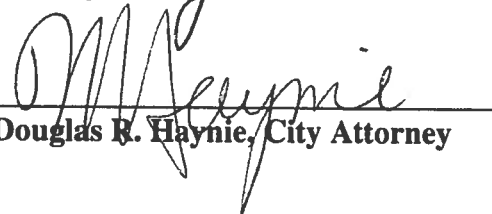
**Section 4:** It is hereby declared to be the intention of this Ordinance that its sections, paragraphs, sentences, clauses, phrases and words are severable, and if any section, paragraph, clause, phrase or word of this Ordinance is declared to be unconstitutional or invalid, it shall not affect any of the remaining sections, paragraphs, clauses, phrases or words of this Ordinance.

**Section 5:** All Ordinances or parts of Ordinances in conflict with this Ordinance are hereby repealed.

**DATE:** July 13, 2011

**APPROVED:**   
R. Steve Tumlin, Jr., Mayor

**ATTEST:**   
Stephanie Guy, City Clerk

**Approved as to Form:**   
Douglas R. Haynie, City Attorney