Town Of Danvers Information Privacy Policy

(DAN-SG-POL-PRV)

Table of Contents

1 Purpose and Scope 3
2 Exceptions 3
3 Requirements 3
3.1 Direction 3
3.2 Definition of Personal Information 3
3.3 Collection of Personal Information 4
3.4 Protection and Disclosure of Personal Information 4
3.5 Handling of Personal Information 5
3.6 Assignment of Privacy Officer 6
3.7 Communication of Privacy Policy 6
3.8 Access by an Individual to their Personal Information 6
3.9 Privacy Complaints 6
3.10 Employee Personal information 6
3.11 E-Commerce Security 6
3.12 Review of Privacy Program 8
3.13 Penalties 8
4 Roles and Responsibilities 8
5 Glossary of Terms 8
6 Records 13
7 Distribution 13
8 References 13
9 Revision History 14

1 Purpose and Scope

This policy articulates the technical and process security measures which must be followed by all employees, contractors and third-parties to ensure the protection of personal information under the control of the Town of Danvers throughout the lifecycle of this information. This policy also provides the requirements for the secure configuration of Electronic Commerce (E-commerce) sites and services (i.e., both internal and external) provided by the Town of Danvers and its IT Service Providers for use by customers and employees. This policy amplifies on the policy statements related to information privacy made in the policy entitled ***Town of Danvers Cyber Security Policy (i.e., DAN-SG-POL-SEC).*** At the present time this policy applies to the Town of Danvers Business, Electric and Water Divisions, and specifically to the Smart Grid Implementation. The security services and mechanisms in this policy are intended to mitigate the risks of fraud, misappropriation, unauthorized transactions, breach of privacy and denial of service.

This policy shall be reviewed and updated as required on an annual basis.

2 Exceptions

In situations where, for whatever reason, there is an inability to comply with the security measures specified in this policy document, specific exceptions may be requested. Every effort shall be made to comply with the prescribed security measures. Where the security measures cannot be implemented, a security risk assessment must be conducted to quantify the residual risk. The individual seeking the exception shall obtain approval from the Director of Management Information Systems (i.e., MIS Director) or a delegate for any specific deviations from the requirements stipulated in this policy document. The risk assessment shall document the risk to the Town and the mitigating or compensating measures to be implemented to bring the residual risk to an acceptable level. Exceptions shall be reviewed on an annual basis to determine the continuing requirement for such exceptions.

3 Requirements

3.1 Direction

The Town of Danvers is committed to respecting the privacy of individuals through the protection of personal information consistent with the direction provided in the Massachusetts Data Privacy Law.

3.2 Definition of Personal Information

Personal information to be protected includes an individual's name (either first and last name or first initial and last name) combined with a complete social security number, driver's license, or other state-issued number, a financial account number or a complete credit card or bank account number. This encompasses a wide variety of informational records - everything from

employee, client, customer and investor records to supplier, patient and student records. What it does not include is any information that is lawfully obtained from publicly available information or from federal, state or local government records lawfully made available to the general public.

3.3 Collection of Personal Information

The Town of Danvers gathers information regarding its customers in order to provide electricity, water, construction services and maintenance services. This information is used for billing, providing services and for collections. New sources of personal information relating to electricity and water consumption in real-time may also be collected as a result of the implementation of Smart Grid Technologies.

An individual about whom personal information is being collected must consent to the recording of their personal data within the corporate records of the Town of Danvers and to the specific use or uses made of that data. The data shall only be used for the purposes stated when the data is collected and shall only be obtained directly from the individual to whom the information pertains. Each area of the Town of Danvers that collects personal data shall inform the individual concerning the intended use of their personal data and obtain their consent before recording the information. As well, only the minimum amount of information required to perform the business function shall be recorded.

3.4 Protection and Disclosure of Personal Information

Personal information within the Town of Danvers shall be protected by administrative, technical, contractual and physical controls designed to ensure that inappropriate access to or disclosure of this information is limited to the greatest extent possible. As new forms of personal information are collected by the Town of Danvers as a result of the implementation of Smart Grid Technologies a Privacy Impact Assessment shall be conducted to clearly define the personal information being collected and to allow for the specification of the security controls required to protect this personal information throughout its lifecycle within the Town of Danvers.

