|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Description: TOCH SEAL M | **Town of Chapel Hill, NC**  **Technology and Data Security Policy** | **Policy Number:**  **TS-01**  **Issue Date:**  **January 1, 2018** | 1. [**POLICY**](#Policy) 2. [**PURPOSE**](#Purpose) 3. **[PROCEDURE](#Procedures)** 4. **[FORMS/INSTRUCTIONS](#forms)** 5. **[ADDITIONAL CONTACTS](#AdditionalContacts)** 6. **[DEFINITIONS](#Definitions)** 7. **[RESPONSIBILITIES](#Responsibilities)** 8. **[APPENDICES](#FAQ)** 9. **[FAQ](#Scope)** 10. [**SCOPE**](#Scope) 11. **[RELATED INFORMATION](#RelatedInformation)** 12. [**POLICY HISTORY**](#PolicyHistory) | **Approved By:**    **Roger L. Stancil,  Town Manager** |
| Technology and Data Security Policy | | | |

|  |  |  |
| --- | --- | --- |
| 1. POLICY | The Town will establish rules and procedures to securely maintain sensitive information and to implement a response plan in the event of a breach in accordance with all applicable federal or state regulations and the Town values of Professionalism and Safety. |  |
| 1. PURPOSE   III. PROCEDURE | As an employer and business and community partner in Chapel Hill, the Town collects, maintains and stores sensitive and personal identifying information as a regular course of business. The Town recognizes that the safety of this data is paramount. Therefore, this policy and corresponding procedures are designed to protect this sensitive data and provide an adequate response in case of a breach.  H:\Department\Policy Manual\Template\RESPECT- safety.png  H:\Department\Policy Manual\Template\RESPECT-professionalism.png  The Town’s Chief Information Officer is authorized to issue procedures consistent with this policy. |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Description: TOCH SEAL M | **Town of Chapel Hill, NC**  **Technology and Data Security Policy** | **Policy Number:**  **TS-01**  **Issue Date:**  **January 1, 2018** | 1. **[POLICY](#Policy)** 2. **[PURPOSE](#Purpose)** 3. **[PROCEDURE](#Appendices)** 4. **[FORMS/INSTRUCTIONS](#FormsInstructions)** 5. **[ADDITIONAL CONTACTS](#AdditionalContacts)** 6. **[DEFINITIONS](#Definitions)** 7. **[RESPONSIBILITIES](#Responsibilities)** 8. **[APPENDICES](#Appendices)** 9. **[FAQ](#FAQ)** 10. **[SCOPE](#Scope)** 11. **[RELATED INFORMATION](#RelatedInformation)** 12. [**POLICY HISTORY**](#PolicyHistory) | **Approved By:**    **Scott Clark,**  **Chief Information Officer** |

**III.** Technology and Data Security Procedures

**These procedures are issued by the Chief Information Officer, to implement the Technology and Data Security Policy, issued by the Chapel Hill Town Manager. These procedures may be periodically updated.**

The Town maintains additional procedures to protect the security and proper maintenance of the Town’s technology infrastructure.

|  |  |  |
| --- | --- | --- |
| **Name of associated procedure, guideline, or manual** | **Description** | **Status** |
| Appropriate Use of Technology Policy | Provides guidance to Town Staff regarding equipment and software use | Approved January 1, 2018 |
| Data Security Breach Response Plan | Outlines responsibilities and actions in event of a data breach | Approved on January 1, 2018. Not posted for security reasons, Copy available through TS |
| Data Security Red Flags Checklist | Supports Breach Response Plan | Approved on January 1, 2018. Not posted for security reasons, Copy available through TS |
| Security Camera Policy | Governs use of security cameras on Town property | Approved January 1, 2018 |
| Incident Response Policy |  | Approved on January 1, 2018. Not posted for security reasons, Copy available through TS |
|  | ***Intentionally Left Blank for Future Use*** |  |

Technology and Data security expectations exist at multiple levels: External Expectations, Supervisor Expectations, Employee Expectations, and Technology Staff expectations. All employees are expected to consider whether their use of technology is in compliance with best practices for protecting technology and data and to seek clarification or guidance in uncertain circumstances.

