Town of Atlantic Beach

October 27, 2008

TO: **Mayor and Council**

FROM: **Sabrina Simpson, Admin. Services**
Kelly Cyrus, Town Clerk

SUBJECT: **RESOLUTION 08-10-01;**
Security of Sensitive Information and Breach Response Plan

Attached is proposed Resolution 08-10-01. The proposed resolution is the Security of Sensitive Information and Breach Response Plan for the Town of Atlantic Beach, North Carolina as mandated by the Federal Fair and Accurate Credit Transactions Act of 2003; Identity Protection Act of 2005; Federal Trade Commission's Red Flag Rule 16 C.F.R. section 681.2; North Carolina General Statues (N.C.G.S.) 75-60 of the Identity Theft Protection Act; N.C.G.S. 14-113.20 Identity Theft and N.C.G.S. 132-1.10 of the Public Records Act.

This proposed plan has been created to protect and respond to the potential unlawful use of its "customers" (i.e. utility account customers, employees, vendors) sensitive information.

Council Action Requested: **To approve Resolution 08-10-01.**

TOWN OF ATLANTIC BEACH
NORTH CAROLINA
RESOLUTION ADOPTING
Security of Sensitive Information and Breach Response Plan

WHEREAS, the Town of Atlantic Beach, North Carolina in accordance with the mandates of the Federal Fair and Accurate Credit Transactions Act of 2003, the Identity Protection Act of 2005, the Federal Trade Commission's Red Flag Rule 16 C.F.R. section 681.2, North Carolina General Statutes (N.C.G.S) 75-60 of the Identity Theft Protection Act, N.C.G.S 14-113.20 Identity Theft, and N.C.G.S 132-1.10 of the Public Records Act (together, the "Act") has created a plan to protect and to respond to the potential unlawful use of the sensitive information of its customers (hereinafter "Plan"); and

WHEREAS, the plan was developed after meetings and discussions with Town employees and relevant service organizations utilized by the Town, with the oversight and approval of the Town Manger who shall be the Program Administrator for the Plan; and

WHEREAS, the plan takes into consideration the size and complexity of the Town's water, sewer, and other service departments' operations and account systems, and the nature and scope of these department's activities; and

WHEREAS, the Town Manager has recommended the adoption of the Plan by the Town Council; and

WHEREAS, the Town Council has reviewed the Plan and has determined the Plan to be appropriate for the Town of Atlantic Beach;

NOW THEREFORE, the Town Council of the Town of Atlantic Beach does hereby resolve and adopt the Plan as hereinafter presented:

Town of Atlantic Beach, North Carolina
Security of Sensitive Information and Breach Response Plan

SECTION 1. Purpose

In accordance with the Federal Fair and Accurate Credit Transactions Act of 2003, the Identity Protection Act of 2005, the Federal Trade Commission's Red Flag Rule 16 C.F.R. section 681.2, North Carolina General Statutes (N.C.G.S) 75-60 of the Identity Theft Protection Act, N.C.G.S 14-113.20 Identity Theft, and N.C.G.S 132-1.10 of the Public Records Act (together, the "Act"), the Town of Atlantic Beach is required to safeguard certain information of customers, vendors, employees, and other individuals who provide information to the Town that is covered by the Act ("Covered Accounts'). The purpose of this policy is to detect, prevent and mitigate identity theft and to communicate to employees and third parties their responsibility for protecting sensitive and confidential information pursuant to the Act, including a response plan in the event that there is a breach or attempted breach of information subject to the Act.

SECTION 2. Definitions

2.1 **Covered Account** – continuing relationship established by a person with the Town to obtain services for personal, family, household, or business purposes that involves or is designed to permit multiple payment or transactions, such as utility accounts and any other account that 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, including financial, operational, compliance, reputation or litigation risks.

