APICS SOUTHWEST MICHIGAN CHAPTER (SWMI) CHAPTER STANDARD OPERATING PROCEDURE	
Position: Data Privacy	**Document No: SOP0060 Data Protection & Privacy Policy**
Original Issue Date: 10/02/2012	**Issued By: VP of Membership**
Last Revised Date: 10/02/2012	**Revised By: Board of Directors**

1. **Purpose And Scope**
    a. To establish and maintain a Private and Sensitive Data protection policies in the Southwest Michigan and affiliated chapters

2. **References**
    a. **Data Privacy:** The expectation of careful and ethical use of personal information only in ways **known and acknowledged** by the individual
    b. **Data Security:** The practices employed through people, process and technology to protect information and to minimize the potential of a security compromise
    c. **Personal Data / Persona Identifiable information (PII)**: Any information that identifies or can reasonably, contact, or locate the individual to whom the information pertains. Data may be in electronic, hard copy machine readable or any other format and may include sensitive personal information.
    d. **Sensitive Data/ Sensitive Personal Information (SPI)**: Any data that pertains to racial or ethnic origins, political or religious beliefs, or health or sex life, or as otherwise defined in national laws where the individual resides.

3. **Policy**

APICS Southwest Michigan Chapter operates under the auspices of APICS in Southwest Michigan and has registered members in surrounding states and potentially other countries as its members are deployed internationally. As a membership organization, APICS Southwest Michigan Chapter is required to collect certain types of personal information from or about members under national law and wants to take advantage of technology to more efficiently administer member benefits. APICS Southwest Michigan Chapter Member and Board Websites represent an effort to leverage technology to better serve its membership, its affiliated chapters and its commitments to APICS.

APICS Southwest Michigan Chapter Member Data Privacy

To maintain the security of its membership data, APICS Southwest Michigan Chapter has created a Data Privacy Policy. This Policy provides information on the types of personal information being processed, the purpose of processing and the categories of potential recipients. This Policy intends to create awareness among Board Members, Volunteers and any entity with access to the information about the following:

- Collection of Membership Data
- Processing of Membership Data
- Transfer of Membership Data
- Use of Membership Data

The chapter adheres to the following principles while handling personal data:

- Fairness and Lawfulness
- Adequacy, Relevancy and Accuracy
- Limited Use, Disclosure
- Data Security
- Destruction
- Access
- Onward Transfer
- Enforcement
- Accountability

Data Security and Data Privacy:

- Data security and data privacy has a widespread impact potentially affecting nearly everyone in an organization
- Data security and data privacy are **related but not identical**
- Data security is defined as the defense of informational assets from the following threats:
    - Natural disasters, such as earthquake, fire, or damage from storm and flood
    - System, such as breakdown, malfunction, or disoperation of systems
    - People, such as misbehavior or unauthorized operation
- Data security promotes the preservation of the following three basic fundamental requirements:
    - Confidentiality: To protect sensitive information from unauthorized disclosure
    - Integrity: To protect the accuracy and completeness of information and computer software
    - Availability: Ensure that information and vital services are available to the chapter when required
- Data security is a prerequisite of effective data privacy, but it does not assure it
- Data privacy is the expectation of careful and ethical use of personal information only in ways known and acknowledged by the individual
- The purpose of data privacy is to provide protection to the individual whose data is being processed
- Data privacy is achieved through a combination of:
    - Rights of the individual
    - Obligations of people and organizations that process data or exercise control over such processing
- The ability of individuals to determine when, how and to what extent information about them is used or disclosed is key to maintaining the appropriate level of data privacy

Personal Identifiable Information (PII) and Sensitive Personal Information (SPI)

- Personal data contains both PII and SPI
- PII is any information that identifies or can reasonably be used to identify, contact, or locate the individual to whom such information pertains
- Examples of such information include an individual’s name in conjunction with:
    - Home or business address
    - Telephone number
    - E-mail address
    - Other data elements that reflect the individual's physical, social or financial characteristics

- To safeguard PII and SPI, APICS Southwest Michigan Chapter is required to minimize the collection, processing, storage and transfer of PII and SPI where possible unless necessary for the business
- Minimization reduces the associated risks and will positively impact other areas, such as auditing of access to PII and SPI requirements
- While APICS Southwest Michigan Chapter recognizes that different countries have different laws for the protection of data; given its regional / Southwest Michigan scope it will observe all laws of the United States of America and the States of Michigan.

Controls and Information Security

- The Executive Committee of the APICS Southwest Michigan Chapter is responsible for ensuring that service providers, hosts and personal computers used by board members are set to:
    - o Provide technical controls through equipment and software (examples anti-virus, etc.)
    - o Administrative controls are implemented via policies procedures and standards (examples include: password standards)
    - o Vendors/hosts of the chapter information have the correct perimeter security, detective controls, preventive controls, and corrective controls.
- The VP of Membership and Regional Chapter Representatives are responsible for the restrictions and ensuring only those entitles to access PII have access and are trained on privacy policies and are subject to an authorization process.
- The Web Master / Technology officer/ Information Technology (IT) at APICS Southwest Michigan Chapter undertakes the monitoring of systems and the review and update of technical, administrative and operational data security measures regarding PII and SPI on a regular basis
- IT then advises the organization about the effectiveness of the existing data security measure used at APICS Southwest Michigan Chapter, implements upgrades, and minimizes the potential for security lapses

Chapter Officers / Directors at Large Obligations:

- APICS Southwest Michigan Chapter Volunteer Board Members at all levels should understand their responsibilities for management of their own PII and SPI, and shared responsibilities for appropriately handling and safeguarding sensitive PII and SPI they may encounter

- Every APICS Southwest Michigan Chapter Volunteer Board Member has a responsibility to understand the HR Data Security and Privacy Policy and standards

- Every APICS Southwest Michigan Chapter Volunteer Board Member has a responsibility to understand any contractual security and privacy requirements with which they are working

Revision Box

Requests for changes to this document must be made in writing to the issuing and approving authority together with documentation on which to base the review and approval. Listed below is the record of changes for this document. Revision level and approval of revisions are recorded on title page.				
Rev	Date	Page	Paragraph	Nature of change
0	09/27/2012	All	All	New Document