## Communications Policy

It is the policy of the Shrewsbury Electric & Cable Operations ("SELCO") to ensure effective business communications among all individuals within SELCO and with others outside of SELCO, in particular SELCO's clients. All forms of communication, whether verbal, written or transmitted via the electronic communications systems of SELCO shall be governed by this Policy.

### Customer Service Communications

All communications regarding SELCO or its personnel, will either originate from or be approved by SELCO prior to distribution. No individual in SELCO is to send or distribute any communication to "All Personnel" or "All Users" without prior authorization from SELCO. Managers are authorized to send or distribute communications regarding their scope of business.

**Bulletin Boards.** SELCO maintains bulletin boards, which are designated for the posting of SELCO notices. Employees are not authorized to post any form of literature, printed or written materials, or notices of any kind on SELCO's bulletin boards, without authorization in advance from SELCO. Notices will be removed and/or deleted if prior authorization has not been obtained, when they have become outdated, or when space requires removal of some notices.

**Solicitations.** To prevent disruption of business activities, to minimize distractions for all employees and to preserve SELCO security, solicitation and/or distribution of literature, materials, goods, contest promotions, requests for donations or any other solicitation and/or distribution is prohibited during working time and in work areas. Work time does not include rest periods, breaks or lunch periods. Employees are prohibited from selling or buying merchandise at any time. Persons not employed by SELCO are prohibited from soliciting employees on SELCO's premises or distributing materials on SELCO's premises at any time for any purpose.

**Workplace Environment.** SELCO is committed to maintaining a working environment free from all forms of abuse and unlawful harassment. Use of SELCO's electronic communication systems to download, reproduce, send or forward messages that threaten violence, or that contain abusive, vulgar, offensive or discriminatory messages is prohibited. Among those which are considered offensive are any messages that contain overt sexual language, sexual implications or innuendo or comments that offensively address someone's age (as defined by law), gender, race, sexual orientation, religious beliefs, transgender status, gender identity, national origin, genetic information, military status or disability.

Harassing or discriminatory comments may be deemed inappropriate in violation of this Policy even if SELCO's name or the names of any of its employees are not posted in the comment. Employees of SELCO are responsible for the content of all text, audio or images that they place or send over the Internet and for ensuring that the Internet is used in an effective, ethical and lawful manner. The transmission or downloading of any sexually explicit materials including abusive, profane or offensive language or images is prohibited. As noted above, SELCO reserves the right to access and monitor all messages and files as it deems necessary and appropriate.

**Effective Business Communications.** While e-mail and voicemail may be the quickest and easiest way to communicate, it may not always be the most appropriate or effective way to communicate when managing or conducting SELCO's business. Employees of SELCO should avoid using e-mail when the message that must be communicated involves extremely important, confidential or sensitive internal customer service center matters (e.g., discussions regarding an employee's work performance

or a candidate's application for employment). Such communications, including dialogues that call for extensive back-and-forth discussion, are best held in person or on the phone.

**Confidential/Proprietary/Trade Secret and Copyrighted Information.** Users of SELCO's electronic communications systems and devices are prohibited from sending externally any confidential, proprietary and/or trade secret information without prior authorization by SELCO. Illegal duplication of software is prohibited. Copyright holders are granted exclusive rights, including the right to make and distribute copies of their copyrighted material. Users are, therefore, prohibited from copying, sending or receiving copyrighted material belonging to a third party without prior authorization by SELCO, with the exception to make a backup of software for archival purposes. In addition, use of electronic communication systems and devices, in particular cell phones, to discuss SELCO confidential, proprietary or trade secret information must be done with caution so as to eliminate the possibility of a breach of confidentiality or the inadvertent disclosure of such information.

## Electronic Communication and Information Security

This policy states acceptable usage for SELCO technology. It is intended to be in compliance with all Commonwealth of Massachusetts and the United States federal regulatory laws, policies, and guidelines. The policy applies to all aspects of computer technology that is owned, maintained, distributed, and/or provided by SELCO. It applies to all internal users of SELCO systems, and all users of public access equipment that SELCO has provided.

Staff should make themselves acquainted with this policy, do their best to adhere to these guidelines, and request additional information or training as they require.