This procedure provides instructions on:

1. Securing Sensitive Information - [Breach Prevention](#Breach_Prevention)
2. [Response in the event of a breach](#Response_to_breach)
3. [Technology Incident Response](#TechnologyIncidentResponse)
4. [Identity Theft Prevention](#Identity_theft_prevention)

Contractors and vendors who have direct access to computer systems and networks that contain Criminal Justice Information (CJI) shall be required to verify identification via a state of residency and a  national fingerprint-based records check.

(FBI CJIS Security Policy v5.6, section 5.12.1.2 “*Personnel Screening for Contractors and Vendors*”)

1. **Breach Prevention: How to Appropriately Manage, Maintain and Store Sensitive Information** 
   1. Managers will control access to sensitive information by employees as described in the [Checklist for Managers and Employees for Protecting Sensitive Information](#protectingsensitiveinfochecklist).
   2. Employees will securely maintain sensitive information as described in the [Checklist for Managers and Employees for Protecting Sensitive Information](#protectingsensitiveinfochecklist).
   3. Records will be destroyed according to Town policy and procedure and applicable NC Records Retention Laws.
   4. Technology Solutions will maintain automated tools designed to prevent, detect and contain data breaches.
   5. Business Management (BMD) and Technology Solutions (TS) staff will conduct regular system reviews related to access, storage and destruction of sensitive information. This review may be included within the annual internal control reviews as a part of the external audit. They will also review all policies and procedures related to the security of sensitive information annually. Reviews may happen more frequently if major changes occur in operations that affect the handling of sensitive information. Changes will be made to ensure continued security of the sensitive information.
   6. The Director of BMD and the CIO will also review the Town’s incident response plan annually.
   7. Any significant system procurements and changes (technological or manual) relating to sensitive information management will be reviewed by BMD and TS and must be approved in advance.
   8. Individuals should report any suspected security weaknesses, but should not attempt to prove or test the weakness.
   9. Criminal and Credit Background Checks:The Town will conduct background checks on personnel where required by policy, contract, state or federal laws or by prudent financial management.
      1. Communication of Procedure to Users:All employees who manage, work with or are exposed to sensitive information are required to read and sign this standard procedure. Any changes or clarifications to this standard procedure will be communicated to the affected employees in a timely manner with proper documentation. This standard procedure as signed by the employee becomes a part of the employee’s permanent personnel file.
2. Annual Training: The following employees are required to participate in annual training regarding the security of sensitive information:
   1. Users and handlers of sensitive information
   2. Department Directors
   3. Division Managers
   4. Facility Managers
   5. All Town Manager’s office employees
   6. All Public Information office employees
   7. All Business Management employees
   8. All Technology Solutions employees
3. Individual departments may develop a detailed set of guidelines that supplement but do not conflict with or supersede this procedure or Town Policy. These guidelines may include specific examples that relate to the department.
4. Communicate to employees and third-parties their responsibility for protecting sensitive information pursuant to governmental laws and regulations and as is required by current merchant services contracts, various legislation (including the “Identity Theft Protection Act of 2005”), data security standards and prudent financial management as these laws may periodically be updated. If it is necessary for a third party to handle and/or manage sensitive information, the Town will require by written contract that the third party adhere to this standard procedure, using the guidance in [Checklist for Third-Party Contracts When the Scope of Work Includes Sensitive Information](#Checklistforthirdpartycontracts).

