

TITLE 20

MISCELLANEOUS

CHAPTER

1. AUTOMATIC SPRINKLER SYSTEMS.
2. CEMETARY POLICY.
3. IDENTITY THEFT PREVENTION PROGRAM.
4. KNOX BOXES.

CHAPTER 1

AUTOMATIC SPRINKLER SYSTEMS

SECTION

- 20-101. New building construction.
- 20-102. Building additions and requirements of other codes.
- 20-103. Definitions.
- 20-104. Additional requirements of sprinkler systems.
- 20-105. Maintenance of system required.
- 20-106. Fire inspection.
- 20-107. Fee for industrial and commercial customers.
- 20-108. Enforcement.
- 20-109. Authority and purpose.
- 20-110. Severability.

20-101. New building construction. An approved automatic sprinkler system shall be installed in all areas of all new buildings according to the applicable code of NFPA 13, 13R, or 13D. For the purpose of this chapter, the term "new building" shall mean any building, as defined herein, for which a permit has been issued after the adoption of Ordinance No. 114-07, having an effective date of October 17, 2007; and shall additionally include the replacement of buildings that have sustained a total loss, as determined by the fire chief and building official, as a result of fire or acts of God; and replacement buildings on lots/parcels where an existing building has been demolished; and, renovated buildings, to the extent that such renovation, as determined by the fire chief and building official, represents a complete and total rehabilitation of the building to be renovated.

Exceptions:

- (1) Buildings, as defined herein, that existed, or for which a permit has been issued prior to the adoption of Ordinance No. 114-07 having an effective date of October 17, 2007.
- (2) Any detached accessory building containing no life hazards and not used for human occupancy as determined by the fire chief and building official.

(3) Manufactured homes which meet the definition and criteria in NFPA 501 and the standards of the U.S. Department of Housing and Urban Development's (HUD) federal advisory committee on manufactured housing, also known as the Manufactured Housing Consensus Committee (MHCC). (as added by Ord. #114-07, Oct. 2007, and replaced by Ord. #247-14, Nov. 2014)

20-102. Building additions and requirements of other codes. An approved automatic sprinkler system shall also be installed in any of the following circumstances:

(1) When an existing building is altered or renovated, an approved automatic sprinkler system must be installed in the altered or renovated portion of the building if the building has an existing approved automatic sprinkler system. When the square footage of an existing building that does not have an approved automatic sprinkler system is increased by one hundred percent (100%), then an approved automatic sprinkler system must be installed in the entire building.

(2) When any other applicable ordinance, code, regulation, rule or statute so requires, an approved automatic sprinkler system must be installed accordingly.

(3) When an automatic sprinkler system is installed in a building, it must comply with NFPA 13D. (as added by Ord. #114-07, Oct. 2007, and replaced by Ord. #247-14, Nov. 2014)

20-103. Definitions. (1) "An approved automatic sprinkler system" means a system installed in accordance with National Fire Protection Association Standards or a system approved by the state fire marshal's office.

(2) "Approved supervisory alarm system" means it must be connected to an UL listed and approved central station facility meeting the requirements of NFPA 72.

(3) "Building" means any structure (excluding any barn or stable used exclusively for agricultural purposes), regardless of occupancy, having a roof supported by columns or walls and intended for the shelter, housing, use or enclosure of persons, animals or property. For purposes of determining when an approved automatic sprinkler system is required by this chapter, portions of buildings separated from other portions by a fire wall shall not be considered separate buildings. (as added by Ord. #114-07, Oct. 2007, and replaced by Ord. #247-14, Nov. 2014)

20-104. Additional requirements of sprinkler systems. (1) Any multi-tenant building having more than one (1) sprinkler riser shall have the risers separately zoned and wired to a local energy alarm panel to provide zone identification upon activation. The energy alarm panel shall be located as near as possible to the main exit door. There shall also be a building map located at the energy alarm panel showing each zone of the building.

(2) Automatic sprinkler flow alarms shall be zoned to indicate a water flow and not a general fire alarm to the central station.

(3) Where building fire alarm facilities are provided, actuation of the extinguishing system shall also cause the building alarm to sound in accordance with NFPA 72.

(4) Any multi-tenant building that is required to be equipped with a fire department connection, such connection shall be located on the front street side of the facility. Special circumstances that would prevent this shall be reviewed and altered only by the fire chief or his designee on a case by case basis. All fire department connections shall be within one hundred feet (100') of a fire hydrant. Exception: Buildings below five thousand (5,000) square feet must be within four hundred feet (400'). Exception: High hazard buildings must have FDC within one hundred feet (100') of hydrant.

