

inside the mask without any air leaking out between the mask and the face of the wearer.

2. **Negative Pressure Test:** Close off the inlet openings of the cartridge with the palm of your hand. Inhale gently so that a vacuum occurs within the face piece. Hold your breath for 10 seconds. If the vacuum remains, and no inward leakage is detected, the respirator is properly fit.

SEC. 16-112 RESPIRATOR USERS

- A. Employees and non-employees who work in areas which may require the use of respirators which need a facial seal, will be clean shaven.
- B. Contractors who perform services for the Town that require the use of a respirator will be responsible for providing the necessary respiratory protective equipment and training for their people.

ARTICLE 17 ELECTRONIC COMMUNICATION POLICIES

The Town of Bucksport (“the Town”), in an age of growing technology and electronic communication, is implementing a policy to clearly define expectations and responsibilities that apply to all employees, contractors, part-time employees, volunteers and other individuals who are provided access to the e-mail system. Third parties will only be provided access to the e-mail system as necessary for their business purpose with the Town, and only if they abide by all applicable rules.

“**System**” means all telephones, computers, facsimile machines, voicemail, e-mail, and other electronic communication, copying or data storage systems or equipment leased, owned or in the possession of the Town, including, but not limited to, any computer, computer system, or any storage device or medium that the Town provides to an employee or that is physically or electronically connected to any other part of the System.

“**Electronic Communication**” means all electronic communications, data, software, files, and other information created, modified, located upon, received or transmitted by, or stored upon, and part of the System, including, but not limited to e-mail, voicemail, and internet usage.

All parts of the System are owned by the Town and/or are provided solely for use in the Town’s business activities. All Electronic Communications are the Town’s property. The Town has the right and the ability to monitor and review all Electronic Communications at any time without notice to its employees or any other party and for any purpose whatsoever. Under certain circumstances, e-mail messages have been found to be public record and may be subject to right-to-know laws, depending on their content.

While users may have a confidential password, users should be aware that this does not mean that the system is for personal confidential communication, nor does it suggest that e-mail is the property right of the user. The use of the e-mail system is for Town business. Passwords should be periodically changed to ensure security of the System. Users should not share passwords with anyone else, other than his or her supervisor or as applicable state and federal laws may require. A computer user who has been authorized to use a password-protected account may be subject to civil and criminal liability if the user discloses their password or otherwise makes the account available to others without express permission of the Town Manager.

Users may not utilize the System, or send, receive, create or store Electronic Communications upon the System, in a manner that is illegal, disruptive to others, or that interferes with the Town's business activities. All users are prohibited from utilizing any part of the System to harass others, or to download, obtain, display, store, receive or transmit: (a) any information that is sexually explicit, obscene, or of a sexual nature, that contain libelous or defamatory material, or that would not be permitted on any bulletin located on Town property; (b) any ethnic, racial or religious slurs, or anything that is, or may be construed as, disparagement of others based on race, color, national origin, ancestry, gender, sexual orientation, age, disability, religious or political beliefs, or any other basis prohibited by law; or (c) any communications that are derogatory of fellow users (except as may be required as part of the Town's business activities). The System may also not be used to solicit anyone for any commercial, religious, charitable, or political causes, or for outside organizations. Except as otherwise provided below, the System may not be used for any purpose that is not related to Town business.

E-mail is used to transmit and receive messages internally and externally on matters of business connected to the Town. The occasional use of e-mail with permissible content for personal matters is not prohibited, but is discouraged. Voicemail is used to leave messages for employees regarding matters of a business nature. Voicemail boxes will occasionally be emptied to free up System space. Internet usage is to be limited to matters of business connected to the Town. The occasional use of the Internet for otherwise permissible personal matters is not prohibited, but is discouraged. Any downloading of materials or loading of programs/software onto any part of the System without permission from the Town Manager is prohibited.

In addition, e-mail messages are intended to be temporary communications that are non-vital and may be discarded routinely. However, depending on the content of the e-mail message, it may be considered a more formal record and should be retained pursuant to the Town's record retention schedule. As such, these e-mail messages are similar to printed communication and should be written with the same care.

Users should also be aware that when they delete a message from their workstation mailbox it might not have been deleted from the System. The message may reside in the recipient's mailbox or forwarded to other recipients. Furthermore, the message may be stored on the computer's back-up system for an indefinite period. Again, note that e-mail

has been classified as a public document, i.e., available to the media, in at least one state. Keep this in mind when you create or store e-mail.

Users should store and/or delete e-mail messages as soon as possible after reading, as System disk space is limited. The Town Manager or his/her designee will automatically delete all messages after 60 days, unless archived by the user. Contact the Town Manager if you are unsure as to how to archive messages.

