METRO
SOUTH
CHAMBER OF
COMMERCE

DATA PROTECTION & PRIVACY POLICY 2010 - 2011

UNITED STATES CHAMBER OF COMMERCE
ACCREDITED®
★ ★ ★ ★ ★

Metro South Chamber of Commerce
Sixty School Street, Brockton, MA 02301, 508-586-0500, fax 508-587-1340
www.metrosouthchamber.com

TABLE OF CONTENTS

Privacy Policy & Data Protection

Privacy Statement

The Metro South Chamber of Commerce is committed to protecting the privacy of our members' personal information, as well as to visitors of the Chamber website at www.metrosouthchamber.com. Information collected will be used strictly for analytics and not for user invasion or distribution of information. This Statement of Privacy serves to outline our policies and how we store and handle information provided by the user, member, customer or visitor.

Massachusetts Data Security Law

As of March 1, 2010, Massachusetts enacted a strict data security law 201 CMR 17.00, requiring every person (business) who owns or licenses personal information about a resident of the Commonwealth to implement and to document an Information Security Program that is compliant with the new regulations. As such, the Chamber adheres to the strict Data Protection Laws. **See Appendix A for the Chamber's Security Policy and WISP (Written Information Security Program).**

Collection of Personal Information

The Metro South Chamber of Commerce automatically collects information about users experience on the website as they read pages, perform searches, and download information. The information does not identify the user personally. It is used to learn more about our visitors, popular content and the types of technology our visitors use. The following information is collected:

- The Internet domain and IP address from which the user accesses the Chamber Website
- The type of browser and operating system used to access our site
- The date and time of access
- The pages visited
- If the user linked to our website from another website

The Metro South Chamber of Commerce does not enable "cookies" to monitor use of the Chamber website.

Please keep in mind that if you disclose personally identifiable information or personally sensitive data via a message board or social media site such as Facebook, Twitter or the Chamber Ning site, the information may be collected and used by others. The Chamber is not responsible for any information shared in this manner.

Merchant Accounts

The Chamber utilizes iCommerceGateway and Plug and Pay Technologies, Inc., as its merchant account vendor. The following statement is listed at checkout:

NOTICE: It is the policy of Plug & Pay Technologies, Inc. to respect the privacy of its customers and the people doing business through its service. As such all information presented here WILL NOT be sold or distributed to any party other than the merchant you have currently elected to do business with.

The Chamber also uses an SSL (Security Socket Layer) digital certificate provider (iCommerce Gateway), providing our Members the strongest certificate services available. When credit card information is transmitted, industry standard encryption is used. **For full statement, see Appendix B.**

Information Users Supply

The Metro South Chamber of Commerce will collect information about members annually through the Chamber Verification Form Process. Any information supplied, including names, addresses and websites will be made available to the public on the Chamber Online Member Directory. Members are welcome to login and change information at anytime. Email addresses will not be distributed unless consent has been received. If a user submits information through an online form containing personal information, we may use the information to respond, however the personal information will not be collected or stored. Business addresses and phone numbers are distributed as a form of referral to community members calling and requesting information about a type of business. Member addresses are also distributed in the form of mailing labels to Chamber members, however may not be duplicated or sold. Members are encouraged to contact the Chamber if they choose not to be listed in the online or book directory and do not want their mailing addresses revealed to others.
For Mailing Label Agreement, see Appendix C.

Links to Other Sites

The Metro South Chamber of Commerce website contains links to other agencies and associations of regional interest that support the mission of the Chamber. This does not however, mean that we endorse their policies or products. Once you have connected to another website from the Chamber website, you are subject to the privacy policy of that new site.

Site Security

We ensure that our website remains available to all users by using a computer system that employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage. The Metro South Chamber of Commerce secures personally identifiable information provided in a controlled, secure environment, protected from unauthorized access, use or disclosure. When personal information, such as a credit card, is entered, it is protected through the use of encryption.

Email Listserv

The Chamber requests email addresses and business names to enter into our Constant Contact Listserv. Distribution lists include the E-Update, 10 Things Around the Corner Community Event blast, Higher Education list, Connecting Activities list, and Government Affairs Updates. Members may opt in or out of different distribution lists. The Chamber tracks the rate of emails opened, as well as which members have opened certain links. This information may be used for marketing purposes, as well as for the distribution of information to advertisers. The service is CAN-SPAM Act compliant. Every email generated contains an unsubscribe link which allows subscribers to opt-out of future emails. In addition, the Chamber eUpdate subscribers list is not sold or distributed. **For the Constant Contact Privacy Policy, see Appendix D.**

Designated Information Security Manager

Christopher Cooney, The President & CEO at the Chamber of Commerce is our Information Security Manager (ISM). He keeps the Written Information Security Plan updated, trains staff in compliance, and audits staff compliance.

Protection and Disposal of Paper Records That Contain Personal Information (PI)

All paper records that have PI are locked in cabinets in the Controller's office which is also locked at the end of the day. We destroy obsolete records using an office-grade shredder. When we receive checks from customers, we scan them and keep a copy in a computer directory that can only be accessed by the Controller. The checks are kept under lock and key until they are deposited in the bank.

Restricted Employment Records

Paper employment records are kept under lock and key, and accessed only by the staff responsible for employment issues which are the Controller and the President/CEO.

Password Policy

Chamber computer passwords are changed every 90 days to ensure that data is protected remotely and on the server. Passwords must be at least 6 characters. The past 2 cycles of passwords may not be reused.