It is the policy of the Town of Danvers to not provide personal information to any party outside of the Town. There are, however, limited circumstances under which it is necessary to disclose personal information. The disclosure of information to third parties for specific limited circumstances may include disclosure to:

- a contractor or service provider acting on behalf of the Town of Danvers;
- an agency who collects funds owing to the Town of Danvers;
- where required by law or as a result of a court order;
- police, where the Town of Danvers believes that there is a possible breach of the law such as, for example, the theft of power; and,
- emergency response agencies during emergency situations.

In general, apart from the specific circumstances described above, no personal information shall be provided to any party outside of the Town of Danvers without the consent of the individual to which the personal information relates. As well, vendors, contractors and services providers conducting business with the Town of Danvers shall have their purchase orders and/or contracts structured so as protect the privacy of any personal information provided to them.

Personal information shall only be collected to the extent that it is necessary to fulfill a business function and access to such information within the Town shall only be provided to an employee of the Town when there is a specific business need. When the personal data is no longer required by the Town it shall be deleted or destroyed in a manner consistent with the policies describing the treatment of information classified with the Town of Danvers as "Confidential".

Data retention periods shall be defined for all personal information collected by the Town of Danvers depending on the purpose for which the data was collected. After the retention period has expired the personal information may be disposed of as long as it is not associated with a current inquiry. It is considered a serious offence to dispose of personal information that is the subject of an inquiry.

3.5 Handling of Personal Information

Information collected by the Town of Danvers may be stored or processed both inside and outside of the United States. In either case the information must be protected by appropriate physical and electronic security safeguards.

In general, personal information shall not be left in plain view or unattended in an unsecure area. All Town of Danvers employees with electronic access to personal data shall be required to lock their computers with an appropriate password when they leave their desks.

When not in use all personal data must be maintained in locked storage cabinets.

Hardcopy records containing personal information must be shredded when disposal is required. Electronic media containing personal information must be securely erased or destroyed according to the policy articulated in the ***Town of Danvers Information Protection and Management Policy (i.e., DAN-SG-POL-INP)*** when disposal is required.

Electronic records containing personal information stored and processed on Town of Danvers Systems shall be secured by application, network and server based security controls as defined in the ***Town of Danvers Cyber Security Policy (i.e., DAN-SG-POL-SEC)***, the ***Town of Danvers Network Security Policy (i.e., DAN-SG-POL-NET)*** and the ***Town of Danvers User Access Control Policy (i.e., DAN-SG-POL-UAC)***. The security controls employed shall be consistent with the handling of information classified as "Confidential".

3.6 Assignment of Privacy Officer

The Town of Danvers shall appoint an individual to the position of Privacy Officer. The Privacy Officer shall be responsible for overseeing the implementation of this policy with the Town of Danvers and for monitoring the compliance with this policy as part of ensuring the implementation of an effective Privacy Program.

3.7 Communication of Privacy Policy

The Town of Danvers Privacy Policy shall be made available on the Town of Danvers website at http://www.danvers.govoffice.com.

3.8 Access by an Individual to their Personal Information

An inquiry by an individual in relation to the personal information held by the Town of Danvers concerning that individual shall be handled in such a manner that only the information concerning that specific individual is shared with that individual. If the employee within the Town of Danvers is unsure as to how to handle such a request he or she should first consult with the Privacy Officer of the Town of Danvers.

3.9 Privacy Complaints

Complaints regarding the Privacy Policy of the Town of Danvers or any suspected breach of this policy shall be forwarded immediately to the Privacy Officer of the Town of Danvers. The Privacy Officer shall investigate any complaints received promptly and recommend corrective action to senior management within the Town of Danvers.

3.10 Employee Personal information

Personal information pertaining to employees of the Town of Danvers shall be collected and protected in the same manner as all other personal data. Employee data should be treated as "Confidential" in nature. It should be safeguarded within the Human Resources Department of the Town of Danvers and should not be circulated outside of the Human Resources Department.

3.11 E-Commerce Security

Customer personal information obtained as a result of electronic commerce (i.e., E-commerce) activities shall be classified as "Confidential" and safeguarded against misuse and unauthorized disclosure.

E-commerce sites providing services to Town of Danvers customers or the general public shall disclose their information privacy practices on the Web site. The disclosure shall include the specific types of information being collected and retained, and the specific usage of the information. The site shall provide information regarding the manner in which to resolve complaints related to the accuracy, completeness and distribution of customer information. As

well, E-commerce sites providing services to customers or the general public shall disclose their business practices (i.e., delivery methods, payment terms, warranty information, etc) on the Web site.