2.2 **Confidential information** – Under State statute (N.C.G.S 132-1), the Town also has an obligation to secure and limit access to other information involving customers and employees. The following are identified as confidential information, although this is not a complete listing:

1. Communication with legal counsel
2. State and local tax information that contain information about a taxpayer's income or receipts except as provided in G.S. 153A-148.1 and G.S. 160A-208.1.
3. Public enterprise billing information (utility customer data)
4. Records of criminal investigations conducted by public law enforcement agencies
5. Names, addresses, telephone numbers, or email addresses that are contained in the 911 database, emergency notification system, or reverse 911 system.
6. Emergency response plans
7. Economic development incentives

2.3 **Customer** – person or business having a covered account with the Town.

2.4 **Identity Theft** – fraud committed or attempted using the identifying information of another person without authority.

2.5 **Notice of Address Discrepancy** – a notice sent to a user by a consumer reporting agency pursuant to 15 U.S.C. 1681c(h)(1) of the Federal Code that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the agency's file for the customer.]

2.6 **Program Manager** – Town Manager or his/her designee.

2.7 **Red Flag** – a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

2.8 **Security Breach** – A breach is considered to have taken place if any sensitive or confidential information is suspected to have been stolen, viewed, copied, or otherwise compromised by an unauthorized individual or if it is suspected that information has been lost and could be accessed by unauthorized individual(s). A breach of information can occur physically or virtually via technology. Access and use of sensitive or confidential information by an employee or agent of the Town for a legitimate purpose is not a security breach, provided that the sensitive or confidential information is not used for a purpose other than a lawful purpose and is not subject to further unauthorized disclosure.

2.9 **Sensitive Information** – Information that is identifying information according to the Act and through contractual obligations related to merchant services (credit card acceptance). The following are specifically identified as sensitive information:

1. Social security and employer taxpayer identification numbers
2. National and international identification
3. Drivers license, State identification card, or passport numbers
4. Credit card and debit card numbers
5. Savings and checking account numbers
6. Personal Identification (PIN) Code
7. Passwords
8. Electronic identification numbers, electronic mail names or addresses, internet account numbers, internet identification names, computer internet protocol address, or routing codes

9. Customer credit information (credit history, pay arrangements, and financial transactions)

10. Parent's legal surname prior to marriage

11. Other Identifying Information - Any other names, numbers or information that can identify a specific person or can be used to access a person's financial resources, including name, address, telephone number, date of birth, alien registration number, employer or taxpayer identification number

12. Digital signatures

13. Biometric data

14. Fingerprints

15. Customer's address

16. A persons first name or first initial and last name in combination with identifying information

SECTION 3. Responsibilities of Departments

3.1 Each department will develop and maintain a standard procedure to provide staff with specific guidance on the protection of sensitive and confidential information applicable to the department. Departmental procedures will supplement, but not supersede this policy or applicable laws.

3.2 Each department will ensure that service providers who are in contact with sensitive or confidential information are aware of security requirements, as well as the need for confidentiality, through proper contractual agreements and arrangements.

3.3 Department heads are responsible for determining which employees are authorized to access and handle sensitive and confidential information and the department head must ensure that the authorized employees are trained to handle such information in accordance with this policy.

3.4 All employees who manage and work with sensitive and confidential information are required to read and sign the Sensitive Information User Agreement which will be maintained in the employees personnel file.

3.5 All third party contractors who may have access to sensitive and confidential information are required to read and sign the Sensitive Information Service Agreement which will be maintained with the contract.

3.6 Initial Detection:

1. New Accounts:

   a. 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;

   b. Verify the customer's identity (for instance, review a driver's license or other identification card);

   c. Compare the information in consumer reports received by the department with information provided by the customer, information that the Town has in its own records, and information obtained from third parties;

   d. Review documentation showing the existence of a business entity; and

   e. Independently contact the customer.

2. Existing Accounts:

   a. Verify the identification of customers if they request information (in person, via telephone, via facsimile, via email);

   b. Verify the validity of requests to change billing addresses;

   c. Verify changes in banking information given for billing and payment purposes; and

SECTION 4. Managing, maintaining, and storing sensitive and confidential information

4.1 Employees who have access to sensitive and confidential information are required to create, handle, maintain, and dispose of such information with prudent care in order to ensure proper security. Access to sensitive and confidential information will be limited and only provided in order for authorized employees and contractual third parties to perform essential tasks for Town business.