(5) An approved automatic sprinkler system in multi-tenant buildings shall include an evacuation alarm which will sound and be audible throughout the entire building when the sprinkler system is activated. An internal fire alarm system may be utilized to meet this requirement, provided it is interconnected to activation of the sprinkler system.

(6) Plans for an approved automatic sprinkler system shall be certified engineered plans and shall be subject to all applicable fees as set forth in the current city fee schedule, and any other costs incurred by the City of Pipeston for third party review. (as added by Ord. #114-07, Oct. 2007, and replaced by Ord. #247-14, Nov. 2014)

20-105. Maintenance of system required. Occupied or unoccupied buildings or portions thereof having a sprinkler system in place, whether or not such system is required by this chapter, shall maintain all sprinklers and standpipe systems and all component parts in workable condition at all times, and it shall be unlawful for any owner or occupant or agent of either to reduce the effectiveness of the protection those systems provide. This section does not prevent the owner or occupant of a building from temporarily reducing or discontinuing the protection when necessary in order to conduct testing, repairs, alterations or additions to the system, provided that the testing, repairs, alterations or additions are done in such a way to avoid the creation of a safety hazard, and provided that the fire department has been notified that the work will be done, informed of the time the system will be shut down and then notified when the system is put back on line. For buildings that are vacant and present no safety hazard, protection may be discontinued while building is in such condition. Protection must be resumed when building is occupied. (as added by Ord. #114-07, Oct. 2007, and replaced by Ord. #247-14, Nov. 2014)

20-106. Fire inspection. The fire chief for the respective fire district or his designee shall provide an initial inspection of the automatic fire suppression system or automatic sprinkler system for structures meeting the criteria of this

chapter. This inspection shall not guarantee proper installation of said system, but will insure that the system exists. This inspection shall also afford the property owner a safety inspection of the facility to provide proactive planning for fire prevention.

Further, all automatic sprinkler systems and appurtenances shall be installed, tested, inspected, and maintained in accordance with National Fire Protection Association (NFPA) Standards and the International Code Council (ICC). (as added by Ord. #114-07, Oct. 2007, and replaced by Ord. #247-14, Nov. 2014)

20-107. Fee for industrial and commercial customers. (1) Initial tap inspection fee. A one-time tap inspection fee of two hundred fifty dollars (\$250.00) shall be charged to all commercial and industrial customers when connecting a fire suppression system to the municipal water distribution system.

(2) Monthly connection fee for fire suppression system. Commercial and industrial customers whose fire suppression systems are separately connected to the municipal water distribution system shall be charged a monthly fee equal to \$0.005 per square foot of protected space, based on the building permit(s) issued to the structure. The maximum monthly fee will be capped at two hundred fifty dollars (\$250.00). This rate will apply whether or not the customer is required by its insurance company to install a fire water tank.

(3) Effective date. This section shall be in full force and effect after two (2) readings and enactment by the board of mayor and commissioners and as specified in section 6-20-215 of the Piperton City Charter. (as added by Ord. #242-14, Nov. 2014)

20-108. Enforcement. Any person, firm or corporation being the owner or having control or use of any building or premises who violates any of the provisions of this chapter, shall be guilty of a civil offense and shall be fined not in excess of fifty dollars (\$50.00) for each offense. Each day such violation is permitted to exist after notification shall constitute a separate offense.

When any violation of any provision of this chapter shall be found to exist, the fire chief for the respective fire district, or his designee, is hereby authorized and directed to institute any and all actions and proceedings either legal or equitable, that may be appropriate or necessary to enforce the provisions of this resolution in the name of the city, including but not limited to the issuance of a "stop work" order to aid in the enforcement of any of the provisions of this chapter. (as added by Ord. #114-07, Oct. 2007, renumbered by Ord. #242-14, Nov. 2014, and replaced by Ord. #247-14, Nov. 2014)

20-109. Authority and purpose. The ordinance comprising this chapter is adopted pursuant to all applicable laws of the State of Tennessee. (as added

by Ord. #114-07, Oct. 2007, renumbered by Ord. #242-14, Nov. 2014, and replaced by Ord. #247-14, Nov. 2014)

20-110. Severability. If any section, sentence, clause or phrase of this chapter should be held to be invalid or unconstitutional by a court of competent jurisdiction, such invalidity or unconstitutionality shall not affect the validity or constitutionality of any other section, sentence, clause, or phrase of this resolution. (as added by Ord. #114-07, Oct. 2007, renumbered by Ord. #242-14, Nov. 2014, and replaced by Ord. #247-14, Nov. 2014)

CHAPTER 2

CEMETERY POLICY

SECTION

20-201. Creation.