The workplace activities of System users reflect upon, and may create liability for, the Town. The person signing as a System user below, acknowledges receiving a copy of this policy and understands that the Town may take disciplinary action, up to and including termination of employment, against a user who violates the terms of this policy as those terms may be changed and/or supplemented from time to time by the Town.

The Town Manager will be responsible for overseeing the implementation of this policy and the accompanying rules, and for advising the Town Council of the need for any future amendments or revisions to the policy. The Town Manager may develop procedures governing the day-to-day management and operations of the Town's System as long as they are consistent with the Council's policy. The Town manager may delegate specific responsibilities to others as deemed appropriate.

Article 18 – Identity Theft Prevention Program

I. PROGRAM ADOPTION

The Town of Bucksport ("Town") developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's Red Flags Rule ("Rule"), which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. 16 C. F. R. § 681.2. This Program was developed with oversight and approval of the Management and Town Council of Bucksport. After consideration of the size and complexity of the Town's operations and account systems, and the nature and scope of the Town's activities, the Town Council determined that this Program was appropriate for the Town of Bucksport, and therefore approved this Program on April 30, 2009.

II. PROGRAM PURPOSE AND DEFINITIONS

A. Fulfilling requirements of the Red Flags Rule

Under the Red Flag Rule, every financial institution and creditor is required to establish an "Identity Theft Prevention Program" tailored to its size, complexity and the nature of its operation. Each Program must contain reasonable policies and procedures to:

1. Identify relevant Red Flags for new and existing covered accounts 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 or to the safety and soundness of the creditor from Identity Theft.

B. Red Flags Rule definitions used in this Program

The Red Flags Rule defines “Identity Theft” as “fraud committed using the identifying information of another person” and a “Red Flag” as a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

According to the Rule, a municipal utility is a creditor subject to the Rule requirements. The Rule defines creditors “to include finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies. Where non-profit and government entities defer payment for goods or services, they, too, are to be considered creditors.”

All the Town’s accounts that are individual service-type accounts held by customers of the Town whether residential, commercial or industrial are covered by the Rule. Under the Rule, a “covered account” is:

1. Any account the Town offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions; and
2. Any other account the Town offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the Town from Identity Theft.

“Identifying information” is defined under the Rule as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including: name, address, telephone number, social security number, date of birth, government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number, unique electronic identification number, computer’s Internet Protocol address, or routing code.

C. Risk Assessment

The Town of Bucksport has conducted an internal risk assessment to evaluate how at risk the current procedures are at allowing customers to create a fraudulent account and evaluate if current (existing) accounts are being manipulated. The risk assessment evaluated how new accounts were opened and the methods used to access the account information. Using this information the Town was able to identify Red Flags that were appropriate to prevent Identity Theft. The following is a list of assessment findings:

1. The Town is a creditor pursuant to 16 C. F. R. § 681.2 due to its provision or maintenance of covered accounts for which payment is made in arrears.

2. Covered accounts offered to customers for the provision of service include wastewater and ambulance accounts.
 - a. Covered accounts may be opened in-person, via telephone request (human interaction) or change in ownership based on recorded deed.
 - b. Covered accounts may be accessed in-person and via telephone (human interaction) or mail request.
3. The Town has identified the following methods in which Identity Theft could occur:
 - a. Opening of a new covered account
 - b. Restoring an existing covered account
 - c. Making a fraudulent change of address request on an existing covered account
 - d. Making fraudulent payments on a covered account
4. Based on the foregoing determinations, the Town considers that there is a low level of Identity Theft risk to covered accounts occurring in the following ways:
 - a. Use of another's identifying information to establish a new covered account; ***The Town does not request social security numbers from its customers;***
 - b. Use of a previous customer's identifying information by another person in an effort to have service restored;
 - c. Use of another's debit or credit card or other method of payment by a customer to pay such a customer's covered account or accounts; ***The Town does not accept debit or credit cards or electronic funds transfers (EFT's) for payment of covered accounts;***
 - d. The Town limits access to personal identifying information to those employees responsible for or otherwise involved in opening or restoring covered accounts or accepting payment for use of covered accounts. Information provided to such employees is entered directly into the Town's computer system(s) and is not otherwise recorded.
 - e. The Town has ***no*** previous experience with Identity Theft related to covered accounts.

III. IDENTIFICATION OF RED FLAGS

In order to identify relevant Red Flags, the Town considers the types of accounts that it offers and maintains, the methods it provides to open its accounts, the methods it provides to access its accounts, and its previous experiences with Identity Theft. The Town identifies the following Red Flags, in each of the listed categories:

A. Suspicious Documents

Red Flags

1. Identification document or card that appears to be forged, altered or inauthentic;

2. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
3. Other information provided by applicant that is not consistent with existing customer information; and
4. Application for service that appears to have been altered or forged.