Securing Our Network

Our computer network is a Secure Network. We follow the advice of our Technology Consultant, Wright Technology. As such our Firewall has Gateway security services and is reviewed at least annually. Passwords are changed when staff leaves. Our Wireless is encrypted at least 128bit. Login Passwords and multiple attempt lockout is used. Antivirus software is kept up to date both in version and in signatures. When a staff person leaves our organization, all passwords that person used are changed. The person also returns any keys used to physically secure personal information

Personal Information on Portable Devices

The Metro South Chamber of Commerce does not keep personal information on laptops, or other handheld or portable devices. We store backups on external hard drives and flash drives, encrypted with Strong Passwords using Strong Encryption.

Chamber Privacy Protection Contracts with Employees/Outside Users

The Metro South Chamber has created a Data Protection for Employees/Internet Rules Contract **(see Appendix E)** employees sign upon joining the staff of the Chamber, as well as an Internet Access Policy for tenants **(see Appendix F)**.

If a Breach Occurs

If our Information Security Manager (ISM) determines that PI has been accessed without authorization, she will notify the Office of Consumer Affairs & Business Regulation (OCABR) and the Attorney General's Office, describing the theft in detail, and work with authorities to investigate the crime and to protect the victim's identity and credit. To the extent possible, our ISM will also warn the victims of the theft so that they can protect their credit and identity.

APPENDIX A
Security Policy (WISP)

I. POLICY

A. It is the policy of the Metro South Chamber of Commerce (MSCC) that information, as defined hereinafter, in all its forms--written, spoken, recorded electronically or printed--will be protected from accidental or intentional unauthorized modification, destruction or disclosure throughout its life cycle. This protection includes an appropriate level of security over the equipment and software used to process, store, and transmit that information.

B. All policies and procedures must be documented and made available to individuals responsible for their implementation and compliance. All activities identified by the policies and procedures must also be documented. All the documentation, which may be in electronic form, must be retained for at least 6 (six) years after initial creation, or, pertaining to policies and procedures, after changes are made. All documentation must be periodically reviewed for appropriateness and currency, a period of time to be determined by each entity within the MSCC.

C. At each entity and/or department level, additional policies, standards and procedures will be developed detailing the implementation of this policy and set of standards, and addressing any additional information systems functionality in such entity and/or department. All departmental policies must be consistent with this policy. All systems implemented after the effective date of these policies are expected to comply with the provisions of this policy where possible. Existing systems are expected to be brought into compliance where possible and as soon as practical.

II. SCOPE

A. The scope of information security includes the protection of the confidentiality, integrity and availability of information.

B. The framework for managing information security in this policy applies to all Metro South Chamber entities and workers, and other Involved Persons and all Involved Systems throughout the Metro South Chamber as defined below in **INFORMATION SECURITY DEFINITIONS.**

C. This policy and all standards apply to all protected health information and other classes of protected information in any form as defined below in **INFORMATION CLASSIFICATION.**

III. RISK MANAGEMENT

A. A thorough analysis of all MSCC information networks and systems will be conducted on a periodic basis to document the threats and vulnerabilities to stored and transmitted information. The analysis will examine the types of threats – internal or external, natural or manmade, electronic and non-electronic-- that affect the ability to manage the information resource. The analysis will also document the existing vulnerabilities within each entity which potentially expose the information resource to the threats. Finally, the analysis will also include an evaluation of the information assets and the technology associated with its collection, storage, dissemination and protection.

From the combination of threats, vulnerabilities, and asset values, an estimate of the risks to the confidentiality, integrity and availability of the information will be determined. The frequency of the risk analysis will be determined at the entity level.

B. Based on the periodic assessment, measures will be implemented that reduce the impact of the threats by reducing the amount and scope of the vulnerabilities.

IV. INFORMATION SECURITY DEFINITIONS

Affiliated Covered Entities: Legally separate, but affiliated, covered entities which choose to designate themselves as a single covered entity for purposes of HIPAA.

Availability: Data or information are accessible and usable upon demand by an authorized person.

Confidentiality: Data or information is not made available or disclosed to unauthorized persons or processes.

HIPAA: The Health Insurance Portability and Accountability Act, a federal law passed in 1996 that affects the healthcare and insurance industries. A key goal of the HIPAA regulations is to protect the privacy and confidentiality of protected health information by setting and enforcing standards.

Integrity: Data or information has not been altered or destroyed in an unauthorized manner.

Involved Persons: Every worker at MSCC -- no matter what their status. This includes employees, contractors, consultants, temporaries, volunteers, interns, etc.

Involved Systems: All computer equipment and network systems that are operated within the MSCC environment. This includes all platforms (operating systems), all computer sizes (personal digital assistants, desktops, mainframes, etc.), and all applications and data (whether developed in-house or licensed from third parties) contained on those systems.

Protected Health Information (PHI): PHI is health information, including demographic information, created or received by the MSCC entities which relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual and that identifies or can be used to identify the individual.

Risk: The probability of a loss of confidentiality, integrity, or availability of information resources.

V. INFORMATION SECURITY RESPONSIBILITIES

A. **Information Security Officer:** The Information Security Officer (ISO) for each entity is responsible for working with user management, owners, custodians, and users to develop and implement prudent security policies, procedures, and controls, subject to the approval of MSCC. Specific responsibilities include:

1. Ensuring security policies, procedures, and standards are in place and adhered.
2. Providing basic security support for all systems and users.
3. Advising owners in the identification and classification of computer resources.
4. Advising systems development and application owners in the implementation of security controls for information on systems, from the point of system design, through testing and production implementation.
5. Educating custodian and user management with comprehensive information about security controls affecting system users and application systems.
6. Providing on-going employee security education.
7. Performing security audits.
8. Reporting regularly to the MSCC Executive Committee on entity’s status with regard to information security.