**Computer Use** The following standards relate to the use of SELCO computers, devices, information systems and networks. This encompasses all computers, laptops, phones, tablets and peripherals that are owned by SELCO. All devices and network resources are the property of SELCO and should be used for appropriate business purposes. Standards of use of the computer and network resources are outlined as follows:

1. Only SELCO owned devices may be directly connected to the network (AKA hard-wired). All purchases must be approved by the General Manager or the Chief Information Officer. No devices may be moved, altered or removed without authorization.
2. Software piracy is a crime, and cannot be tolerated. All employees will adhere to the licensing agreements or network subscription agreements entered into by SELCO. Only authorized copies of software may be used on computers, and employees shall not operate with unlicensed software that has been copied illegally. Employees shall not use SELCO computers to illegally copy licensed software. Employees shall not use SELCO licensed software on their own personally owned devices unless the license agreement allows that, and the installation has been approved.
3. All virus protection, Internet filtering and security controls that have been installed on town computers must remain active at all times. Any attempts to bypass any of these controls is a violation of this policy. Any addition of other virus software without authorization will also be considered a violation of this policy.

4. All data, documents, and files should be stored on common (network) drives to ensure files and data are properly protected and backed up on a regular basis. Employees should limit their use of their computer's local hard drive to temporary storage only. In either case, only business related data and files should be stored on SELCO computer systems. This applies to any cloud account for data storage under SELCO's control.
5. It is strictly forbidden to help anyone other than authorized SELCO employees or identified vendors in gaining access to, or using the resources of, the SELCO network.

**Internet Acceptable Use.** The following standards relate specifically to accessing the Internet via the SELCO computer network. Internet browsing capability is extended to SELCO employees requiring information that may be accessed via the Internet. Additionally "guest" access to the Internet is provided in some SELCO buildings for use by the public, or by employees using their own personally owned devices.

1. Employees may use the Internet for professional activities, to accomplish job related activities, and to gather business and industry related information that may assist the employee in completing his/her job related responsibilities.
2. Filters have been put in place to protect SELCO systems from virus software, and to exclude non business access. If as part of their job, an employee needs access to an Internet resource that has been blocked, that employee's manager can request for that filter to be removed.
3. A wireless "Guest" access network has been provided in some SELCO buildings. This network is intended to allow minimal access for employees and the public to the Internet. This network is extremely limited in speed and highly filtered for content. All users of this network must agree to all terms and conditions of the SELCO's policies, and may only use this network temporarily. Employees who bring their personally owned devices to work may use this network.
4. Employees who wish to have their personally owned devices connected to the SELCO network must only do so for work related use. They may request this in writing via their manager.

**Remote Access Acceptable Use.** The following standards relate to accessing the SELCO computer network remotely for employees who need remote access to SELCO systems as part of their normal job functions.

- Employees who require remote access to our system must request access via their manager. This access must be documented, and follow the security protocols and software as outlined by the Chief Information Officer.
- Employees should not use third-party services (e.g. LogMeIn, GoToMyPC, PC Anywhere, etc.) to access their desktop computers, PCs, Servers, or other network devices without approval from the General Manager or the Chief Information Officer.
- Employees should be familiar with the risks inherent to using a public wife such as a hotel, library or cafe. These should be avoided, unless the proper software protections are taken.

**Data and Information Security.** Our Computer systems are used to store a great deal of data. Some of this data falls under the Commonwealth guidelines for "personal information" (201 CMR 17.00) and therefor is deserved of certain protections. As per the Commonwealth, personal information is defined as a Massachusetts resident's first name (or first initial) and last name in combination with any one or more of the following:

- Social Security Number
- Driver's License Number
- State-issued Identification Card Number
- Financial Account Number
- Credit or Debit Card Number (with or without any required security codes)
- Passport Number

Also as per the Commonwealth, the above information must be secured whether recorded digitally or not. Paper notes, photo copies and even carbon inserts are covered under the law (and this policy).

Employees may have access to the above listed personal information. It's extremely important that you familiarize yourself with this policy, and be aware of how to protect this data.

**Password and Access Control Policy.** The following standards relate to password security for accessing SELCO systems. This applies to domain accounts, email, cloud resources, applications and systems.

- All employees will be issued a unique login credential. Shared accounts are strongly discouraged.
- Password complexity rules apply; upper and lower case, numbers, and greater than 8 characters.
- Employees should protect their passwords and user ID from unauthorized use, and never share their login ID or password with anyone.
- Passwords may not be written down and should not be transmitted via email or over the phone.
- Passwords for work should be unique; employees should not reuse passwords for their personal access at home on work accounts (and vice versa).