20-201. Creation. (1) The creation of private cemeteries shall be limited to those created in association with an active church on property owned by the applicable church;

(2) The designated cemetery shall be surveyed by a registered land surveyor and the property deed and plat map legally revised to truthfully and explicitly show the existence and location of the created cemetery;

(3) The designated cemetery shall be secured with an appropriate fence erected on its perimeter lines.

(4) All burial sites within the designated cemetery shall be clearly marked with an appropriate monument;

(5) The county health department shall approve proposed burial sites;

(6) All private cemeteries shall have all-weather access from a public road;

(7) The applicable church shall provide for the perpetual maintenance of the cemetery grounds;

(8) All graves or burial sites shall be set back at least thirty (30) feet from any lot line and/or street right-of-way;

(9) Screening located along the perimeter lines of the cemetery may be required to block such cemetery view from adjacent property;

(10) Sites for cemeteries shall not obstruct the development of any major road proposed on the City of Piperton Major Road Plan; and

(11) Private cemeteries shall adhere to all applicable requirements of Tennessee Code Annotated, title 46, cemeteries. (as added by Ord. #146-08, Oct. 2008)

CHAPTER 3

IDENTITY THEFT PREVENTION PROGRAM

SECTION

- 20-301. Purpose.
- 20-302. Definitions.
- 20-303. The program.
- 20-304. Administration of program.
- 20-305. Identification of relevant red flags.
- 20-306. Detection of red flags.
- 20-307. Responses.
- 20-308. Procedures established.
- 20-309. Updating the program.
- 20-310. Oversight of the program.
- 20-311. Oversight of service provider arrangements.
- 20-312. Duties regarding address discrepancies.

20-301. Purpose. The purpose of this chapter is to establish an identity theft prevention program (the "Program") for the City of Piperton that is designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or an existing covered account and to provide for continued administration of the Program in compliance with Part 681 of Title 16 of the Code of Federal Regulations implementing sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003. (as added by Ord. #149-08, Oct. 2008)

20-302. Definitions. (1) "Identify theft" means fraud committed or attempted using the identifying information of another person without authority.

(2) "Covered account" means:

(a) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions. Covered accounts include credit card accounts, mortgage loans, automobile loans, margin accounts, cell phone accounts, utility accounts, checking accounts and savings accounts; and

(b) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation or litigation risks.

(3) "Red flag" means a pattern, practice or specific activity that indicates the possible existence of identity theft.

(4) "Sensitive information" means and includes the following, whether kept in electronic or print format, as to any employee or customer:

(a) Credit card information, including card number, expiration date, cardholder name or address, or card security number;

(b) Tax identification numbers, including social security number and employer identification number;

(c) Payroll information, including paychecks, pay stubs and payroll records;

(d) Personal insurance information, including cafeteria plan check requests and associated paperwork;

(e) Medical information for employee or employee's covered family members, including doctor names and claims, insurance claims, prescription information and other related personal medical information;

(f) Other personal information, including birth date, address, telephone numbers, maiden name and customer number.

(5) "Suspicious document" means:

(a) A document provided for identification that appears to have been altered or forged;

(b) A document on which the photograph or physical description is not consistent with the appearance of the applicant or customer presenting the identification;

(c) A document on which other information is not consistent with information provided by the person opening a new covered account or the customer presenting the document;

(d) A document on which information is not consistent with readily accessible information on file with the city, such as a signature card, recent check or application for services; and

(e) An application that appears to have been altered or forged or that gives the appearance of having been destroyed and reassembled.
(as added by Ord. #149-08, Oct. 2008)

20-303. The program. The City of Piperton hereby establishes an identity theft prevention program to detect, prevent and mitigate identity theft. The program shall include reasonable policies and procedures to:

(1) Identify relevant red flags for covered accounts it offers or maintains and incorporate those red flags into the program;

(2) Detect red flags that have been incorporated into the program;

(3) Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and

(4) Ensure the program is updated periodically to reflect changes in risks to customers and to the safety and soundness of the creditor from identity theft.