B. **Information Owner (President & CEO):** The owner of a collection of information is usually the manager responsible for the creation of that information or the primary user of that information. This role often corresponds with the management of an organizational unit. In this context, ownership does not signify proprietary interest, and ownership may be shared. The owner may delegate ownership responsibilities to another individual by completing the MSCC Information Owner Delegation Form. The owner of information has the responsibility for:

1. Knowing the information for which she/he is responsible.
2. Determining a data retention period for the information, relying on advice from the Legal Department.

3. Ensuring appropriate procedures are in effect to protect the integrity, confidentiality, and availability of the information used or created within the unit.
4. Authorizing access and assigning custodianship.
5. Specifying controls and communicating the control requirements to the custodian and users of the information.
6. Reporting promptly to the ISO the loss or misuse of MSCC information.
7. Initiating corrective actions when problems are identified.
8. Promoting employee education and awareness by utilizing programs approved by the ISO, where appropriate.
9. Following existing approval processes within the respective organizational unit for the selection, budgeting, purchase, and implementation of any computer system/software to manage information.

C. **Custodian (Wright Technology):** The custodian of information is generally responsible for the processing and storage of the information. The custodian is responsible for the administration of controls as specified by the owner. Responsibilities may include:

1. Providing and/or recommending physical safeguards.
2. Providing and/or recommending procedural safeguards.
3. Administering access to information.
4. Releasing information as authorized by the Information Owner and/or the Information Privacy/ Security Officer for use and disclosure using procedures that protect the privacy of the information.
5. Evaluating the cost effectiveness of controls.
6. Maintaining information security policies, procedures and standards as appropriate and in consultation with the ISO.
7. Promoting employee education and awareness by utilizing programs approved by the ISO, where appropriate.
8. Reporting promptly to the ISO the loss or misuse of MSCC information.
9. Identifying and responding to security incidents and initiating appropriate **actions when problems are identified.**

D. **User Management (President & CEO):** MSCC management who supervise users as defined below. User management is responsible for overseeing their employees' use of information, including:

1. Reviewing and approving all requests for their employees access authorizations.

2. Initiating security change requests to keep employees' security record current with their positions and job functions.

3. Promptly informing appropriate parties of employee terminations and transfers, in accordance with local entity termination procedures.

4. Revoking physical access to terminated employees, i.e., confiscating keys, changing combination locks, etc.

5. Providing employees with the opportunity for training needed to properly use the computer systems.

6. Reporting promptly to the ISO the loss or misuse of MSCC information.

7. Initiating corrective actions when problems are identified.

8. Following existing approval processes within their respective organization for the selection, budgeting, purchase, and implementation of any computer system/software to manage information.

E. **User (Staff):** The user is any person who has been authorized to read, enter, or update information. A user of information is expected to:

1. Access information only in support of their authorized job responsibilities.

2. Comply with Information Security Policies and Standards and with all controls established by the owner and custodian.

3. Refer all disclosures of PHI (1) outside of MSCC and (2) within MSCC, other than for treatment, payment, or health care operations, to the applicable entity’s Medical/Health Information Management Department. In certain circumstances, the Medical/Health Information Management Department policies may specifically delegate the disclosure process to other departments. (For additional information, see MSCC Privacy/Confidentiality of Protected Health Information (PHI) Policy.)

4. Keep personal authentication devices (e.g. passwords, SecureCards, PINs, etc.) confidential.

5. Report promptly to the ISO the loss or misuse of MSCC information.

6. Initiate corrective actions when problems are identified.

VI. INFORMATION CLASSIFICATION

Classification is used to promote proper controls for safeguarding the confidentiality of information. Regardless of classification the integrity and accuracy of all classifications of information must be protected. The classification assigned and the related controls applied are dependent on the sensitivity of the information. Information must be classified according to the most sensitive detail it includes. Information recorded in several formats (e.g., source document, electronic record, report) must have the same classification regardless of format. The following levels are to be used when classifying information:

A. **Protected Health Information (PHI)**

1. PHI is information, whether oral or recorded in any form or medium, that:

   a. is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university or health clearinghouse; and

   b. relates to past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past present or future payment for the provision of health care to an individual; and

   c. includes demographic data, that permits identification of the individual or could reasonably be used to identify the individual.

2. Unauthorized or improper disclosure, modification, or destruction of this information could violate state and federal laws, result in civil and criminal penalties, and cause serious damage to MSCC and its patients or research interests.

B. **Confidential Information**

1. Confidential Information is very important and highly sensitive material that is not classified as PHI. This information is private or otherwise sensitive in nature and must be restricted to those with a legitimate business need for access.

   Examples of Confidential Information may include: personnel information, key financial information, proprietary information of commercial research sponsors, system access passwords and information file encryption keys.

2. Unauthorized disclosure of this information to people without a business need for access may violate laws and regulations, or may cause significant problems for MSCC, its customers, or its business partners. Decisions about the provision of access to this information must always be cleared through the information owner.

C. **Internal Information**

1. Internal Information is intended for unrestricted use within MSCC, and in some cases within affiliated organizations such as the MSCC Foundation. This type of information is already widely-distributed within MSCC, or it could be so distributed within the organization without advance permission from the information owner.

   Examples of Internal Information may include: personnel directories, internal policies and procedures, most internal electronic mail messages.

2. Any information not explicitly classified as PHI, Confidential or Public will, by default, be classified as Internal Information.

3. Unauthorized disclosure of this information to outsiders may not be appropriate due to legal or contractual provisions.