4.2 The following procedures should be followed while creating, handling, maintaining, storing, and disposing of sensitive and confidential information.

1. Enter information directly to a final destination (i.e. computer system) and refrain from documenting the information in other areas.

2. If sensitive and confidential information is written on paper for reference, shred immediately upon recording the information in the final destination.

3. Electronic payment data should be handled by authorized personnel and only the last 4 digits of the customer's credit or debit account number should be visible on reports.

4. Sensitive and confidential information should not be included on e-mails.

5. Sensitive and confidential information should not be included on printed reports except as needed for the performance of essential tasks.

6. Maintain documents that contain sensitive or confidential information in a secured room and limit access to the area.

7. If possible, utilize encryption to secure information in the database or storage system.

8. Do not leave a computer unattended if sensitive or confidential information could be accessed by unauthorized individuals. While away from the computer, log off or lock the workstation.

9. Do not store files with sensitive or confidential information on laptops or on flash drives unless the information and the device can be secured are not accessible to unauthorized individuals.

10. Take reasonable measures when destroying sensitive or confidential data that will prohibit the information from being read or reconstructed. Documents with sensitive or confidential data should be shredded by the individual who has authorized access to the data or by another employee while in the presence of the authorized employee. The Town may enter into a written contract with a third party in the business of record destruction to destroy sensitive and confidential information in a manner consistent with this policy.

4.3 In order to protect sensitive and confidential information, the Town will only release sensitive information to the account holder or individual(s) who own the information upon confirmation of personal identifying information or a valid picture ID. The confirmed account holder or individual may authorize the release of sensitive information to a third party. Other than public enterprise billing information, (which shall be treated as sensitive information for release) confidential information will be released only in accordance with state statute. The only exception will be the release of specified information pursuant to a court order, warrant, subpoena or other requirement by law.

SECTION 5. Identify Theft Risk (Red Flags)

5.1 The Town has a responsibility to define high risk areas for identity theft and identify potential threats for identity theft known under the Act as red flags. The red flags are indicators that sensitive or confidential information is being fraudulently used or is attempting to be so used. This policy in combination with department specific guidelines should help to detect a potential for identify theft and unauthorized use of information.

5.2 The following are red flags that have been identified as indicators that sensitive information is being used fraudulently. Red flags are most commonly associated with activity on customer accounts (utilities, taxes, activity registrations, vendors). Other red flags may exist that are unique to a department and should be included in departmental guidelines.

1. The customer or individual provides notice that he, she, or it is a victim of identify theft.

2. A consumer reporting agency or service provider has provided an alert, notification, or other warning including without limitation, a report of fraud accompanying a credit report, notice or report of a credit freeze on a customer or applicant; notice or report of an active duty alert for an applicant, and indication of activity that is inconsistent with a customer's usual pattern or activity.

3. Unusual number of recent and significant inquiries.

4. Unusual or significant change in recently established credit or financial relationships such as a change in address followed by a request to change the account holder's name, payment stops in an otherwise consistently up-to-date account, unusual change in activity, mail sent is returned undeliverable, notice of unauthorized activity, and notice that customer is not receiving mail.

5. Conflicting names on identification and other documentation.

6. Any documents provided appear to have been altered or forged or are otherwise suspicious.

7, Picture identification is not consistent with the appearance of the individual presenting the identification or the physical description on the identification does not match.

8. Shortly after establishing an account, there is a request to change a mailing address or to add authorized users to the account.

9. Personal identifying information provided is not consistent with other external information sources:

a. Social security number does not match or is listed on the Social Security Administration's death master file

b. Address does not match or is fictitious, a mail drop, or prison

c. The phone number is invalid or associated with a pager or answering service

d. Authenticating information (i.e. PIN, password) provided is incorrect

e. Name on credit card or check does not match name on account or names associated with the account

f. Birth date inconsistency

g. Information presented is the same as given by another customer

h. Information presented is the same as shown on other applications that were fraudulent

i. Information presented is inconsistent with other records of the Town

10. Notice from an identity theft victim, law enforcement officer or other person that an account has been fraudulently opened or maintained by a person engaged in identity theft.