1. **Response in Case of a Breach**
   1. The Federal Trade Commission has developed regulations pertaining to the identification of signs (“red flags”) that identity theft has occurred or that fraudulent identification is being used for the purposes of conducting Town business or receiving Town services.
   2. Employees should be familiar with the [Breach Identification checklist](#BreachIdentificationChecklist) and report any suspected breaches immediately to their supervisor and Technology Solutions.
   3. In case of a breach, the [Security Breach Response Plan](#RelatedInformation) shall be implemented.
2. **Technology Incident Response**

Technology Solutions staff will use the [Technology Incident Response Procedures](#RelatedInformation) when reporting and responding to security incidents involving Town of Chapel Hill information technology.

1. **Identity Theft Prevention**

The Town’s identity theft prevention program and associated procedures designed to detect, prevent and mitigate identity theft in connection with Town ‘covered accounts’ as required by the Fair and Accurate Credit Transactions (FACT) Act of 2003.

Identity theft prevention is designed to detect, prevent and mitigate reasonable foreseeable risks of identity theft to customers or to the Town of Chapel Hill in connection with an existing utility account or the opening of a new utility account (or other covered account), and to satisfy the requirements of 16 CRF Part 681 (‘Red Flag Requirements’).

Business Management staff will use their best judgment when signing customers into service and when dealing with existing accounts to identify patterns, practices or specific activity that would indicate the possible existence of identity theft – also known as “Red Flags”. Red Flags are indicators that alert staff when customer account information and consumer identity may be fraudulent. By having procedures in place to identify, detect, prevent, and respond to Red Flags, the Town is limiting identity theft in connection with the opening of a covered account. In addition to the [specific guidance in the Red Flags Checklist](#RelatedInformation), staff will also consider other triggers identified in the federal Red Flag Requirements.

Staff will balance the response to red flags with the degree of risk posed. The Business Management department will establish a identify theft prevention committee to serve as a review panel for red flags, and to review identity theft policies and procedures on an annual basis. The identity theft committee will be made up of at least the Director of Business Management, and the Utility Accounts Manager or their designee.

* 1. **Training, Oversight and Review**

The Business Management Director or their designee is responsible for oversight related to this procedure.

* + 1. Business Management staff will conduct training as necessary to effectively implement the identity theft prevention program.
    2. Business Management staff will report the compliance and training measures related to this procedure at least annually to the Town Manager.
       1. The report will evaluate the effectiveness of the applicable policies and procedures in addressing the risk of identity theft in connection with opening and maintaining accounts and in the handling of sensitive information.
       2. The report will include changes in risk to customers and to the Town of Chapel Hill from identity theft based on factors such as experience with identity theft, changes in methods of identity theft, changes in methods to detect, prevent, and mitigate identity theft, changes in the types of accounts maintained, changes in the type of information stored and handled, and changes in business arrangements.

1. **Special Provisions:** Contractors and Vendors who have direct access to computer systems and networks that contain Criminal Justice Information (CJI) shall be required to verify identification via a state of residency and a national fingerprint-based records check. [(FBI CJIS Security Policy v5.6, section 5.12.1.2 “*Personnel Screening for Contractors and Vendors*”)](https://www.fbi.gov/file-repository/cjis-security-policy-v5_6_20170605.pdf/view)

IV. FORMS/INSTRUCTIONS:

**EXHIBIT A**: SENSITIVE INFORMATION USER AGREEMENT For Town Employees

**EXHIBIT B**: SENSITIVE INFORMATION SERVICE AGREEMENT For Town of Chapel Hill Vendors

**EXHIBIT C**: RED FLAG IDENTIFICATION AND DETECTION USER AGREEMENT For Town Employees

ACKNOWLEDGEMENT FORM

I acknowledge that I read and received a copy of the Town of Chapel Hill Technology Security Policy. I fully understand the terms of this policy and agree to abide by them. I understand that the Town’s security software may record for management use the internet address of any site that I visit and keep a record of any network activity in which I transmit or receive any kind of file. I acknowledge that any message I send or receive will be recorded and stored in an archive file for management use. I know that any violation of this policy could lead to disciplinary action, dismissal, or even criminal prosecution.