D. **Public Information**

1. Public Information has been specifically approved for public release by a designated authority within each entity of MSCC. Examples of Public Information may include marketing brochures and material posted to MSCC entity internet web pages.

2. This information may be disclosed outside of MSCC.

VII. COMPUTER AND INFORMATION CONTROL

All involved systems and information are assets of MSCC and are expected to be protected from misuse, unauthorized manipulation, and destruction. These protection measures may be physical and/or software based.

A. **Ownership of Software:** All computer software developed by MSCC employees or contract personnel on behalf of MSCC or licensed for MSCC use is the property of MSCC and must not be copied for use at home or any other location, unless otherwise specified by the license agreement.

B. **Installed Software:** All software packages that reside on computers and networks within MSCC must comply with applicable licensing agreements and restrictions and must comply with MSCC acquisition of software policies.

C. **Virus Protection:** Virus checking systems approved by the Information Security Officer and Information Services must be deployed using a multi-layered approach (desktops, servers, gateways, etc.) that ensures all electronic files are appropriately scanned for viruses. Users are not authorized to turn off or disable virus checking systems.

D. **Access Controls:** Physical and electronic access to PHI, Confidential and Internal information and computing resources is controlled. To ensure appropriate levels of access by internal workers, a variety of security measures will be instituted as recommended by the Information Security Officer and approved by MSCC. Mechanisms to control access to PHI, Confidential and Internal information include (but are not limited to) the following methods:

1. **Authorization:** Access will be granted on a "need to know" basis and must be authorized by the immediate supervisor and application owner with the assistance of the ISO. Any of the following methods are acceptable for providing access under this policy:

a. *Context-based access:* Access control based on the context of a transaction (as opposed to being based on attributes of the initiator or target). The "external" factors might include time of day, location of the user, strength of user authentication, etc.

b. *Role-based access:* An alternative to traditional access control models (e.g., discretionary or non-discretionary access control policies) that permits the specification and enforcement of enterprise-specific security policies in a way that maps more naturally to an organization's structure and business activities. Each user is assigned to one or more predefined roles, each of which has been assigned the various privileges needed to perform that role.

c. *User-based access:* A security mechanism used to grant users of a system access based upon the identity of the user.

2. **Identification/Authentication:** Unique user identification (user id) and authentication are required for all systems that maintain or access PHI, Confidential and/or Internal Information. Users will be held accountable for all actions performed on the system with their user id.

a. At least one of the following authentication methods must be implemented:

1. **strictly** controlled passwords (Attachment 1 – Password Control Standards),

2. biometric identification, and/or

3. tokens in conjunction with a PIN.

b. The user must secure his/her authentication control (e.g. password, token) such that it is known only to that user and a designated security manager (President & CEO). The President & CEO will maintain a master list of user names and passwords and keep them locked up.

c. An automatic timeout re-authentication must be required after a certain period of no activity (maximum 15 minutes).

d. The user must log off or secure the system when leaving it.

3. **Data Integrity:** MSCC must be able to provide corroboration that PHI, Confidential, and Internal Information has not been altered or destroyed in an unauthorized manner. Listed below are some methods that support data integrity:

a. transaction audit

b. disk redundancy (RAID)

c. ECC (Error Correcting Memory)

d. checksums (file integrity)

e. encryption of data in storage

f. digital signatures

4. **Transmission Security:** Technical security mechanisms must be put in place to guard against unauthorized access to data that is transmitted over a communications network, including wireless networks. The following features must be implemented:

    a. integrity controls and

    b. encryption, where deemed appropriate

5. **Remote Access:** Access into MSCC network from outside will be granted using MSCC approved devices and pathways on an individual user and application basis. All other network access options are strictly prohibited. Further, PHI, Confidential and/or Internal Information that is stored or accessed remotely must maintain the same level of protections as information stored and accessed within the MSCC network. This will be maintained and supervised by Wright Technology Group.

6. **Physical Access:** Access to areas in which information processing is carried out must be restricted to only appropriately authorized individuals.

    The following physical controls must be in place:

    a. Mainframe computer systems must be installed in an access-controlled area. The room in which the server is located is locked at night for security. The area in and around the computer facility must afford protection against fire, water damage, and other environmental hazards such as power outages and extreme temperature situations. The server will be backed up off-site.

    b. File servers containing PHI, Confidential and/or Internal Information must be installed in a secure area to prevent theft, destruction, or access by unauthorized individuals.

    c. Workstations or personal computers (PC) must be secured against use by unauthorized individuals. Local procedures and standards must be developed on secure and appropriate workstation use and physical safeguards which must include procedures that will:

        1. Position workstations to minimize unauthorized viewing of protected health information.

        2. Grant workstation access only to those who need it in order to perform their job function.

        3. Establish workstation location criteria to eliminate or minimize the possibility of unauthorized access to protected health information.

        4. Employ physical safeguards as determined by risk analysis, such as locating workstations in controlled access areas or installing covers or enclosures to preclude passerby access to PHI.

5. Use automatic screen savers with passwords to protect unattended machines.

d. Facility access controls must be implemented to limit physical access to electronic information systems and the facilities in which they are housed, while ensuring that properly authorized access is allowed. Local policies and procedures must be developed to address the following facility access control requirements:

1. Contingency Operations – Documented procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

2. Facility Security Plan – Documented policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

3. Access Control and Validation – Documented procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

4. Maintenance records – Documented policies and procedures to document repairs and modifications to the physical components of the facility which are related to security (for example, hardware, walls, doors, and locks).