B. Suspicious Personal Identifying Information

Red Flags

1. Identifying information presented that is inconsistent with other information the customer provides (example: inconsistent birth dates);
2. Identifying information presented that does not match other sources of information (for instance, a given address does not match an address on a credit report);
3. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
4. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
5. An address or phone number presented that is the same as that of another person;
6. A person fails to provide complete personal identifying information on an application when reminded to do so (however, by law social security numbers must not be required); and
7. Personal information provided is not consistent with the information on file for a customer.

C. Suspicious Account Activity or Unusual Use of a Covered Account

Red Flags

1. Change of address for an account followed by a request to change the account holder's name;
2. Payments stop on an otherwise consistently up-to-date account;
3. Account used in a way that is not consistent with prior use (example: very high activity);
4. Mail sent to the account holder is repeatedly returned as undeliverable;
5. Notice to the Town that a customer is not receiving mail sent by the Town;
6. Notice to the Town that an account has unauthorized activity;
7. Breach in the Town's computer system security; and
8. Unauthorized access to or use of customer account information.

D. Alerts from Others

Red Flag

1. Notice to the Town from a customer, Identity Theft victim, law enforcement or other person that it has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

IV. DETECTING RED FLAGS

A. New Accounts

In order to detect any of the Red Flags identified above associated with the opening of a **new account**, Town personnel will take the following steps to obtain and verify the identity of the person opening the account:

Detect

1. Require certain identifying information such as name, date of birth, residential or business address, principal place of business for an entity, driver's license or other identification;
2. Verify the customer's identity (for instance, review a driver's license or other identification card);
3. Review documentation showing the existence of a business entity; and
4. Independently contact the customer.

B. Existing Accounts

In order to detect any of the Red Flags identified above for an **existing account**, Town personnel will take the following steps to monitor transactions with an account:

Detect

1. Verify the identification of customers if they request information (in person, via telephone, facsimile, or email);
2. Verify the validity of requests to change billing addresses; and
3. Verify changes in banking information given for billing and payment purposes.

V. PREVENTING AND MITIGATING IDENTITY THEFT

In the event Town personnel detect any identified Red Flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

Prevent and Mitigate

1. Continue to monitor an account for evidence of Identity Theft;
2. Contact the customer;
3. Change any passwords or other security devices that permit access to accounts;
4. Not open a new account;
5. Close an existing account;

6. Reopen an account with a new number;
7. Notify the Program Administrator for determination of the appropriate step(s) to take;
8. Notify local law enforcement; or
9. Determine that no response is warranted under the particular circumstances.

Protect customer identifying information

In order to further prevent the likelihood of Identity Theft occurring with respect to Town accounts, the Town will take the following steps with respect to its internal operating procedures to protect customer identifying information:

Physical Security of Personal Identifying Information

1. Request only the last 4 digits of social security numbers (if any);
2. Require and keep only the kinds of customer information that are necessary for Town purposes;
3. Keep offices clear of papers containing customer information when employees leave their work areas;
4. Keep files containing personally identifiable information in locked file cabinets except when an employee is working on the file;
5. Ensure complete and secure destruction of paper documents and computer files containing personally identifiable information;
6. Access to offsite storage facilities is limited to employees with a legitimate business need;
7. Ensure any sensitive information shipped using outside carriers or contractor is secure; use a shipping service that allows tracking of the delivery of this information.

Security of Electronic Records

General Network Security

1. Prohibit sensitive consumer data from being stored on any computer with an Internet connection unless essential for conducting business;
2. Ensure secure storage of sensitive information on a computer network or portable storage devices used by Town employees;
3. Run most current version of anti-virus and anti-spyware programs on individual computers and servers daily;
4. Ensure that remote access to the computer network where sensitive information resides by service providers to troubleshoot and update software or provide training be allowed on an as-needed basis only. Employees will monitor each session continually until the session is discontinued and the connection is broken;
5. Ensure that its website is secure or provide clear notice that the website connection is not secure;
6. Ensure secure Internet connections are used when credit card information or other sensitive data is received or transmitted;
7. Ensure the use of a secure wireless network only;

8. Prohibit staff from loading software without prior authorization of the Program Administrator;

Password Management

1. Ensure access to sensitive information will be controlled using “strong” passwords. Employees will choose passwords with a mix of letters, numbers, and characters. User names and passwords will be different.
2. Prohibit the sharing or posting of passwords near workstations;

Laptop Security –

1. The use of laptops is restricted to those employees who need them to perform their jobs;
2. Laptop users will not store sensitive information their laptops unless essential for conducting business;

Firewalls

1. Have a “border” firewall where the computer network connects to the Internet; and
2. Monitor incoming and outgoing traffic for signs of a data breach.