Employee’s Department

Employee’s Signature Date

Supervisor’s Signature Date

V. ADDITIONAL CONTACTS:

Business Management 919-968-2712 [finance@townofchapelhill.org](mailto:finance@townofchapelhill.org)

Technology Solutions 919-968-2020 or [ITSupport@townofchapelhill.org](mailto:ITSupport@townofchapelhill.org)

Human Resource Development 919-968-2700 or [HR@townofchapelhill.org](mailto:HR@townofchapelhill.org)

Ombuds office 919-265-0806 or [Ombuds@townofchapelhill.org](mailto:Ombuds@townofchapelhill.org)

Employee Assistance Program 1-800-326-3864

VI. DEFINITIONS

Breach – A breach is considered to have happened if any sensitive information has or is suspected to have been stolen, viewed, copied, lost, compromised or intruded upon by an unauthorized person or persons or if it is suspected that information has been lost and could be accessed by unauthorized person or persons. A breach can occur physically or virtually via technology.

Cashier station – Any location in town that accepts payments.

Covered Account – A covered account is (1) an account primarily for personal, family, or household purposes, that is designed to permit multiple payments or transactions, or (2) any other account for which there is a reasonably foreseeable risk to customers or the safety and soundness of the financial institution or creditor from identity theft.

Essential tasks – Job duties required for managing the responsibilities of a position.

Red Flags – Patterns, practices, or specific activities that indicate the possible existence of identity theft.

Sensitive Information – Includes criminal justice information (CJI), credit card information, banking account information, social security and federal tax identification information, driver license information and any other identifying information as identified in (N.C.G.S 14-113)

System - Refers to computers and or computer programs that are used for financial reporting, bill processing, and account maintenance or in any other way that may contain sensitive information.

Technology – Resources belonging to the Town or used in connection with Town business as defined in the Town Appropriate Use of Technology Policy.

VII.  RESPONSIBILITIES

**All Employees are expected to:**

1. Be aware of this policy, procedures and associated checklists
2. Ask questions about anything they do not understand
3. Attend training that is relevant to their positions
4. Protect all sensitive information to which they have access

**All Supervisors/Managers are expected to:**

1. Be aware of this policy, procedures and associated checklists
2. Ask questions about anything they do not understand
3. Periodically review this policy, procedures and associated checklists as they assign technology and access to sensitive information to their employees
4. Assure that employees who handle sensitive information are aware of any training they are required to complete

**All Department Heads are expected to:**

1. Be aware of this policy, procedures and associated checklists
2. Ask questions about anything they do not understand
3. Periodically review this policy, procedures and associated checklists as they assign technology and access to sensitive information to their employees
4. Work with the Town’s Contracts Manager and the Financial Services Administrator to assure that vendors for contracts they execute have the appropriate checklists and other information about Town expectations regarding data security.

**All Business Management is expected to:**

1. Work with Technology Solutions to communicate about and implement this policy and procedures throughout the Town.
2. Work with the Learning and Development Manager and Technology Solutions to design and conduct training on the various aspects of these procedures
3. Assure that employees who complete training sign the appropriate acknowledgements and that they are forwarded to HRD for inclusion into the employees’ personnel files

**All Human Resource Development staff members are expected to:**

1. Work with Technology Solutions and Business Management to provide guidance and training for employees and managers on technology, managing sensitive information, and disposal of sensitive information as they are hired.
2. Consult with and assist departments and employees on maintaining accurate records of completed training.