E-commerce services and applications used by the Town of Danvers shall meet the requirements of all applicable Town of Danvers IT Security Policies. Particular attention should be given to:

- Business Continuity and Disaster Recovery capabilities
- Protection of Town of Danvers data on servers using strong access authentication mechanisms and while in transit through communication facilities using cryptographic mechanisms
- Backup and recovery of Town of Danvers data
- Physical Security
- Personnel Security
- The security hardening, malware protection and electronic monitoring of the hosting environment (which may be provided by an external IT Service Provider)

The implementation and configuration of E-commerce sites supported by external IT Service providers shall be governed by specific contracts or service level agreements between the Town of Danvers and the external service provider. Also, evidence of audits by independent parties that support the statements of the external provider with respect to the privacy of customer information and business practices is preferable. Where possible, the Town of Danvers shall also attempt to ensure the ability to audit the infrastructure of the external IT Service Provider to confirm that acceptable security measures have been implemented.

Audit logs shall be maintained and reviewed on at least a monthly basis by the Town of Danvers or its IT Service Provider to confirm the validity of E-commerce transactions. Indications of fraud or other improper use of the service shall be brought to the attention of the Town of Danvers MIS Director.

Servers used for E-commerce shall be hardened to resist attempts at penetration or unauthorized use. Unnecessary services and applications should be disabled or removed from the server. All relevant vendor security patches shall be applied to the operating system and application software.

Digital certificates shall be installed on E-commerce servers to authenticate the server and support the encrypted sessions using the Secure Socket Layer (SSL) protocol with at least 128-bit keys. Sensitive or confidential data, including credit card numbers, shall be protected by suitable encryption methods. As well, "Confidential" information shall not be transmitted in unencrypted form or provided to an unsecure server.

After an E-commerce session is completed, users shall be directed to clear the web browser cache to ensure that confidential data is not retained in the cache. Login names and passwords shall not be remembered or cached by web browsers or other E-commerce client software.

3.12 Review of Privacy Program

On an annual basis the Privacy Officer of the Town of Danvers shall undertake a review of the privacy practices and controls within the Town and provide a report outlining any compliance issues to the Senior Management within the Town of Danvers for purposes of instituting a program of corrective actions.

3.13 Penalties

Failure to conform to the requirements of this policy may result in disciplinary action up to and including the termination of employment for employees. For contractors the disciplinary actions may include termination of contracts with the Town and possible legal action by the Town in order to recover damages.

4 Roles and Responsibilities

Privacy Officer – The Privacy Officer is accountable for the following with respect to this policy:

- The implementation of an effective Privacy Program within the Town of Danvers aimed at ensuring the protection of customer and employee personal information throughout its lifecycle within the Town of Danvers
- The annual monitoring of compliance with the requirements of this policy document
- The timely investigation and resolution of privacy related complaints and issues

MIS Director – The MIS Director is accountable for the following with respect to this policy:

- The development, ongoing maintenance and execution of the security processes required to properly secure electronic commerce sites utilized by the Town of Danvers
- Review, approval, and retention of a list of all approved Security Exceptions to this policy

General Users – General Users are accountable for the following with respect to this policy:

- Compliance with the requirements contained within this policy document

5 Glossary of Terms

Access token – an **access token** contains the security information for a login session and identifies the user, the user's groups, and the user's privileges.

Advanced Metering Infrastructure – **Advanced Metering Infrastructure (AMI)** are systems that measure, collect and analyze energy usage, and communicate with metering devices such as electricity meters, gas meters, heat meters, and water meters, either on request or on a schedule. These systems include hardware, software, communications, consumer energy displays and controllers, customer associated systems, Meter Data Management (MDM) software, and supplier business systems.

Anti-virus Definitions – Virus definitions are identifying characteristics that anti-virus software can use to positively match malicious software on a computer system with known viruses that have been reported.

Anti-Virus Software – **Antivirus** or **anti-virus software** is used to prevent, detect, and remove malware, including but not limited to computer viruses, computer worm, trojan horses, spyware and adware.

Authentication - Authentication is any process by which you verify that someone is who they claim they are. This usually involves a username and a password, but can include any other method of demonstrating identity, such as a smart card, retina scan, voice recognition, or fingerprints. Authentication is equivalent to showing your driver's license at the ticket counter at the airport.