VI PROGRAM UPDATES

This Program will be periodically reviewed and updated to reflect changes in risks to customers and the soundness of the Town from Identity Theft. At least annually, the Program Administrator will consider the Town's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, changes in types of accounts the Town maintains and changes in the Town's business arrangements with other entities. After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Administrator will update the Program and present the Town Council with his or her recommended changes and the Town Council will make a determination of whether to accept, modify or reject those changes to the Program.

VII. PROGRAM ADMINISTRATION.

A. Oversight

The Town Manager will be designated as the Program Administrator. The Program Administrator will be responsible for the Program administration, for ensuring appropriate training of Town staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program.

B. Staff Training and Reports

Town staff responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator in the detection of Red Flags,

and the responsive steps to be taken when a Red Flag is detected. (*The Town may include in its Program how often training is to occur. The Program may also require staff to provide reports to the Program Administrator on incidents of Identity Theft, the Town's compliance with the Program and the effectiveness of the Program.*)

C. Service Provider Arrangements

In the event the Town engages a service provider to perform an activity in connection with one or more accounts, the Town will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft.

1. Verify that service providers have such policies and procedures in place; and
2. Request that service providers review the Town's Program and report any Red Flags to the Program Administrator.

D. Specific Program Elements and Confidentiality

For the effectiveness of Identity Theft Prevention Programs, the Red Flag Rule envisions a degree of confidentiality regarding the Town's specific practices relating to Identity Theft detection, prevention and mitigation. Therefore, under this Program, knowledge of such specific practices is to be limited to the Program Administrator and those employees who need to know them for purposes of preventing Identity Theft. Because this Program is to be adopted by a public body and thus publicly available, it would be counterproductive to list these specific practices here. Therefore, only the Program's general Red Flag detection, implementation and prevention practices are listed in this document.

*Personnel Rules & Regulations was adopted on December 14, 1972. It was amended on May 13, 1976 (add two holidays)
Chapter 2, Administration, was adopted in conjunction with the Town Code on March 9, 1978 and amended on the following dates:
April 13, 1978 (sections 2-216, 2-225)
October 11, 1979 (sections 2-201, 2-212, 2-213)
May 14, 1981 (section 2-208 repealed & replaced) (sections 2-213, 2-216. section 2-202)
October 8, 1981 (section 2-302)
May 8, 1986 (section 2-202, 2-208. 2-212, 2-213, 2-223, 2-216, 2-302)
May 29, 1986 (workplace smoking policy)
July 10, 1986 (chemical hazard communication policy)
March 12, 1987(section 2-226 alcohol & drug use policy, section 2-222)
December 10, 1987 (employee safety policies)
October 12, 1989 (sections 2-225, 2-230, 2-301)
February 14, 1991 (section 2-225, 2-500 work place smoking policy)
March 12, 1992 (sexual harassment policy)*

June 11, 1992 (sections 2-409, 2-411, 2-414A, 2-416, 2-416A, 2-416B)
December 10, 1992 (ADA grievance procedures) (blood-born pathogen exposure control plan)
February 25, 1993 (workplace smoking policy)
April 8, 1993 (workplace smoking policy)
December 14, 1995 (alcohol & drug policy)
July 10, 1997 (sections 10-101, 10-201, 10-301, 10-401, 10-501, 10-601, 10-701, 10-801, 11-101, 11-201) (article 11 video display)
December 11, 1997 (article 2 repeal & replace) (sections 2-419, 2-420, 2-421, 2-422)
January 29, 1998 (article 13)
January 14, 1999 (section 2-416A, 2-416B, 2-420, 2-422, article 6 R&R, article 14, article 15, article 16)
January 25, 2001 (section 2-225)
September 25, 2003 (sections 2-213, 2-225)
March 11, 2004 (article 17)
September 30, 2004 (section 2-503)
December 13, 2007 (Replace Article 2, delete content of Article 3, 5 & 10)
July 9, 2009 (Article 18 added)
July 29, 2010 (Section 1.7)
March 10, 2011 (Article 2 Section 1.13.1.b, Section 2.3.2, Section 2.4, Section 2.4.3, Section 2.4.4, Section 2.4.5, Section 2.15.2. Article 4 Section 2-407, Section 13-113.)
September 29, 2011 (Sections 1.7 & 2.17)
November 10, 2011 (Article 17)

Town Clerk note: *A scrivener's error in Article 2 was corrected. The use of section number 1.16 was inadvertently omitted in the ordinance approved on December 13, 2007. On January 12, 2008, it was replaced and sections 1.17 through 1.32 were renumbered. The table of contents was also renumbered.*