PMI PHOENIX CHAPTER
POLICY STATEMENT

Technology Policy

Approved by Board of Directors on: 3/25/19

Purpose

This policy statement addresses technology issues of the PMI Phoenix Chapter. It applies to all members of the Board of Directors and all member volunteers.

Responsibilities

Serving on the Board of Directors or other leadership position is an honor and carries with it the responsibility for ethical behavior on and off the job. The constituents of PMI Phoenix Chapter rely on the members of the Board of Directors and other volunteers to: act in the chapter's best interests; to be knowledgeable about and proactive on the issues facing the organization and the industry; to base decisions on reliable and factual information; to be good stewards of the organization's resources; and to be honest and trustworthy in all actions. This policy has been adopted by PMI Phoenix Chapter to codify those expectations around technology and to ensure they are clearly understood. All members of the Board of Directors are responsible for implementing the provisions of this policy and for ensuring that member volunteers on their teams understand and abide by it as well.

Parameters

- *The technology of the chapter* – The Chapter's technology consists of its physical electronic assets as well as its Chapter data, including member data, and access to PMI and Chapter online resources.
- *Credit and debit cards* – The Chapter and the third party that provides the chapter's website and web hosting services do not store anyone's debit or credit card numbers. When members and non-members alike register for chapter sponsored events, they do so through the Chapter's gateway and merchant services provider. The Chapter and its website do not acquire or store debit or credit card numbers for any reason, ever.

Policy

- The Chapter will never acquire or store debit or credit card numbers for any reason.
- Only members of the Chapter can be authorized to have access to Chapter technology.
- Access to Chapter technology (physical assets, online data sources, and chapter data) must be granted in writing by a member of the Board of Directors. A written authorization to have access to, and use, Chapter technology must come from the Board member who is sponsoring the member. It should be in email format with a copy to the VP Operations. It should: (1) list the specific assets that are included in the authorization and (2) emphasize that Chapter technology is only to be used for chapter activities.
- The authorizing Board member and the VP Operations will jointly maintain a copy of active authorizations on a shared folder in SharePoint / Board of Directors. Authorizations may be terminated by either the sponsoring Board member or the VP Operations at any time. Authorizations will be automatically rescinded as part of the deboarding process.
- Board members who grant access to chapter technology are responsible for ensuring that Chapter technology is used appropriately by those to whom they have granted access.
- Chapter volunteers who have been granted the use of physical assets will maintain such assets with reasonable care. Such persons must be able to produce such assets for a random

inspection at the discretion of the Vice President of Operations and/or the sponsoring Board member.

- In the event there is a breach of security of any type involving a credit / debit card reader that belongs to the Chapter or, if it is learned that a Chapter member is collecting and storing debit or credit card numbers, the Chapter member who learns of the breach must immediately report it to a Board member. The Board member is then responsible for immediately reporting the breach to the Chapter's President and VP Finance who will then notify the bank and the local police department of the issue. If the name and location of the person who obtained credit card data without authorization are known, then the VP Finance must also report the breach to the police department in that city.