7. **Emergency Access:**

a. Each entity is required to establish a mechanism to provide emergency access to systems and applications in the event that the assigned custodian or owner is unavailable during an emergency.

b. Procedures must be documented to address:

1. Authorization,

2. Implementation, and

3. Revocation

E. **Equipment and Media Controls:** The disposal of information must ensure the continued protection of PHI, Confidential and Internal Information. Each entity must develop and implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain PHI into and out of a facility, and the movement of these items within the facility. The following specification must be addressed:

1. **Information Disposal / Media Re-Use of:**

   a. Hard copy (paper and microfilm/fiche)

   b. Magnetic media (floppy disks, hard drives, zip disks, etc.) and

   c. CD ROM Disks

2. **Accountability:** Each entity must maintain a record of the movements of hardware and electronic media and any person responsible therefore.

3. **Data backup and Storage:** When needed, create a retrievable, exact copy of electronic PHI before movement of equipment.

F. **Other Media Controls:**

1. PHI and Confidential Information stored on external media (diskettes, cd-roms, portable storage, memory sticks, etc.) must be protected from theft and unauthorized access. Such media must be appropriately labeled so as to identify it as PHI or Confidential Information. Further, external media containing PHI and Confidential Information must never be left unattended in unsecured areas.

2. PHI and Confidential Information must never be stored on mobile computing devices (laptops, personal digital assistants (PDA), smart phones, tablet PC's, etc.) unless the devices have the following minimum security requirements implemented:

   a. Power-on passwords

   b. Auto logoff or screen saver with password

   c. Encryption of stored data or other acceptable safeguards approved by Information Security Officer

   Further, mobile computing devices must never be left unattended in unsecured areas.

3. If PHI or Confidential Information is stored on external medium or mobile computing devices and there is a breach of confidentiality as a result, then the owner of the medium/device will be held personally accountable and is subject to the terms and conditions of MSCC Information Security Policies and Confidentiality Statement signed as a condition of employment or affiliation with MSCC.

H. **Data Transfer/Printing:**

1. **Electronic Mass Data Transfers:** Downloading and uploading PHI, Confidential, and Internal Information between systems must be strictly controlled. Requests for mass downloads of, or individual requests for, information for research purposes that include PHI must be approved through the Internal Review Board (IRB). All other mass downloads of information must be approved by the Application Owner and include only the minimum amount

of information necessary to fulfill the request. Applicable Business Associate Agreements must be in place when transferring PHI to external entities (see MSCC policy B-2 entitled “Business Associates”).

2. **Other Electronic Data Transfers and Printing:** PHI, Confidential and Internal Information must be stored in a manner inaccessible to unauthorized individuals. PHI and Confidential information must not be downloaded, copied or printed indiscriminately or left unattended and open to compromise. PHI that is downloaded for educational purposes where possible should be de-identified before use.

I. **Oral Communications:** MSCC staff should be aware of their surroundings when discussing PHI and Confidential Information. This includes the use of cellular telephones in public areas. MSCC staff should not discuss PHI or Confidential Information in public areas if the information can be overheard. Caution should be used when conducting conversations in: semi-private rooms, waiting rooms, corridors, elevators, stairwells, cafeterias, restaurants, or on public transportation.

J. **Audit Controls:** Hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use PHI must be implemented. Further, procedures must be implemented to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. These reviews must be documented and maintained for six (6) years.

K. **Evaluation:** MSCC requires that periodic technical and non-technical evaluations be performed in response to environmental or operational changes affecting the security of electronic PHI to ensure its continued protection.

L. **Contingency Plan:** Controls must be in place and ensure that MSCC can recover from any damage to computer equipment or files within a reasonable period of time. Each entity is required to develop and maintain a plan for responding to a system emergency or other occurrence (for example, fire, vandalism, system failure and natural disaster) that damages systems that contain PHI, Confidential, or Internal Information. This will include developing policies and procedures to address the following:

1. Data Backup Plan:

a. A data backup plan must be documented and routinely updated to create and maintain, for a specific period of time, retrievable exact copies of information.

b. Backup data must be stored in an off-site location and protected from physical damage.

c. Backup data must be afforded the same level of protection as the original data.

2. **Disaster Recovery Plan:** A disaster recovery plan must be developed and documented which contains a process enabling the entity to restore any loss of data in the event of fire, vandalism, natural disaster, or system failure.
3. **Emergency Mode Operation Plan:** A plan must be developed and documented which contains a process enabling the entity to continue to operate in the event of fire, vandalism, natural disaster, or system failure.
4. **Testing and Revision Procedures:** Procedures should be developed and documented requiring periodic testing of written contingency plans to discover weaknesses and the subsequent process of revising the documentation, if necessary.
5. **Applications and Data Criticality Analysis:** The criticality of specific applications and data in support of other contingency plan components must be assessed and documented.

Compliance [§ 164.308(a)(1)(ii)(C)]

A. The Information Security Policy applies to all users of MSCC information including: employees, students, volunteers, and outside affiliates. Failure to comply with Information Security Policies and Standards by employees, medical staff, volunteers, and outside affiliates may result in disciplinary action up to and including dismissal in accordance with applicable MSCC procedures, or, in the case of outside affiliates, termination of the affiliation. Failure to comply with Information Security Policies and Standards by students may constitute grounds for corrective action in accordance with MSCC procedures. Further, penalties associated with state and federal laws may apply.

B. Possible disciplinary/corrective action may be instituted for, but is not limited to, the following:

1. Unauthorized disclosure of PHI or Confidential Information as specified in Confidentiality Statement.
2. Unauthorized disclosure of a sign-on code (user id) or password.
3. Attempting to obtain a sign-on code or password that belongs to another person.
4. Using or attempting to use another person's sign-on code or password.
5. Unauthorized use of an authorized password to invade patient privacy by examining records or information for which there has been no request for review.
6. Installing or using unlicensed software on MSCC computers.
7. The intentional unauthorized destruction of MSCC information.
8. Attempting to get access to sign-on codes for purposes other than official business, including completing fraudulent documentation to gain access.