5.3 The Town has a responsibility to define high risk areas for identity theft and identify potential threats for identity theft. Upon identification of a red flag indicating a potential risk of identify theft, staff should notify his or her immediate supervisor in person or by telephone to determine the validity of the red flag. Once an identify theft risk is confirmed, staff should respond in accordance with the breach response plan (Section 6).

SECTION 6. Sensitive and Confidential Information Breach Response Plan

6.1 Step 1. Confirm that a breach of sensitive or confidential information has occurred or has been attempted.

1. *Physical Breach* - The following are indications that there has been unauthorized access to sensitive or confidential information via a physical breach. Other activities may occur that are also physical breaches that are not included in the listing.

a. Evidence of lock tampering on file cabinets or office doors

b. Evidence of unauthorized entry in an area where sensitive or confidential information is stored

c. Missing files or documents that do or may contain sensitive or confidential information

2. *Technology Breach* - The following are indications that there has been or has been attempted unauthorized access to sensitive or confidential information via a technology breach. Other activities may occur that are also technological breaches that are not included in the listing.

a. Unknown or unauthorized name in the computer logon window

b. Disconnected computer cables or power cables

c. Missing computer equipment (desktop, laptop)

d. Evidence that electronic files have been accessed by unknown or unauthorized individuals or are missing

e. Devices or media attached to the computer that are not known or authorized

f. Unusual programs running, icons, or windows that appear that are not known and are not part of the normal work process

g. Any other suspicious activity which indicates an attempt to use technology without approval

6.2 Step 2. Notify the appropriate internal and external contacts.

1. *Internal notification* – Any Town employee who becomes aware of a suspected or actual security breach must notify his or her immediate supervisor. The immediate supervisor will notify department management which is responsible for further investigation and notification. If the breach involves electronic equipment, the Information Systems Manager should be notified by telephone or in person.

2. *External notification* – Unless it is determined by departmental management that no response is warranted under the particular circumstances, the Town will notify affected individuals of actual or suspected security breaches. Each confirmed or suspected breach will be reviewed by the city manager's office, the department where the breach occurred, law enforcement, and Information Systems Manager to determine the appropriate action that will include the following:

a. Notifying the affected individuals without unreasonable delay providing information in general terms about the incident, the type of sensitive information that was subject to the unauthorized access, the actions that the Town will take to protect the information from further access, a telephone number that the person may call for further information and assistance, and advice that directs the person to remain vigilant by reviewing account statements and monitoring credit reports.

b. Notifying law enforcement.

c. Providing affected individuals with information about how to alert credit agencies to potential fraud and identity theft.

d. Notice to affected individuals may be provided by one or more of the following methods:

   i. Written notice

   ii. Electronic notice for those individuals for whom the Town has a valid email address and who have agreed to receive communications electronically

   iii. Telephonic notice provided the contact is made directly with the affected persons and appropriately documented by the Town.

e. A substitute notice may be given if the cost of providing the notice exceeds $250,000, the number of affected persons is greater than 500,000, or the Town does not have the necessary contact information to notify the individual in any of the aforementioned manners. A substitute notice will include posting a notice on the Town's website and notifying major statewide media.

f. If a security breach involves more than 1,000 persons, the Town will provide written notice of the timing, distribution, and content of the notice to the Consumer Protection Division of the North Carolina Attorney General's Office, as well as to all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S. C. 1681a(p).

g. Notice may be delayed if law enforcement informs the Town that disclosure of the breach would impede a criminal investigation or jeopardize national security. Such request by law enforcement must be documented in writing.

6.3 Step 3. Implement Plan

The Town Manager will designate a security breach response team to investigate and handle the breach until such time as the threat has ended and affected individuals and agencies are notified.

