

ORGANIZATIONAL POLICY

June 30, 2009 (v3)



ONLINE INFORMATION ACCESS

Each member of the Board of Directors is authorized to access and view certain confidential and sensitive information about the administration and operation of the HSCG. In addition, employees, contractors and some others may be authorized to access certain information.

The following details cover who is authorized and for what, and who is responsible for keeping access up-to-date.

ONLINE ACCOUNTING SOFTWARE

The Executive Director shall be designated as the "Account Owner".

Every current member of the Board of Directors and HSCG staff as designated by the Executive Director, shall have access to view all HSCG financial information in a report format, but not to add, edit or delete transactions.

The President, Executive Director, Office Manager and CPA on retainer shall have unrestricted access to create, edit and delete transactions as necessary in the course of their jobs. The Board of Directors may grant other uses unrestricted access as necessary.

The Executive Director is responsible for adding or removing users as needed when Board Members start or end their terms, or at other times as appropriate.

MERCHANT SERVICES

The Executive Director shall be designated as the "Account Owner" and as such shall have full administrative rights. The Executive Director may assign limited or full access rights to others for the purpose of viewing information or processing credit card payments as needed.

HSCG WEBSITE ADMIN AREA

The Executive Director, Office Manager and Webmaster shall have access to all sections the HSCG Admin Area, including the ability to assign or remove the access rights of others. HSCG Staff shall have access to all sections of the HSCG website, with the exception of the ability to assign or remove the access rights of others.

The President and all members of the Board of Directors shall have basic viewing rights and may be assigned additional access as needed.

Others, including Local Chapter board members, volunteers, committee members and contractors, may be assigned access to specific areas at the discretion of the Office Manager or Executive Director.

WEB SERVICES

The Webmaster shall be the account owner of any web services utilized by the HSCG Website and Blog, such as domain registrations, blog plugins, hosting services, etc. The Webmaster shall provide the login details and site information to the Office Manager on a regular basis.

EMAIL ACCOUNTS

Email accounts and forwarders shall be assigned and managed by the Office Manager.

FINANCIAL & HUMAN RESOURCES ACCOUNTS

The Executive Director shall be the “owner” of the account.

The President, Office Manager and Executive Director shall have access to the account. Additional access may be authorized by the Board of Directors as needed.

PROJECT MANAGEMENT SERVICES

The HSCG may use a third party project management service such as Basecamp.

All Board Members shall have normal access to most areas of any project management service, including all committee spaces, with the exception of any spaces used for deliberations by the Nominating Committee or Ethics Committee.

Employees, contractors, and/or volunteers be granted access to limited areas of any project management service by the Executive Director.

SOCIAL MEDIA ACCOUNTS

The Executive Director shall be the “owner” of all Social Media accounts .

The Executive Director may provide access to certain individuals to manage such accounts or represent the HSCG on social media platforms. See HSCG Policy *Social Media* for details

PRIVACY AND SECURITY

It is the responsibility of every person who has access to online HSCG information to keep the information secure. Login credentials information or downloaded files containing private information stored on a personal computer or device must be kept secure and password protected. Care must be taken when a browser password manager is used and automatically fills in login credentials.

Any documents printed which contain personal information about members and, particularly, credit card or financial information should be shredded, burned or otherwise disposed of properly. Electronic documents that are “deleted” must be permanently deleted, not left in a “recycle bin” where they can be accessed and recovered.

In the event that a person no longer has authority access to a particular online service, the person in charge of granting access must immediately remove the user from the service and/or change any login credentials associated with the account. For example, if the person assigned to access Facebook to post for the HSCG is changed, then the username and/or password should be changed so the previous

person assigned can no longer access that account. The person who no longer has access must delete all references to the account and login credentials , as well as any files or downloads, from any computer used to access the service.

The HSCG Policies *Board Protocol* and *Privacy Policy* apply to all on-line information viewed, saved to personal computers of devices and/or printed.

RECORDS

The Office Manager is responsible for keeping a permanent, hardcopy record of:

- ◆ All online services and accounts with their users and login credentials
- ◆ All email accounts used, with login credentials
- ◆ All email forwarders assigned

It is the responsibility for all online account owners to provide updated information to the Office Manager when login credentials are changed.

The Office manager must keep the information secure, such as in a locked cabinet. The Executive Director must have unrestricted access to the online access information.

Approved by the Board of Directors
June 30, 2009

History:

- June 30, 2009 (v1) Original Publication Date
- October 7, 2013 (v2) Amended to include name changes, including post titles. Removed HSMG Member Forum section, revised Basecamp section and added Social Media section
- March 20, 2018 (v3) Revised to update Online Accounting (previously "Quickbooks"), Project Management (previously "Basecamp"), Web Services, Email, HR sections, and Records section and to include additional security requirements.; Reformat to new branding.