--- ATTACHMENT 1 ---

Password Control Standards

MSCC Information Security Policy requires the use of **strictly** controlled passwords for accessing Protected Health Information (PHI), Confidential Information (CI) and Internal Information (II). (See MSCC Information Security Policy for definition of these protected classes of information.)

Listed below are the minimum standards that must be implemented in order to ensure the effectiveness of password controls.

Standards for accessing PHI, CI, II:

Users are responsible for complying with the following password standards:

1. Passwords must never be shared with another person, unless the person is a designated security manager.
2. Every password must, where possible, be changed regularly – (between 45 and 90 days depending on the sensitivity of the information being accessed)
3. Passwords must, where possible, have a minimum length of six characters.
4. Passwords must never be saved when prompted by any application with the exception of central single sign-on (SSO) systems as approved by the ISO. This feature should be disabled in all applicable systems.
5. Passwords must not be programmed into a PC or recorded anywhere that someone may find and use them.
6. When creating a password, it is important not to use words that can be found in dictionaries or words that are easily guessed due to their association with the user (i.e. children's names, pets' names, birthdays, etc…). A combination of alpha and numeric characters are more difficult to guess.

Where possible, system software must enforce the following password standards:

1. Passwords routed over a network must be encrypted.

2. Passwords must be entered in a non-display field.

3. System software must enforce the changing of passwords and the minimum length.

4. System software must disable the user identification code when more than three consecutive invalid passwords are given within a 15 minute timeframe. Lockout time must be set at a minimum of 30 minutes.

APPENDIX B:
Privacy & Security Statement for Plug & Pay Technologies, Inc.

Plug and Pay Technologies, Inc. (PnP) has created this privacy statement in order to demonstrate our firm commitment to privacy and security and to clearly define these standards to our customers and the community we serve. We have established these policies to protect the security and privacy of the information we collect In addition to these policies, we maintain strict internal policies against unauthorized disclosure or use of customer information. Security protocols have been implemented to restrict access to information according to job responsibility.

Any suspected attempt to breach our policies and procedures, or to engage in any type of unauthorized action involving our information systems, is regarded as potentially criminal activity, and all suspected computer mischief is reported to the appropriate authorities.

The following discloses our information gathering and dissemination practices for this website(s) identified by the domain name: plugnpay.com.

Definitions:

Merchants – Merchants are defined as direct customers of Plug & Pay Technologies, Inc. to whom PnP provides a service.

Consumers – Consumers are defined as customers of Merchant and end users of the service PnP provides to Merchant.

For Merchants:

We use the IP address of both Merchant to help diagnose problems with our server, and to administer our Web site.

We use cookies to keep track of referral information.

Our site's registration form requires users to give us contact information (like their name and email address). We use Merchant contact information from the registration form to send the Merchant information about our company.

The Merchant's contact information is also used to contact the visitor when necessary.

Users may opt-out of receiving future mailings; see the choice/opt-out section below.

Financial information that is collected is used to check the users' qualifications for registration and to bill the user for products and services.

We do not share/sell or in anyway distribute Merchant data with any other companies.

This policy does not preclude PnP unrestricted use of non-personal, summarized, derived, or aggregate information (i.e., volumes, totals, averages, etc.).

For Consumers:

We use the IP address of Consumers to help diagnose problems with our server, and to administer our Web site.

We use the IP address of Consumers to help identify their shopping cart.

We use cookies to keep track of shopping cart contents, and/or referral information.

Our site uses an order form for Consumers to request information, products, and services. We collect Consumer's contact information (like their email address) and financial information (like their account or credit card numbers). Contact information from the order form is used by the Merchant to send products, information and fulfill orders.

The Consumer's contact information may also be used to get in touch with the Consumer if necessary to solve a problem. Users may opt-out of receiving future mailings; see the choice/opt-out section below.

Financial information that is collected is used to check the users' qualifications and bill the user for products and services ordered by Consumer from Merchants.

We do not share/sell or in anyway distribute Consumer data with any other companies (apart from the Merchant(s) we are acting as agents for in providing our Service to Consumer).

This policy does not preclude PnP unrestricted use of non-personal, summarized, derived, or aggregate information (i.e., volumes, totals, averages, etc.).

Security

This site has security measures in place to protect the loss, misuse and alteration of the information under our control. Security of information in transit to and from our web site is encrypted using SSL encryption protocols. We store all user information in secure databases protected via a variety of access controls as well as using encryption of sensitive information. This data is accessed only for the purposes specified in this privacy statement.

Children

We do not provide content on our Web sites which are intended to attract or encourage the participation of children. We do not solicit or knowingly accept information from persons under the age of 18.

Choice/Opt-Out

This site gives users the following options for removing their information from our database to not receive future communications or to no longer receive our service.

1. You can send email to support@plugnpay.com

Change/Modify

This site gives users the following options for changing and modifying information previously provided.

1. email support@plugnpay.com

Your responsibility

As a customer of PnP, you may be provided with a unique identifier such as a username and password which is intended to authenticate your identity when accessing our systems. Such identifying items are intended to be secret and to be known, possessed, and used only by you. The effectiveness of these mechanisms for authenticating your identity are dependent upon your keeping them in your exclusive possession and upon your protecting them from the discovery, access, or possession of others. If you fail to keep such identifying information in your exclusive possession (i.e., you allow others to have knowledge or possession of your password or pin), you may bear responsibility for the actions of other persons who use this information in accessing our systems.