Technology Breach Response – The Information Systems Manager is responsible for the following response upon being notified of a technology security breach or an attempted security breach by the Town Manager.

a. The Information Systems Manager will notify computer users that a technology breach has occurred or has been attempted and the breach response plan is being implemented

b. The Information Systems Manager will secure the computer infrastructure as deemed appropriate which may include but is not limited to disconnecting network connections to outside locations, disconnecting servers or any other device on the network until the breach is isolated, changing passwords and/or security codes, closing accounts, and reopening accounts with new account numbers.

c. Information services will preserve evidence that may be needed by law enforcement for investigative purposes

6.4 At least annually, the Town will review all incidents of potential or actual security breaches and report findings and recommendations to the Town Council. This Plan will be periodically reviewed and updated to reflect changes in risks to customers and the soundness of the Plan. As part of it review, the Town will perform a risk assessment to include evaluation of how the Town opens new accounts, provides access to its accounts, and its previous experience with identity theft.

SECTION 7. Program Administration.

7.1 Oversight - the Program Administrator will be responsible for the Plan administration, for ensuring appropriate training of staff on the Plan, 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.

7.2 Staff Training and Reports - staff personnel responsible for implementing the Plan 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.

7.3 Specific Program Elements and Confidentiality - For the effectiveness of this Plan, a degree of confidentiality regarding the Utility's specific practices relating to identity theft detection, prevention and mitigation is required. Therefore, under this Program, knowledge of such specific practices under this Plan are to be limited to the Program Administrator and those employees who need to know them for purposes of preventing identity theft. Because this Plan is to be adopted by a public body and thus publicly available, it would be counterproductive to list any further specific practices within this document. Therefore, only the Program's general red flag detection, implementation and prevention practices are listed.

The Town shall begin implementation of this Plan immediately upon its passage.

SENSITIVE INFORMATION USER AGREEMENT

I have read the Security of Sensitive and Confidential Information and Breach Response Plan policy for the Town of Atlantic Beach, North Carolina and understand how to properly manage, maintain, store, and dispose of sensitive and confidential information at the Town of Atlantic Beach, North Carolina. I will abide by the policy and will handle sensitive and confidential information with prudent care in order to ensure proper security of the information.

In the event of a suspected or actual breach of sensitive or confidential information, I will notify my immediate supervisor without delay and follow the breach response plan.

I understand that negligent handling or inappropriate use of the Town's sensitive and confidential information will be subject to disciplinary action up to and including dismissal and may be criminally and civilly prosecuted as allowed by law.

I have read, understand, and agree to the conditions above.

Printed Name of Employee: _____

Department: _____

Signature of Employee: _____

Date Signed: _____

SENSITIVE INFORMATION SERVICE AGREEMENT

I, _____, an authorized representative of _____ ("Company"), hereby acknowledge that I have read and will adhere to the requirements listed below as they apply to the services procured by the Town of Atlantic Beach, North Carolina ("Town").

1. The appointed representative(s) of the Company have read the Town of Atlantic Beach, North Carolina administrative policy "Security of Sensitive and Confidential Information and Breach Response Plan."

2. The Company accepts responsibility for the security of sensitive or confidential information in their possession.

3. Data can be used only to complete the service as described by the Town for which the Company is engaged to perform.

4. If the Company is providing service that is related to a key function of the Town, the Company must assure business continuity in the event of a major disruption, disaster, or failure as provided for by contract.

5. If a security intrusion or attempted intrusion has been detected, the Company will notify the Town immediately. If the Company has placed sensitive or confidential data on its system and the system has been breached, the Company will allow their system to be thoroughly reviewed at the Company's expense. This review may be conducted by the Town or an appointed representative. In the event the intrusion is related to credit card numbers, the review may be conducted by a Payment Card Industry representative who will validate compliance with Payment Card Industry Security Standards for protecting cardholder data.

Name of Company: _____

Address: _____

_____

Name of Representative: _____

Title: _____

Signature: _____

Date: _____

Adopted on motion of council Member BRILEY, seconded by Council Member PALMA on a vote of 4 in favor and 0 against.

This the 27th day of October, 2008.

TOWN OF ATLANTIC BEACH

A. B. Cooper, III – Mayor

ATTEST:

Kelly L. Cyrus – Town Clerk