PASSWORD MANAGEMENT POLICY

Purpose

The password policy identifies the steps required for password use and to protect the data system and data.

Applicability

This policy applies to all users, including administrative consultants, employees, contractors, administrators, and third parties that have access to the Town Network. By using the Internet access provided, the user must agree to this policy and acknowledge that we may record and monitor records of Town user IDs and Internet access at all times with no expectation of privacy, whether using a Town computer or using their own device, but connecting though the Town Network or using Town credentials.

Scope

We believe information assets that process data electronically in conjunction with the Internet, if used properly in conducting business related purposes, can be a valuable asset. Used correctly, the Town Network can provide a wide range of information, as well as facilitate the appropriate secure transmission of business-related information efficiently.

Policy

This document provides the guidelines for establishing a culture of trust and integrity where users are committed to playing an integral part in protecting employees, administrative consultants, contractors, and partners, clients, Town Consultants, and the Town of Livermore from malicious, illegal or damaging actions, either knowingly or unknowingly. Inappropriate use exposes us to potential risks and vulnerabilities that might compromise this same data.

Internet/intranet/extranet access is granted expressly for employees and other users for the purpose of conducting approved business; computing equipment, operating systems, software, storage media, email, web browsing, FTP and network accounts are all associated with and the property of the Town of Livermore.

An effective Information Security Program requires a team effort involving the participation and support of all Town employees, administrative consultants, contractors and users who handle our information and connect to the Internet via the Town Network.

Authorized and Unauthorized Usage

Personal or incidental use is authorized for limited purposes and will be subject to the following guidelines:

- The use must not constitute a conflict of interest. Personal business or use for personal gain constitutes a conflict of interest.

- Use is on personal time (hours not charged to the Town of Livermore) and must not interfere with business or normal work activities, and must not adversely affect

performance of the employee, surrounding employees, the organization, or business functions.

- Illegal, obscene, pornographic, or offensive material must not be accessed, viewed, downloaded, or sent.

- Any access that could result in significant incremental cost, such as noticeable additional electronic mail traffic, large non-business related file transfers, and the like are not permitted.

- Use must not involve any illegal or unethical activity (e.g. gambling, Warez sites containing pirated software, movies, games, or illegal hacking/cracking tools).

- Transmitting or sending sensitive or proprietary information, including software applications or personal information, to unauthorized persons or organizations is prohibited. Authorization for any transmission of PII must be approved by a supervisor prior to transmission and done using authorized protocols (e.g. encryption, VPN, SSL).

- Downloading or sending of unapproved software, computer viruses, malicious code, or any unauthorized attempts to access another person's data or Town's intranet are prohibited.

- The addition of any hardware that would allow additional access to the Internet are prohibited.

- Users should not bring personal computers or data storage devices (such as CDs/DVDs, external hard drives, USB or flash drives, iPods, or other data storage media) to connect them to our systems without permission. Personal electronic devices are subject to inspections; if a user does not wish his or her personal computer or other devised inspected, then the user should not bring those items to work at all.

- Users may not download software from any outside systems without permission. Users should not use any externally provided software without first getting approval. Users should not download unapproved or unauthorized software from the Internet. Users are responsible for determining the sensitivity and need for further encryption to secure Town Sensitive Information or PII prior to posting, transmitting or sending it via the Internet. If unsure, the user is responsible for contacting the Administrative Assistant for assistance.

- Town websites or web servers are not to be used for posting non-business related data or for the illegal distribution of data, such as software, games, movies, code or other inappropriate data.

Privacy and Monitoring

By using the Internet access provided by the Town, users, must agree to this policy and acknowledge that records of Internet access, such as sites visited, images reviewed, and email sent, may be recorded and monitored at any time with no expectation of privacy and that:

- The Town owns the rights to all data and files in our computers, network, or other information system, subject to applicable laws. Users may not access networks, servers, drives, folders, or files to which the user has not been granted authorization. Users may not destroy, delete, erase or conceal files or other data, or otherwise make files or data unavailable or inaccessible. In addition, users may not access another employee's computer, computer files, or electronic mail without authorization.

- We license the use of certain commercial software application programs from third parties for business purposes. Third parties retain the ownership and distribution rights to this software. Users may not use or distribute licensed software.

- Electronic mail ("email") messages sent and received using our equipment or Internet access provided by us are not private and are subject to viewing, downloading, inspection, release, and archiving by us. We have the right to inspect files stored in private areas of the Town Network or on individual computers or storage media in order to assure compliance with our policies and state and federal laws. We may monitor electronic mail messages (including personal/private/instant messaging systems).

- We may use software that allows us to monitor messages, files, or other information that is entered into, received by, sent, or viewed on the Town Network. By using our equipment or Internet access provided by us, users will consent to the monitoring of all network information systems.

Electronic Mail and Instant Message Use

I. Policies and procedures governing the sharing of confidential information also apply to the sharing of information via commercial software:

II. Users are prohibited from creating or sending electronic mail

   a. That may be considered offensive or harassing, or that may contribute to a hostile environment;
   b. That contains profanity, obscenities, or derogatory remarks;
   c. That constitutes chain letters or spam
   d. To solicit or sell products or services that are unrelated to our business; or
   e. To distract, intimidate or harass anyone, or to disrupt the workplace.

III. Users are instructed to use caution when opening electronic mail and attachments from unknown senders because these pieces of electronic mail and attachments may contain viruses, root kits, spyware or malware that can put our system and sensitive information at risk.

IV. Users will be provided appropriate instructions about the proper use of IM and measures to prevent unauthorized disclosure of Town sensitive information and PII if IM is used.

Termination

- Even after termination of a user's relationship with the Town of Livermore, users are responsible for maintaining the confidentiality of Town sensitive information and PII the users may have had access to previously.

Compliance

Violations of this policy may lead to the suspension or revocation of system privileges and/or disciplinary action up to and including termination of employment. We reserve the right to advise appropriate authorities of any violation of law.

Accountability

All employees, administrative consultants, contractors, and non-employee users are responsible for the secure handling, processing, transmittal and safeguarding of Town sensitive information. This responsibility is fulfilled by the acceptable use of the Town Network and the Internet access we provide.

Third parties/vendors are responsible for ensuring their use and access to Town of Livermore and its computing resources, whether on their own information assets or on our assets, meet our security protections and safeguards and that the assets are used appropriately.

Information technology is responsible for ensuring that a user acknowledge or a non-disclosure agreement has been signed by all users acknowledging this Acceptable Use Policy before providing access to Town's sensitive computing resources.

Internal Audit is responsible for ensuring compliance with the Acceptable Use Policy and the controls created to safeguard the Town Network.

TOWN OF LIVERMORE

PASSWORD MANAGEMENT POLICY – ADOPTION

By their signatures below this policy is hereby adopted by the Board of Selectpersons.

Date: 1/12/15 **BOARD OF SELECTPERSONS**

MARK CHRETIEN, CHAIR

PETER CASTONGUAY

MEGAN DION

TIMOTHY KACHNOVICH

RODNEY NEWMAN