Should you become aware or have reason to suspect that a PnP personal identifier has been lost or has been disclosed to someone other than yourself, you should immediately notify PnP Technical Support at support@plugnpay.com.

APPENDIX C

MAILING LABELS/MEMBERSHIP DIRECTORY
PROTECTION AGREEMENT

ON BEHALF OF ____, I AM ACCEPTING THE METRO SOUTH CHAMBER OF COMMERCE MAILING LABELS/MEMBERSHIP DIRECTORY. A COPY OF THE PRINTED MATERIAL THAT YOUR COMPANY PLANS TO MAIL MUST BE SUBMITTED TO THE CHAMBER WITH THIS AGREEMENT. ANY MAILING OR PHONE SOLICITATIONS ARE NOT TO:

- CONTAIN ANY REFERENCE TO THE CHAMBER EITHER IN THE SALUTATION OR IN THE TEXT (SUCH AS: "DEAR CHAMBER MEMBER, AS A CHAMBER MEMBER" ETC.)

- BE DUPLICATED OR SOLD IN ANY MANNER

- BE DISTRIBUTED OR SOLD IN ANY MANNER

THE METRO SOUTH CHAMBER OF COMMERCE MAILING LABELS ARE PROPRIETARY AND ARE PURCHASED FOR ONE-TIME USAGE ONLY.

PAYMENT TO BE RECEIVED WITH PLACEMENT OF ORDER.

AMOUNT ENCLOSED $150.00

AUTHORIZED SIGNATURE____

FIRM/ORGANIZATION NAME____

ADDRESS____

DATE_________________________TELEPHONE_______________________________

APPENDIX D

Constant Contact Email Privacy Policy

The security of our site is managed on multiple levels including Physical, Network, Host, Software, and User Account Security.

Constant Contact maintains internal security policies and procedures in support of its ongoing operations. Access to resources is granted only to those who reasonably require access based on their responsibilities.

Physical Security:

Physical access to our machines is restricted to specific individuals and uses multiple levels of security, including:

- The equipment hosting Constant Contact's services is located in physically secure facilities. Access to these facilities is limited to authorized personnel. Badge access and biometric authentication (hand scanners and fingerprint IDs) are required in order to access the facilities.
- Constant Contact equipment is isolated and secured in spaces reserved for Constant Contact equipment only, spaces are not shared with 3rd parties.
- Access to hosting environments is regularly reviewed to ensure authorization.
- Security guards perform random checks of facilities hosting Constant Contact equipment to ensure physical security controls have not been compromised.

Network Security:

- Access to Constant Contact's services is via standard HTTP and HTTPS connections.
- Constant Contact's hosting environment is protected from the public Internet via multiple and distinct firewalls, and monitored with a network-based commercial intrusion detection system.
- All of your account, credit card, and subscriber information and content is encrypted via industry-standard Secure Sockets Layer (SSL) connections over HTTPS. Users may consult their web browser's address or location bar to determine if the currently accessed page is encrypted via SSL.

Host Security:

- Constant Contact undergoes industry-standard security hardening efforts on all systems. In accordance with our security and change management policies, unused services are disabled and software updates are applied on a regular basis.
- Constant Contact regularly reviews information on current security vulnerabilities, including vendor announcements and other industry sources. If security updates are determined to be critical to the Constant Contact environment, they are thoroughly tested and deployed in a timely manner.

- All hosts and services are routinely monitored for integrity and availability. Operations staff review all alerts generated by monitoring systems, and respond promptly.
- Our servers are monitored 24x7 for malicious activity.
- Administrative access to Constant Contact infrastructure is limited to strictly authorized users. Individual usernames and passwords are required for all machine and data access.
- Strong password guidelines are in place, including complexity and minimum length requirements. Passwords are expired and changed on a regular basis.

Software Security:

- All internally developed code is subject to a strict Quality Assurance program, including extensive testing of functionality and business logic. Strong change control processes are in place to ensure that all code deployed to the production environment has been appropriately reviewed.
- Constant Contact regularly undergoes security reviews, including external and internal scanning for vulnerabilities on an ongoing basis by a 3rd party vendor. All vulnerabilities discovered are reviewed by internal security and addressed according to severity.

User Account Security:

- User-level access to Constant Contact services is provided via a username and password selected by the end user.
- Passwords and credit card numbers are encrypted.
- User account setup, maintenance, and termination are under the control of the end user.

APPENDIX E

Data Protection for Employees/Internet Rules

Computer Systems; E-Mail; Voicemail

As a user of a personal Computer, as well as other technologies within the Chamber, you will be held accountable to the Code of Conduct as described below. While employees are encouraged to use this technology, its use carries important responsibilities and guidelines for use. The intent of this policy is to (1) insure that we protect the significant investment that we are making in technology and (2) that we manage this technology in a way that allows us to provide adequate levels of support to our users. Suggestions for improvements are always welcome and will be considered for Chamber wide implementation.

- Employees are responsible for protecting their own passwords. Sharing user ID's, passwords, and account access codes or numbers is prohibited. Employees will be held responsible for misuse that occurs through such unauthorized access.

- Fraudulent, harassing, threatening, discriminatory, sexually explicit or obscene messages and/or materials are not to be transmitted, printed, requested, or stored. "Chain letters", solicitations, and other forms of mass mailing are not permitted. Such conduct will result in disciplinary action up to and including termination.

- Introducing unauthorized software and/or software designed to destroy or corrupt the company's computer system with viruses or cause other harmful effects is prohibited and will result in disciplinary action up to and including termination.