**All Technology Solutions is expected to:**

1. Work with Business Management and the Learning and Development Manager to design and conduct training throughout the Town
2. Assist departments in understanding the technical aspects of this policy
3. Periodically review procedures to assure compliance with applicable laws and other Town policies
4. When requested, help departments identify positions with access to sensitive information

VIII. APPENDICES

EXHIBIT A

**SENSITIVE INFORMATION USER AGREEMENT**

**For Town Employees**

EXHIBIT B

**SENSITIVE INFORMATION SERVICE AGREEMENT**

**For Town of Chapel Hill Vendors**

EXHIBIT C

**RED FLAG IDENTIFICATION AND DETECTION USER AGREEMENT**

**For Town Employees**

**CHECKLIST FOR MANAGERS AND EMPLOYEES FOR PROTECTING SENSITIVE INFORMATION**

EXHIBIT E

**CHECKLIST FOR THIRD-PARTY CONTRACTS WHEN THE SCOPE OF WORK INCLUDES SENSITIVE INFORMATION**

EXHIBIT F

**BREACH IDENTIFICATION CHECKLIST**

IX. FREQUENTLY ASKED QUESTIONS: None

X.  SCOPE: This policy applies to all employees of the Town of Chapel Hill

XI. RELATED INFORMATION

Data Security – Red Flags Checklist

Data Security – Breach Response Plan

Technology Incident Response Procedure

XII: POLICY HISTORY:

Issued January 1, 2018

This policy replaces and supersedes any previous Town policies, departmental policies, handbooks, or unwritten policies or practices covering the same subject.  Departmental policies in compliance with this policy are referenced in Section XI below, **Related Information.** In the event of any disparity between this policy and the Town’s Code of Ordinances and/or applicable local, state, or federal laws, the Town’s Ordinance and/or applicable laws shall prevail.

EXHIBIT A

**SENSITIVE INFORMATION USER AGREEMENT**

**For Town Employees**

I understand that proper management, maintenance and storage of Sensitive Information at the Town of Chapel Hill as well as recognition and report of Breaches of this information are a standard procedure of the Town.

I will handle Sensitive Information at the Town of Chapel Hill under the provisions of the standard procedure.

In the event of a suspected Breach, I will follow the standard procedure for identifying and reporting a Breach of the Town’s Sensitive Information.

I understand that negligent handling or inappropriate use of the Town of Chapel Hill’s Sensitive 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 and related standard procedure:

|  |  |
| --- | --- |
| Name (printed): |  |
| Department/Division: |  |
| Signature: |  |
| Date: |  |

***All employees sign a policy acknowledgement at orientation and are shown where polices can be found on the Town’s website.***

***Questions? Contact Business Management 919-968-2712 or Human Resource Development 919-968-2700.***

EXHIBIT B

**SENSITIVE INFORMATION SERVICE AGREEMENT**

**For Town of Chapel Hill Vendors**

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 Chapel Hill.

1. The appointed representative(s) of the Company have read the Town of Chapel Hill’s Standard Procedure on Security of Sensitive Information and Breach Response Plan.

1. The company accepts responsibility for the security of sensitive information in their possession.

1. Data can ONLY be used to complete the service as described by the Town of Chapel Hill.

1. 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.

1. If a security intrusion has been detected, the Company will notify the Town immediately and will allow their system to be thoroughly reviewed. 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 and will validate compliance with Payment Card Industry Security Standards for protecting cardholder data.

1. The Company will treat all sensitive information confidentially.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Title

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Company

***Responsibility: This form should be attached to any vendor agreement to which it pertains. It is generally for vendors who might handle sensitive information. The Contracts Manager and Department Head are responsible for assuring that vendors sign this form.***

***Questions? Contact the Contracts Manager 919-969-5022 or Business Management 919-968-2712***

EXHIBIT C

**RED FLAG IDENTIFICATION AND DETECTION USER AGREEMENT**

**For Town Employees**

I understand that detection, prevention and mitigating risks of identity theft in connection with an existing utility account or the opening of a new utility account are a standard procedure of the Town.

I will use my best judgment when signing customers into service and when dealing with existing accounts to identify patterns, practices or specific activity that would indicate the possible existence of identity theft – also known as “Red Flags”.

In the event I become aware of a red flag in connection with a utility account, I will follow the standard procedure for response.

