below one hundred sixty (160) hours. (as added by Ord. #1104, June 2005, as amended by Ord. #1158, Feb. 2007, and Ord. #1408, Feb. 2014)

4-248. Laptop computer and removable storage device security policy. Every employee, official or any authorized person using a municipal (city-owned) laptop computer or removable storage device is responsible for protecting the confidential information stored, created, processed or transmitted via the computer or device.

(1) Laptop computers and removable storage devices. Only persons showing necessity to perform specific job-related duties shall be authorized to use municipal laptop computers and/or removable storage devices. Department heads may grant this approval after consulting with the IS department.

(2) Protection of confidential data. Every user of a laptop computer or removable storage device must use reasonable care to protect confidential data.

Protection of confidential data against physical theft or loss, electronic invasion or unintentional exposure is provided through a variety of means, including user care and technological protections. Prior to the use of confidential data via laptop computer or removable storage device, users are responsible for contacting the IS department to ensure appropriate security hardware and software are in place. The use of unprotected equipment to access or store confidential information is prohibited regardless of whether the equipment is owned or controlled by the municipality.

(3) Reporting loss or theft of equipment or data. In the event a municipally-owned or controlled laptop computer or removable storage device is lost or stolen, the theft or loss must be reported immediately to the IS department.

In the event that confidential information contained on any personally-owned computer or removable storage device is lost or stolen, the theft or loss must be reported immediately to the IS department.

In the event a municipally-owned laptop computer or removable storage lost or stolen, resulting in the unencrypted personal information of any Tennessee resident being, or reasonably believed to be breached, the municipality must disclose the breach to the affected citizens in accordance with Tennessee Code Annotated, § 47-18-2107. This notification must occur in the most expedient time possible, consistent with the legitimate needs of law enforcement. The IS director is responsible for this notification process.

The purpose of this policy is to comply with state and federal regulations governing the privacy and security of information, specifically, Tennessee Public Chapter 688, 2008.

Violation of this policy may result in disciplinary action as set forth in § 4-232 or dismissal or demotion as set forth in § 4-233 depending upon the circumstances of the violation. Any employee receiving any proposed disciplinary action, dismissal or demotion may appeal said action directly to the

board of mayor and aldermen, which may affirm, reverse or modify (increase or decrease) the disciplinary action. (as added by Ord. #1246, Oct. 2009)

4-249. Use of internet and electronic mail. (1) Policy. It is the policy of the City of Manchester that all employees having global internet access and e-mail privileges shall use such access only for official work in full compliance with this policy and the policies of the city. Each user must be aware of the risks related to internet access and e-mail which cannot be eliminated but may only be managed through the exercise of prudence and caution.

All city employees authorized to use e-mail will be assigned an official city e-mail address. All official business shall be conducted using this address. No official business shall be conducted using any other address, including but not limited to those provided by Yahoo, Gmail, Netscape, etc. In the event any other address is required to perform the functions of an employee's position, the employee may use such address after written approval from the mayor and information systems director; however, this additional address may be used only when and to the extent the employee's job functions cannot be performed using his or her official city e-mail address.

(2) Procedures. (a) Use of the internet/e-mail. Employees must be individually authorized to use the internet and/or e-mail before doing so during working hours or while using any city equipment. No employee will be so authorized by the city until the employee has signed the internet use form, however failure to sign this form shall not render this policy inapplicable to such employee.

No e-mail messages sent or received on city computers is personal or private; each is the property of the City of Manchester. E-mail messages can be copied, distributed, discovered in litigation and used in disciplinary proceedings even if deleted by the recipient. Users have no expectation of privacy as to any e-mail message at any time.

(c) Principles of acceptable internet and computer system use.

(i) Use must be for legitimate work-related purposes only.

(ii) Users shall respect the legal protections afforded by copyright and license laws for programs and data.

(iii) Use must be for legitimate work-related purposes only.

(iii) Users shall identify themselves as employees of their department and the city when sending any e-mail message via the internet.

(d) Unacceptable use of the internet, e-mail and the city's computer system.

(i) Users shall respect the integrity of the city's computing system and shall not use it for unacceptable purposes or in any unacceptable manner as described below. It is

unacceptable for a user to use, submit, publish, display or transmit on the internet or any part of the city's computer system any information which:

(A) Uses the system for any illegal purpose;

(B) Contains defamatory, false, inaccurate. abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive or otherwise biased, discriminatory or illegal material, whether in the form of a "joke" or otherwise;

(C) Violates or infringes on the rights of any other person, including the right to privacy; or

(D) Modify files or data belonging to other users without explicit permission to do so.

(ii) No user other than the mayor or the various department directors shall have authority to subscribe to any service for which a fee is charged.

(iii) Users shall not use or develop programs that harass other users or infiltrate a computer or computing system or which seek to alter or damage the software components of a computer or computing system.