Password protection is the cornerstone of both system security and data integrity. Employees should protect their passwords at all times. Report any password issues to management immediately

**Email Policy.** Electronic mail (Email), Text messaging (txt) and voicemail (VM) are provided to the employees to both increase productivity and the dissemination of information. The employee must maintain a level of business decorum at all times when using these medium.

The following standards relate to the use of SELCO email system, but also extend to the use of messaging apps embedded within SELCO systems (such as the List Serve on our Website). These standards are intended to assist the employee in using these tools, as well as protecting SELCO systems and personal information

The email system is the property of, and controlled by, SELCO. Employees have no expectation of privacy using this system.

1. Emails are considered public record, and may be discoverable via a public records request. All emails are archived and kept in compliance with public records retention polices.
2. SELCO management may perform automated filtering of emails to detect the disclosure, unauthorized access, or misuse of personal information as defined by 201 CMR 17.00.
3. Staff are prohibited from sending any personal information as deemed by 201 CMR 17.00 via email, text, IM, or other electronic medium that is not fully encrypted a password protected.
4. Staff are discouraged from using their municipal email address for any organization for personal reasons.

Employees should not open any link, attachment, video clip, photo, jpeg non business email all unsolicited email should be treated with the utmost caution. Report any email issues or potential breaches to management immediately.

**Mobile and Portable Storage Policy.** This policy addresses the use of portable or mobile storage devices within SELCO. This includes (but is not limited to), USB drives, phones or tablets (when used as direct data storage connected to a PC), external hard drives, and memory stick devices in any format.

Mobile devices often represent a threat to security depending upon their source. Drives from questionable sources may often carry malware or other malicious code. Even "clean" drives used on the SELCO system may be infected if exposed to another computer. That drive may then infect our system when plugged back in here. External drives should be treated with particular caution.

1. Use only those devices or drives approved and purchased by IT on SELCO Equipment.
2. All external devices should be protected with a security PIN code or otherwise encrypted. This will protect the content of the data on that device.
3. SELCO external drives should not be "shuttled" between SELCO and Non-SELCO computers (to prevent cross contamination if the non-SELCO device is infected).
4. GREAT CARE should be given to the nature of the data stored on a portable drive; data defined as "personal Information (as per 201 CMR 17:00) SHOULD NOT be stored on any removable media.

The confidentiality and integrity of SELCO customer and employee data is paramount. Report the theft, loss, damage or any other potential data concerns to management immediately.

**Mobile Device (Phone/Tablet) Policy.** The approval of use of mobile devices is at the discretion of the General Manager and may be revoked at any time. Managers will be responsible to justify the cost benefit to the organization.

1. All mobile devices connected in any way to our system must provide all full identification and contact information; IE phone number, model number, etc.
2. A secure connection should be used at all times when connecting to our network. Avoid if possible accessing from a public unsecured connection.

3. All users of mobile devices agree to use their devices in accordance with all policies, state laws, ordinances, bylaws, and acceptable use guidelines. Particular traffic laws while driving.

The confidentiality and integrity of SELCO customer, Town, and Employee data is paramount. Report the theft, loss, damage or any other potential data concerns from mobile devices to management immediately.

*Please note, the loss or theft of a SELCO owned device may require a Police Incident Report.*

**Data Incident Response Plan.** This policy outlines the response plan to any potential data breach, issue, disclosure or other potential risk. If there is a potential loss of data, TIME IS OF THE ESSENCE. Report any potential issues to your supervisor immediately. You or your supervisor should immediately notify SELCO IT and document the issue by sending an email ticket to Tech Support.

When reporting a potential security incident, it is vital to provide as much information as possible.

1. Description of the incident, stolen laptop, malware, lost USB, etc.
2. Date and time the incident occurred
3. Potential witnesses, if any
4. Location of the incident
5. Severity/Volume of the data lost.
6. Potential business or customer impact.
7. What (if any) protective controls were in place,

**Data Communications and Security Policy Acknowledgement.** Employees will be briefed on the policy on an annual basis. New hires will be given this policy as part of their orientation. Employees will be required to sign an acknowledgement of the data communications and security policy.

I, the undersigned, hereby acknowledge that I have read, understand, and will abide by the above data communications and security policy.

Signed:_____ Date: _____