I understand that an intentional failure to follow standard procedure will be subject to disciplinary action up to and including dismissal.

I have read, understand and agree to the conditions above and related standard procedure:

|  |  |
| --- | --- |
| Name (printed): |  |
| Department/Division: |  |
| Signature: |  |
| Date: |  |

***Responsibility: This form would be used after an employee completes Red Flag Training. BMD is responsible for obtaining these signatures or otherwise documenting in the Learning Management System that an employee has completed this training.***

***Questions? Contact Business Management 919-968-2712 or Technology Solutions 919-969-2020***

EXHIBIT D

**CHECKLIST FOR MANAGERS AND EMPLOYEES FOR PROTECTING SENSITIVE INFORMATION**

Overview: Many Town employees routinely handle sensitive information including financial information, human resource information, personally identifiable information and other information protected by local, state and federal law. This checklist must be reviewed with all employees during orientation to ensure all are familiar with protecting sensitive information.

**Access to sensitive information**

* + - Access to sensitive information will be provided only in order for employees to perform essential tasks.
    - Employees who have access to sensitive information are required to create, handle, maintain, and dispose of such information prudently to ensure proper security.
    - Managers in each department will minimize the number of employees with access to sensitive information in accordance with applicable federal and state requirements.
    - In order to minimize access, managers should consider the following:
      * + Review job duties on a regular basis, and restrict access to sensitive information where possible. Annual performance reviews are an appropriate time for this evaluation.
        + Only grant access to sensitive information to those employees who need it for essential tasks.
        + Prohibit employees from sharing their system access or using another’s system access.
        + Work with Technology Services to:

Remove employee’s system authority immediately upon termination of employment.

Change employee’s system authority immediately upon any change in duties or position.

**How to securely maintain sensitive information.**

**Daily use and storage:** The following procedures should be followed while creating, handling, maintaining, storing, and disposing of sensitive information:

1. Do:
   1. Where possible, enter the information directly in the system (to its final destination)
   2. If sensitive information is written on paper for reference, shred immediately upon completion of task.
   3. Segregate sensitive information from public information.
   4. Restrict the number of employees who have access to maintenance screens where sensitive information is stored, which includes privileged access (root or administrative access) to systems containing sensitive information.
   5. Only maintain printed documentation of sensitive information in a secured cabinet or room and limit access to these areas.
   6. Properly destroy all documents containing sensitive information on a timely basis according to procedures outlined below.
   7. Where technologically possible, utilize encryption to secure the information in the database or storage system.
2. Do not:
   1. Write sensitive information on notepads, post-it notes or other temporary areas.
   2. DO NOT leave paper containing sensitive information in an unsecured area.
   3. Include any sensitive information in e-mails.
   4. Include sensitive information on printed reports except as needed for the performance of essential tasks and only with supervisor’s approval.
   5. Leave your PC/laptop signed on (or unlocked) while away from your work-area.
   6. Store files with sensitive information on thumb drives or other portable storage devices.

**Destruction of sensitive information**

* Information will be retained according to Town policy and procedure as well as the applicable NC Records Retention Laws.
* Financial records will be destroyed using methods that meet all requirements from merchant service contracts, legislative orders, federal laws, NC statutes and Town policies.
* Police evidence will be disposed of following Police Department procedures and in compliance with CJI requirements.
* Documents containing sensitive information must not be disposed in regular trash or recycling.
* Tainting or destruction of evidence from incident handling actions, including logging on to the affected systems, is prohibited.

There is a reporting requirement for us and for vendors. Use these forms when you suspect a breach.

They are required to report these as quickly as possible. Vendors must report a possible breach to the town within 48 hours.