The program shall, as appropriate, incorporate existing policies and procedures that control reasonably foreseeable risks. (as added by Ord. #149-08, Oct. 2008)

20-304. Administration of program. (1) The city manager shall be responsible for the development, implementation, oversight and continued administration of the program.

(2) The program shall train staff, as necessary, to effectively implement the program; and

(3) The program shall exercise appropriate and effective oversight of service provider arrangements. (as added by Ord. #149-08, Oct. 2008)

20-305. Identification of relevant red flags. (1) The program shall include identification of relevant red flags from the following categories, as appropriate:

(a) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;

(b) A fraud or active duty alert included with a consumer report;

(c) The presentation of suspicious documents;

(d) The presentation of suspicious personal identifying information;

(e) Consumer reports that indicate a pattern of activity inconsistent with the history and usual pattern of activity of an applicant or customer;

(f) The unusual use of, or other suspicious activity related to, a covered account;

(g) A notice of credit freeze from a consumer reporting agency in response to a request for a consumer report;

(h) A notice of address discrepancy from a consumer reporting agency as defined in Sec. 334.82(b) of FACTA; and

(i) Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.

(2) The program shall consider the following risk factors in identifying relevant red flags for covered accounts as appropriate:

(a) The types of covered accounts offered or maintained;

(b) The methods provided to open covered accounts;

(c) The methods provided to access covered accounts; and

(d) Its previous experience with identity theft.

(3) The program shall incorporate relevant red flags from sources such as:

(a) Incidents of identity theft previously experienced;

(b) Methods of identity theft that reflect changes in risk; and

(c) Applicable supervisory guidance. (as added by Ord. #149-08, Oct. 2008)

20-306. Detection of red flags. The program shall address the detection of red flags in connection with the opening of covered accounts and existing covered accounts, such as by:

- (1) Obtaining identifying information about, and verifying the identity of, a person opening a covered account; and
- (2) Authenticating customers, monitoring transactions, and verifying the validity of change of address requests in the case of existing covered accounts. (as added by Ord. #149-08, Oct. 2008)

20-307. Responses. The program shall provide for appropriate responses to detected red flags to prevent and mitigate identity theft. Each response shall be commensurate with the apparent degree of risk posed. Appropriate responses may include any one (1) or more of the following and such other activities as the city shall deem appropriate:

- (1) Monitor a covered account for evidence of identity theft;
- (2) Contact the customer;
- (3) Change any passwords, security codes or other security devices that permit access to a covered account;
- (4) Reopen a covered account with a new account number;
- (5) Not open a new covered account;
- (6) Close an existing covered account;
- (7) Notify law enforcement; and
- (8) Determine no response is warranted under the particular circumstances.

This section shall be read in conjunction with the Tennessee Public Records Act, Tennessee Code Annotated, § 10-7-501 et seq. and the city's open records policy. In the event a city employee is uncertain whether a certain item is "sensitive information" as defined in this chapter, that employee should contact his or her supervisor. If the city, in consultation with the city attorney, is unable to resolve a conflict between the policy and program established by this chapter and the Tennessee Public Records Act., the city shall contact the Tennessee Office of Public Records. (as added by Ord. #149-08, Oct. 2008)

20-308. Procedures established. (1) Each city employee to whom this policy is applicable shall comply with the following policies for protection and destruction of sensitive information in hard copy form:

- (a) File cabinets, desk drawers, overhead cabinets and all other storage spaces that contain documents with sensitive information shall be locked when not in use;

(b) Storage rooms that contain documents with sensitive information and record retention areas shall be locked at the end of each work day or at any time during the work day when not supervised.

(c) Desks, work stations, work areas, printers and fax machines shall be cleared of all documents containing sensitive information when not in use;

(d) Whiteboards, dry-erase boards, writing tablets, etc. in common shared work areas shall be erased, removed or shredded when not in use; and

(e) When documents containing sensitive information are to be discarded, they shall be placed inside a locked shred bin or immediately shredded, using a mechanical cross-cut or Department of Defense-approved shredding device. City records shall be destroyed only in accordance with the city's records retention policy.

(2) Each city employee to whom this policy is applicable shall comply with the following procedures regarding electronic distribution of information:

(a) Sensitive information may be transmitted internally using approved city e-mail. All sensitive information must be encrypted when stored in an electronic format.

