The Town of Somerset

Data Security Policy

As mandated by State law, the Town of Somerset (hereafter referred to as "Town") hereby establishes the following written policies and procedures for the protection of personal information lawfully obtained by the Town. They apply to all Town staff, the Mayor, Council members, volunteers, and contractors ("responsible parties" or "authorized individuals").

Definitions

For the purposes of this policy, the following words have the meanings indicated.

1) "Personal information" means an individual's first name or first initial and last name, personal mark, or unique biometric or genetic print or image, in combination with one or more of the following data elements:
    a. Social Security number;
    b. Driver's license number, state identification card number, or other individual identification number issued by a unit;
    c. Passport number or other identification number issued by the United States government;
    d. Individual Taxpayer Identification Number; or
    e. Financial or other account number, a credit card number, or a debit card number that, in combination with any required security code, access code, or password, would permit access to an individual's account.

"Personal information" does not include the following: (1) publicly available information that is lawfully made available to the general public from federal, State, or local government records; (2) information that an individual has consented to have publicly disseminated or listed; or (3) information that is disclosed according to other applicable law or judicial order.

2) "Records" means personal information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.

Security Measures

To protect personal information from unauthorized access, use, modification, or disclosure, the Town will employ the following security procedures and practices. All records shall be protected with a minimum of two layers of security, which may include but not be limited to, the Town Office door being locked when the Office is not in use; the Town Office computers being

password protected and locked when not in use by authorized individuals; filing cabinets containing personal information being locked when not in use by authorized individuals; and the Town internet service being password protected. The Town will maintain appropriate network security, including firewalls, on all computers.

Destruction of Records

The Town will retain records in the Town Office in accordance with the Town's State-approved document retention schedule. When a record meets the criteria for removal under the retention schedule, it will be purged, destroyed (e.g., by shredding paper files containing personal information), deleted, or returned to the submitting source as required.

Reporting Violations

Responsible parties will promptly and without unreasonable delay report any and all violations of this policy to the Town Manager, Mayor, or Town Council, as appropriate.

Investigating a Possible Breach

The Town Manager or Mayor, or Town contractors, as appropriate, will investigate the circumstances of a possible breach to determine whether the unauthorized acquisition of personal information has resulted in or is likely to result in the misuse of the information. The results of such investigation shall be shared promptly and without unreasonable delay.

If/When a Breach is Confirmed

Notification

The Town Manager or Mayor, as appropriate, will work with the Town's legal counsel to notify impacted individuals promptly and without unreasonable delay. Notification should be made in writing as soon as practicable to the most recent address of the impacted individual(s). Alternatively, notice may be provided by e-mail or telephone.

Notifications shall include the following: (1) to the extent possible, a description of the categories of information that were, or are reasonably believed to have been, acquired by an unauthorized person, including which of the elements of personal information were, or are reasonably believed to have been, acquired; (2) contact information for the responsible party making the notification, including an address, telephone number, and toll-free telephone number

if one is maintained; (3) the toll-free telephone numbers and addresses for the major consumer reporting agencies; and (4) (i) the toll-free telephone numbers, addresses, and Web site addresses for: (a.)The Federal Trade Commission; and (b.) The Office of the Attorney General; and (ii) a statement that an individual can obtain information from these sources about steps the individual can take to avoid identity theft.

Before giving the notification, the responsible party shall provide notice of a breach of the security of a system to the Office of the Attorney General and to the Department of Information Technology.

If, after the investigation is concluded, it is determined that notification is not required, the responsible parties shall maintain records that reflect its determination for 3 years after the determination is made.

Containment

If a breach is confirmed, the Town Manager or Mayor, as appropriate, working with the responsible parties and individuals impacted, shall take the following steps to limit the scope and effect of the breach without unreasonable delay.

1) Stop any unauthorized practice;
2) Recover the records, if possible;
3) Shut down the system that was breached;
4) Change passwords;
5) Change locks on cabinets or doors;
6) Correct weaknesses in security practices; and
7) Notify the appropriate authorities including the Montgomery County, MD Police Department, if the breach involves, or may involve, any criminal activity.

Enforcement

If, after a thorough review, any responsible party is found to be in violation of this policy as it pertains to the gathering, collection, use, retention, destruction, or disclosure of records, the Town will:

1. Immediately suspend access to Town information systems by the person(s) involved in the violation.
2. If an individual is a Town employee or contractor, he or she will be referred to the Town Manager for disciplinary action, up to and including termination of employment or their contract with the Town.

3. If the individual is the Town Manager, he or she will be referred to the Mayor or Town Council for disciplinary action, up to and including termination of employment.
4. If appropriate, refer the violation to the appropriate law enforcement authority to initiate a criminal investigation in their sole discretion.

The Town reserves the right to restrict the qualifications and number of individuals having access to Town information and to suspend or withhold service and deny access to any individual.

Prevention

In order to ensure the Town maintains the most current approach to the protection of personal information, this policy may be periodically updated as deemed necessary by the Town Council. It may also be updated following any confirmed breach to implement any resolution plan resulting from an investigation of the circumstances of the breach, its root cause(s), and any remaining risk(s).

The Town Manager, Mayor, or Council, as the case may be, in their sole discretion, may dispense with the above requirements in the rare case of an emergency in order to protect the health, safety, comfort, and welfare of the Town and its residents.