Authorization - Authorization is finding out if the person, once identified, is permitted to have access to a resource. This is usually determined by finding out if that person is a part of a particular group, if that person has paid admission, or has a particular level of security clearance. Authorization is equivalent to checking the guest list at an exclusive party, or checking for your ticket when you go to the opera.

Availability - For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks.

Boundary protection - **Boundary protection** demarcates logical or physical **boundaries** between unknown users and protected information and systems. **Boundary protection** controls logical connectivity into and out of networks and controls connectivity to and from network-connected devices.

CD - The **Compact Disc** (also known as a **CD**) is an optical disc used to store digital data.

Confidentiality - Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems. For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in databases, log files, backups, printed receipts, and so on), and by

restricting access to the places where it is stored. If an unauthorized party obtains the card number in any way, a breach of confidentiality has occurred.

Credential - Credentials in cryptography establish the identity of a party to communication. Usually they take the form of machine-readable cryptographic keys and/or passwords.

CSIRT - **Computer Security Incident Response Team** is a name given to expert groups that handle computer security incidents.

Distribution Automation – A term used to describe the extension of intelligent control over electrical power grid functions to the distribution level and beyond.

DNS - The **Domain Name System** (**DNS**) is a hierarchical naming system built on a distributed database for computers, services, or any resource connected to the Internet or a private network. Most importantly, it translates domain names meaningful to humans into the numerical identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide.

DVD – DVD is an optical disc storage media format.

Encryption – In cryptography, **encryption** is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

Encryption certificates – In a **Certificate-based encryption** system a certificate is used as a conventional certificate (for signatures, etc.), but also implicitly for the purpose of encryption.

Escrow – **Source code escrow** is the deposit of the source code of software with a third party escrow agent. Escrow is typically requested by a party licensing software (the licensee), to ensure maintenance of the software. The software source code is released to the licensee if the licensor files for bankruptcy or otherwise fails to maintain and update the software as promised in the software license agreement.

Integrity – In information security, integrity means that data cannot be modified undetectably. Integrity is violated when a message is actively modified in transit. Information security systems typically provide message integrity in addition to data confidentiality.

Intrusion Detection and Prevention Systems and Signatures – **Intrusion Prevention Systems** (IPS), also known as **Intrusion Detection and Prevention Systems (IDPS)**, are network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about said activity, attempt to block/stop activity, and report activity. In an IDPS based upon signatures the signatures represent attack patterns that are preconfigured and predetermined. A signature-based intrusion prevention system monitors the network traffic for matches to these signatures. Once a match is found the intrusion prevention system takes the appropriate action.

IPSec – **Internet Protocol Security** (**IPsec**) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session.

Key Management System – Keys are secured in a locked enclosure and each key is assigned a physical and logical location. Each key or key bundle may be assigned to an individual whose security credentials permit the use of that key during that time period. Returned keys are logged in providing management with a report of when and to whom the keys were issued and whether keys are available or remain out.

Logon – In computer security, a **login** or **logon** (also called **logging in** or **on** and **signing in** or **on**) is the process by which individual access to a computer system is controlled by identification of the user using credentials provided by the user.

Malicious software or Malware – **Malware**, short for **malicious software**, consists of programming (code, scripts, active content, and other software) designed to disrupt or deny operation, gather information that leads to loss of privacy or exploitation, gain unauthorized access to system resources, and other abusive behaviour. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.

Multifactor Authentication - Multifactor authentication (MFA) is a security system in which more than one form of authentication is implemented to verify the legitimacy of a transaction. In contrast, single factor authentication (SFA) involves only a user ID and password. In two-factor authentication, the user provides dual means of identification, one of which is typically a physical token, such as a card, and the other of which is typically something memorized, such as a security code.

NERC – The **North American Electric Reliability Corporation (NERC)**, a nonprofit corporation based in Atlanta, GA, was formed on March 28, 2006, as the successor to the North American Electric Reliability Council (also known as NERC). The original NERC was formed on June 1, 1968, by the electric utility industry to promote the reliability and adequacy of bulk power transmission in the electric utility systems of North America. NERC's mission states that it is to "ensure that the bulk power system in North America is reliable."

NPCC – The Northeast Power Coordinating Council, Inc. (NPCC) is a not-for-profit corporation in the state of New York responsible for promoting and improving the reliability of the international, interconnected bulk power system in North Eastern North America.