(b) Any sensitive information sent externally must be encrypted and password protected, and only to approved recipients. A statement substantially the same as the following shall be put on each email:

"This message may contain confidential and/or proprietary information and is intended for the person/entity to whom it was originally addressed. Any use by others is strictly prohibited." (as added by Ord. #149-08, Oct. 2008)

20-309. Updating the program. The program shall be updated periodically to reflect changes in risks to customers or to the safety and soundness of the city from identity theft based on factors such as:

- (1) The experiences of the city with identity theft;
- (2) Changes in methods of identity theft;
- (3) Changes in methods to detect, prevent and mitigate identity theft;
- (4) Changes in the types of accounts that the city offers or maintains;
- (5) Changes in the business arrangements of the city, including but not limited to changes in billing and collection procedures for utility service and other city services, joint ventures with other governmental entities and service provider arrangements. (as added by Ord. #149-08, Oct. 2008)

20-310. Oversight of the program. (1) Oversight of the program shall include:

- (a) Assignment of specific responsibility for implementation of the program;
- (b) Review of reports prepared by staff regarding compliance;

(c) Training of city staff to recognize red flags and take appropriate action; and

(d) Approval of material changes to the program as necessary to address changing risks of identity theft.

(2) Reports shall be prepared as follows:

(a) Staff responsible for development, implementation and administration of the program shall report to the mayor and board of commissioners at least annually on compliance by the city with the program.

(b) The report shall address material matters related to the program and evaluate issues such as:

(i) The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts;

(ii) Service provider agreements;

(iii) Significant incidents involving identity theft and management's response; and

(iv) Recommendations for material changes to the program.

(3) Staff training shall be conducted at least annually for all employees, officials and service providers (as applicable) who do or in the course of their normal activities for the city may come into contact with accounts or personal information that may constitute a risk of identity theft. (as added by Ord. #149-08, Oct. 2008)

20-311. Oversight of service provider arrangements. The city shall take steps to ensure that the activity of a service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft whenever the organization engages a service provider to perform an activity in connection with one or more covered accounts. Specific requirements for prevention of identity theft shall be addressed in any contract with a service provider. (as added by Ord. #149-08, Oct. 2008)

20-312. Duties regarding address discrepancies. The city shall develop policies and procedures designed to enable it to form a reasonable belief that a credit report relates to the consumer for whom it was requested, if the city receives a notice of address discrepancy from a nationwide consumer reporting agency indicating the address given by the consumer differs from the address contained in the consumer report.

The city may reasonably confirm that an address is accurate by any of the following means:

(1) Verification of the address with the consumer;

(2) Review of the city's records;

- (3) Verification of the address through third-party sources; or
- (4) Other reasonable means.

If an accurate address is confirmed, the city shall furnish the consumer's address to the nationwide consumer reporting agency from which it received the notice of address discrepancy if:

- (1) The city establishes a continuing relationship with the consumer;
- and
- (2) The city regularly and in the ordinary course of business, furnishes information to the consumer reporting agency. (as added by Ord. #149-08, Oct. 2008)

CHAPTER 4

KNOX BOXES

SECTION

20-401. Knox boxes.

20-401. Knox boxes. (1) Knox box required for new commercial buildings. All new commercial buildings shall have installed a Knox box, of a UL type and size approved by the city fire official, in a location specified by the city fire official prior to the issuance of the permit of occupancy.

(2) Knox box required for existing commercial buildings with improvements. All existing commercial buildings constructing improvements that require planning commission approval shall have installed a Knox box, of a UL type and size approved by the city fire official, in a location specified by the city fire official prior to the issuance of the construction permit.

(3) Knox box contents. All Knox boxes shall contain labeled keys, easily identified in the field to provide access into the property and/or building, and to any locked areas within the said building as the city fire official may direct.

(4) Penalties. Any property or building owner failing to comply with, or in violation of the terms of this chapter after notice from the city fire official, shall be subject to a fine of fifty dollars and zero cents (\$50.00).

(5) Definitions. "Knox box" means a secure rapid entry system that is designed to be used by the fire department personnel in the event of an emergency to gain entry into a structure by using the enclosed owner provided key(s). This box is usually mounted on the exterior of the building in a location that is specified by the local fire official. All boxes shall be UL (Underwriters Laboratories) certified and approved by the City of Pipeperon Fire Official. (as added by Ord. #233-14, Feb. 2014)