***Use—provide this checklist to a vendor when you execute a contract. It is generally an addendum to a contract***.

***Questions? Contact the Contract Manager 919-969-5022 or Financial Services Administrator 919-969-5021***

***Responsibility: The Contract Manager and Department Head should assure that this information is provided to an applicable vendor.***

EXHIBIT E

**CHECKLIST FOR THIRD-PARTY CONTRACTS WHEN THE SCOPE OF WORK INCLUDES**

**SENSITIVE INFORMATION**

Overview: The Town routinely contracts with third parties that will handle sensitive information. These contracts can be:

1. One-time or short term access.
2. Cloud service applications and/or data storage
3. Transaction processing

When working with third-parties, the Town may request:

* Acknowledgement that the third party is responsible for security of sensitive information in their possession.
* Statement that data can ONLY be used for assisting these parties in completing the tasks described in the contract statement of work, such as a transaction, providing fraud control services, or for others uses specifically required by law.
* Assurance of business continuity in the event of a major disruption, disaster, or failure.
* Immediate notification to the Town for any suspected or potential security breech.
* Allowance for their system to be thoroughly reviewed after a security intrusion has been detected. 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 will be conducted by a Payment Card Industry representative and will validate compliance with Payment Card Industry Security Standards for protecting cardholder data.
* Statement that all sensitive information will be treated confidentially.
* Statement that the third party has received and reviewed the Town’s Standard Procedure for the security of sensitive information.
* For related services provided outside of the contract system, vendors will be required to sign a Sensitive Information Service Agreement (see Exhibit B).

An example paragraph that can be included in a service contract:

*Contractor is responsible for the security of sensitive information and confidential or private employee information that is in their possession and will hold this information in strict confidence. Contractor staff has read the Town's Standard Procedure for the Security of Sensitive Information and agrees to take appropriate measures (as outlined in procedure) to secure sensitive information with the goal of breach prevention. This sensitive and private information can only be used to complete required testing or for other uses specifically required by law. If a security intrusion has been detected involving this information, Contractor will notify the Town of Chapel Hill Business Management Department immediately in order for the Town to implement their breach response plan according to approved procedures. Contractor shall permit the Town, or Town’s agent to review Contractor’s system if a security intrusion is detected. In the event the intrusion is related to credit card numbers, the review may be conducted by a Payment Card Industry representative and will validate compliance with Payment Card Industry Security Standards for protecting cardholder data.*

EXHIBIT F

**BREACH IDENTIFICATION CHECKLIST**

***Use: Employees can use this checklist to scan for a possible breach. Suspected breaches should be immediately reported to Technology Solutions 919-969-2020 or to BMD 919-968-2712.***

**Overview:** A breach includes activities that may indicate an attempt to use or access Town technology, information or systems, or paper files without proper authorization or may have extracted information or transmitted information without proper authorization.

**A technology breach:** This area includes the following items but may also include items not listed:

* Someone else’s name is in your sign-on window and you are the sole user of your machine.
* Someone else’s name is in your sign-on window and you do not recognize them as a user of your machine. Technology Solutions staff may sign on your machine occasionally for maintenance but you should have been notified. Disconnected computer cables or power cables.
* Missing computer equipment (desktop, laptop, etc)
* Evidence that files residing on desktops or laptops have been accessed by unauthorized users.
* Devices or media attached to your computer that you don’t recognize. These could be, CD’s or thumb drives or other portable storage devices that are in your system or on your desk and you do not recognize them as yours.
* Windows that appear on your system that you do not recognize and are not part of your normal start up process.
* Items that have been moved or are missing on your system such as folders that have been placed in other locations.
* Any other activity which arouses suspicion that someone has made an attempt to use your system without approval.

**Physical Breach:** This area includes physical file storage, documents stored in offices and on desktops or laptops. The following are examples of signs that a physical breach may have occurred:

* Evidence of lock tampering on file cabinets or office doors
* Evidence of a break-in in an area where sensitive information is stored
* Missing files or papers that contain sensitive information
* Missing computer or other technology equipment

***Report Suspected Breaches to Technology Solutions 919-969-2020 or to BMD 919-968-2712.***