(e) Personal use. The prohibitions in this policy shall also not be construed to prohibit infrequent and brief use of the system for incidental personal matters by an employee during a meal or other personal break time. This is similar to an employee's limited ability to make a personal telephone call on personal time. For example, an employee may spend a minute or two looking at the weather radar online provided, however, in no event shall any such limited personal use include any activity otherwise prohibited by this policy, e.g., visiting a sexually explicit site.

(f) No right of privacy - monitoring. (i) Pursuant to the Electronic Communications Act of 1986, 18 U.S.C. 2510 et seq., notice is hereby given that there are no facilities provided by the city and its system for sending or receiving private or confidential electronic communications.

(ii) Electronic mail, whether sent via the internet or internally, may be a public record subject to public disclosure under the Tennessee Public Records Law and may be inspected by the public.

(g) Violation of this policy may result in disciplinary action as set forth in § 4-232 or dismissal or demotion as set forth in § 4-233 depending upon the circumstances of the violation. Any employee receiving any proposed disciplinary action, dismissal or demotion may appeal said action directly to the board of mayor and aldermen, which may affirm, reverse or modify (increase or decrease) the disciplinary action. (as added by Ord. #1245, Oct. 2009, and amended by Ord. #1341, Oct. 2012)

4-250. Use of cellular/mobile phones. (1) Purpose. The purpose of this section is to govern the use and application of City of Manchester-owned phones and associated services and devices.

(2) Authorization. Recommendation for the issuance of City of Manchester-owned mobile phones should be approved by the department head. The use of a City of Manchester-owned phone of any type is considered a privilege and may be revoked. Regular landline phones may be provided to employees as is appropriate for their position.

Both landlines and mobile phones will be assigned by need and not every employee will have a unique landline and/or mobile phone assigned to them. Each case for a phone will be reviewed individually; the location, the business requirements, safety issues and appropriateness will be taken into consideration when evaluating the need for a new phone.

(a) Business use. Any phone owned and issued by the City of Manchester shall have as its primary function, business related uses. When an employee is in travel status, he or she is encouraged to use their mobile phone, if service is available.

(b) Personal use. This policy acknowledges that from time to time, a City of Manchester-issued phone may be used for personal calls. As long as this use of the phone is incidental to its primary business use, reasonable personal calls are allowed.

If a situation occurs that warrants personal use of a City of Manchester-owned phone beyond an incidental nature, the individual shall reimburse the city, as appropriate. Should it be determined that an individual is abusing the privilege of using a City of Manchester-owned phone; the phone may be taken from the employee and/or the employee disciplined or discharged.

City employees are not allowed to use their personal phones during designated work hours unless specifically permitted by their department head. Personal calls during designated work hours may not be taken at any time when it may disrupt the employee's assigned task/work and/or may compromise the safety of the employee, other employees or the general public.

(c) Prohibited use. Phones issued by the City of Manchester shall not be used to harass or threaten any individual. Typically, city phones may not be used for personal long distance or fee services. However, in an emergency situation, the expense for any such use shall be reimbursed to the city as soon as possible. When practical, the employee must seek approval from their supervisor.

(d) Driving. The City of Manchester encourages the safe use of phones when operating any vehicle or piece of machinery. Drivers using cell phones may pull off the road into a safe area until the call is

terminated. If available, handsfree devices may be used to conduct calls while driving.

(e) Meetings. Any individual using a City of Manchester mobile phone shall use good judgment in how and where the phone is used. Phones taken into meetings shall be turned off or to vibrate. If a call if taken during a meeting, every effort should be made not to disrupt the meeting. Unless a call is specifically related to the topic of discussion, talking on the phone in a meeting is strongly discouraged.

(f) No right of privacy. All records of use of city-owned cellular/mobile phones are subject to the Tennessee Open Records Act, Tennessee Code Annotated, § 10-7-501, et. seq., subject to any exceptions applicable thereto by statute, rule or judicial decision.

(3) Phone records. Every individual City of Manchester-owned mobile phone user is responsible for checking the accuracy of the bill pertaining thereto before it is processed for payment. Discrepancies in billing data shall be resolved in a timely manner. Landline calls incurring fees shall be assigned to the appropriate departmental budget code.

If a city phone is used for personal long distance or fee services, the supervisor must be notified and the city reimbursed.

(4) Other. The nature of the technology required to support the wireless mobile telephone is rapidly evolving. Phones may have additional features such as cameras, text messaging, internet access, etc. The intent of this policy is to apply the principles enumerated herein to any such add-on or accessory feature.

(5) Recordings. Employees that use devices to record telephone conversations shall do so only in a manner consistent with the status of such applicable local, state and federal laws.

(6) Violation. Violation of this policy may result in disciplinary action as set forth in § 4-232 or dismissal or demotion as set forth in § 4-233 depending upon the circumstances of the violation. Any employee receiving any proposed disciplinary action, dismissal or demotion may appeal said action directly to the board of mayor and aldermen, which may affirm, reverse or modify (increase or decrease) the disciplinary action. (as added by Ord. #1244, Oct. 2009, and amended by Ord. #1443, Dec. 2014)