Patch Management – A **patch** is a piece of software designed to fix problems with, or update a computer program or its supporting data. This includes fixing security vulnerabilities and other bugs, and improving the usability or performance. Patch management is the process of using a strategy and plan of what patches should be applied to which systems at a specified time.

PIN – A **personal identification number** (**PIN**) is a secret numeric password shared between a user and a system that can be used to authenticate the user to the system. Typically, the user is required to provide a non-confidential user identifier or token (the *user ID*) and a confidential PIN to gain access to the system.

Quality of Service – In the field of computer networking **Quality of Service (QoS)** is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow.

Role–based access control – In computer systems security, **role-based access control** (**RBAC**) is an approach to restricting system access to authorized users based on the role they have in an organization.

SCADA – **SCADA** stands for *supervisory control and data acquisition*. It generally refers to industrial control systems: computer systems that monitor and control industrial, infrastructure, or facility-based processes.

Separation of Duties – **Separation of duties** (SoD) is the concept of having more than one person required to complete a task. In business the separation by sharing of more than one individual in one single task shall prevent fraud and error. The concept is alternatively called segregation of duties.

Smart cards – A **smart card**, **chip card**, or **integrated circuit card** (**ICC**), is any pocket-sized card with embedded integrated circuits. Smart cards can provide strong security authentication for single sign-on (SSO) within large organizations.

Smart Grid – **Smart grids** are electricity networks that can intelligently integrate the behaviour and actions of all users connected to it - generators, consumers and those that do both – in order to efficiently deliver sustainable, economic and secure electricity supplies. A smart grid employs innovative products and services together with intelligent monitoring, control, communication, and self-healing technologies.

SSH – **Secure Shell** or **SSH** is a network protocol that allows data to be exchanged using a secure channel between two networked devices.

Steering Committee – The **Steering Committee** is that group of senior managers within the Town of Danvers responsible for the Smart Grid Implementation for the Town.

Threat – A **threat** is anything (man-made or act of nature) that has the potential to cause harm.

USB devices - The **USB mass storage device class**, otherwise known as **USB MSC** or **UMS**, is a protocol that allows a Universal Serial Bus (USB) device to become accessible to a host computing device, to enable file transfers between the two. To the host device, the USB device appears similar to an external hard drive, enabling drag-and-drop file transfers. The USB mass storage device class comprises a set of computing communications protocols defined by the USB Implementers Forum that run on the Universal Serial Bus. The standard provides an interface to a variety of storage devices.

VoIP – **Voice over Internet Protocol** (**Voice over IP**, **VoIP**) is one of a family of internet technologies, communication protocols, and transmission technologies for delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet.

VPN – A **virtual private network** (**VPN**) is a secure way of connecting to a private Local Area Network at a remote location, using the Internet or any unsecure public network to transport the network data packets privately, using encryption. The VPN uses authentication to deny access to unauthorized users, and encryption to prevent unauthorized users from reading the private network packets. The VPN can be used to send any kind of network traffic securely, including voice, video or data.

Vulnerability – A **vulnerability** is a weakness that could be used to endanger or cause harm to an informational asset.

Wireless – In telecommunications, **wireless communication** may be used to transfer information over short distances (a few meters as in television remote control) or long distances (thousands or millions of kilometres for radio communications). The term is often shortened to "wireless". It encompasses various types of fixed, mobile, and portable two-way radios, cellular telephones, personal digital assistants (PDAs), and wireless networking.

6 Records

The following records are required to support audits of compliance with this policy as it pertains to Smart Grid Information System Cyber Assets:

- Records of the review and update of this policy on an annual basis
- Records of exceptions to this policy and of the review of exceptions to this policy on an annual basis
- Records of the annual monitoring and review of the implementation of the Privacy Program within the Town of Danvers

7 Distribution

8 References

- *Town of Danvers Cyber Security Policy (i.e., DAN-SG-POL-SEC)*
- *Town of Danvers Information Protection and Management Policy (i.e., DAN-SG-POL-INP)*
- *Town of Danvers Network Security Policy (i.e., DAN-SG-POL-NET)*
- *Town of Danvers User Access Control Policy (i.e., DAN-SG-POL-UAC)*

9 Revision History

Revision ID	Date	Author	Approval (initials and date)