- Employee passwords are required for access but do not guarantee confidentiality of files or voice mail messages. In fact, use and access may be monitored and tracked by management at any time.

- Employees are reminded that all the information contained in our systems is confidential and must only be used for Chamber related purposes.

Management Information Systems contracted services will be retained to perform the following functions, unless some other individual or entity is otherwise authorized by the President/CEO:

No attempt should be made to log onto any on-line service provider other than the officially authorized Internet service provider.

The Metro South Chamber of Commerce retains the right, without prior notice, to access, review, preserve, and/or destroy any and all data entered into its computer system and is the sole proprietor of any and all data entered into its e-mail, voicemail, and computer systems.

The user of information systems is a privilege extended by the Chamber, which may be withdrawn at any time. An employee's use of computer systems may be suspended immediately upon the discovery of a possible violation of these policies. A violation of the provisions of this policy may result in disciplinary action up to and including termination.

ACKNOWLEDGMENT

I acknowledge that I have received and read the Metro South Chamber of Commerce Email Protection/Privacy Policy.

I understand that the policies and procedures outlined are designed to provide guidance and are not contractual obligations and may be changed at any time deemed necessary to meet the needs of the effective operation of the Chamber.

Employee Signature___________________________

Date_______________________________________

(Please complete and return to the President/CEO.)

APPENDIX F:

Privacy Policy for Web-Based Data Collection and Management

Internet Access and MSCC Tenant Network

The Metro South Chamber of Commerce (MSCC) provides computer access to the Internet to its employees and tenants to enhance communication, operations and to help provide quality services to clients. All users must remember that the MSCC network, including access to the Internet and other systems which enhance communication are MSCC assets provided for use by employees and tenants to assist them in conducting their business. This equipment and the information and work product they contain are MSCC property. MSCC networks including access to the Internet are for business purposes, not for more than incidental personal use, and should not be misused. Examples of misuse include, but are not limited to jokes or materials derogatory to any protected class, developing chain letters, making defamatory statements, inappropriate disclosure of confidential information, unauthorized access or permitting unauthorized access, etc.

To ensure compliance with this policy, the use of networks and Internet are subject to monitoring and review on a periodic basis and as otherwise deemed appropriate by MSSC. At any time and without prior notice, MSCC may examine Internet traffic, firewall logs and other information stored on or passing through MSCC network. MSCC may also log web sites visited, files downloaded, time spent on the Internet, and related information.

In addition, in order to maintain an efficient and virus free network environment, MSCC recommends each tenant have Antivirus software installed and regularly updated.

In addition, individuals should report all potential misuse of MSCC network and Internet access to Christopher Cooney, President and CEO.

Tenants violating this policy may lose access to MSCC Internet access.

- ***Offensive or Harassing Use Prohibited***. The electronic mail and Internet/LAN systems are not to be used to create or distribute any offensive or disruptive messages. Among those that are considered offensive are messages or material that contains sexual implications, racial or ethnic slurs, or other comments that offensively address someone’s age, sex, sexual orientation, religion, national origin, ancestry or disability. In addition, the system must not be used to communicate other improper messages, for example, messages or material that is defamatory, derogatory, obscene or otherwise inappropriate. The electronic mail and Internet/LAN systems must not be used to commit any crime, including but not limited to sending obscene emails over the Internet with the intent to annoy, abuse, threaten, or harass another person.
- ***Compliance with the Law***. The MSCC system shall not be used to commit any crime and shall comply with all state, federal and local laws and regulations.

- ***No Sexually Explicit Sites***. MSCC's Internet system must not be used to visit sexually explicit or otherwise offensive or inappropriate Web sites, or to send, display, download or print offensive material, pornographic or sexually explicit pictures or any other materials which would be found offensive by most reasonable people. Content filters which are designed to disrupt access to these materials must not be bypassed or altered.

- ***Solicitation Prohibited and/or Restricted***. The electronic mail and Internet/LAN systems may not be used to solicit or proselytize for outside or personal commercial ventures, religious or political causes, outside organizations, or other solicitations that are not job-related. MSCC may at a time of its choosing provide access to a public electronic bulletin board system which will facilitate voluntary participation in non business related messages and other transactions. Otherwise, any mass electronic message which is not related to the direct business of MSCC should have prior approval from the President and CEO before being sent. Fund-raising and other messages for Non-Profits may be permitted per approval of the President and CEO.

- ***Chain Letters***. Employees must not send or forward "chain letter" e-mails.

- ***Viruses.*** Employees may not use MSCC e-mail or Internet systems to develop or send any virus or otherwise destructive programs. Employees should not open e-mails or attachments unless they are confident of the identity of the sender and the content of any attachments. MSCC may make available virus protection software when allowed by the licensing vendor.

- ***Copyrighted Material and Trade Secrets.*** The electronic mail and Internet/LAN systems must not be used to send (upload) or receive (download) copyrighted materials, trade secrets, proprietary financial information, or similar materials without proper authorization. Popular peer to peer based sharing systems such as Napster, Gnutella, Kazaa, etc., **may not be used** to transmit or receive copyrighted material. **Any attempt to bypass current bandwidth management systems is strictly prohibited.**

- ***Right to Monitor***. MSCC reserves and intends to exercise the right to review, audit, intercept, access and/or disclose any and all traffic in the system, including messages or material, including attachments created, received or sent, web sites visited and/or files downloaded over the college's electronic mail or Internet/LAN systems. Authorized representatives of the college may monitor the use of its systems in its sole discretion, at any time, with or without notice to any employee and may by-pass any password. Such monitoring is capable of tracking and recording e-mail messages sent and received as well as web sites visited by employees.