California Men's Gatherings Terms of Use for Computer and Information Systems

Preamble

The California Men's Gatherings (CMG) as an organization maintains systems for use by volunteers, leaders, and the public to forward the mission of the organization. This Terms of Use document outlines the responsibilities users of those systems have and the responsibilities the organization has for information security.

If you have additional questions or require more information about these Terms of Use, do not hesitate to contact us.

Consent

The California Men’s Gatherings promote and encourage responsible use of the systems and information that it has provided to users. By using our systems, you hereby consent to use these systems In the manner outlined and agree to its terms. Nothing in this policy can supersede or conflict with applicable laws nor the terms outlined by the providers with whom it contracts.

Scope

It is the collective responsibility of all users to ensure the confidentiality, integrity, and availability of information assets owned, leased, or entrusted to the CMG and to use CMG assets in an effective, efficient, ethical, and legal manner. These systems may not be physically accessible to users but are most often accessed through a user’s personal computer or device. These terms of use shall apply regardless of the medium in which the systems are accessed and may include technology facilities, applications, hardware systems and network resources owned or managed by the CMG.

The purpose of these principles is to provide a frame of reference for user responsibilities and to promote the ethical, legal, and secure use of CMG resources for the protection of all members of the CMG community.

General Principles

Use of CMG information assets shall be consistent with the mission and core values of the CMG, applicable laws, regulations, and policies. All users are required to help maintain a safe computing environment by notifying CMG of known vulnerabilities, risks, and breaches involving its information assets. The CMG makes information assets and services accessible in order to meet the needs of its volunteers, leadership and the general public.

All users, including those with expanded privileges (e.g., system administrators and service providers), shall respect the privacy of person-to-person communications in all forms including telephone, electronic mail and file transfers, graphics, and video. The CMG respects freedom of expression in electronic communications on its computing and networking systems. Although this electronic speech has broad protections, all users are expected to use the information technology facilities considerately with the understanding that the electronic dissemination of information may be available to a broad and diverse audience including those outside the organization.

Other than designated administrators, the CMG does not generally monitor or restrict content residing on its systems or transported across its networks; however, the CMG reserves the right to use appropriate means to safeguard its data, preserve network and information system integrity, and ensure continued delivery of services to users. These activities are not intended to restrict, monitor, or use the content of legitimate personal and organizational communications.

In the normal course of system and information security maintenance, both preventive and troubleshooting, system administrators and service providers may be required to view files and monitor content on the CMG networks, equipment, or computing resources. These individuals shall maintain the confidentiality and privacy of information unless otherwise required by law. The CMG recognizes and acknowledges that use of its computing and network resources for personal use and any personal data that may be stored on its systems shall be treated as private.

User Responsibilities

Users are expected to use good judgment and reasonable care in order to protect and preserve the integrity of CMG equipment, its data and software, and its access. Users must not use or access CMG information assets in a manner that conflicts with its mission; violates applicable laws, regulations, contractual agreements, or standards or causes damage to or impairs CMG information assets or the productivity of other users through intentional, negligent, or reckless action.

Software: Users must take reasonable precautions to avoid introducing harmful software, such as viruses, into CMG computing and networking systems. Users must take reasonable precautions to ensure their personal and/or provided devices (e.g., computers, tablets, smart phones) are secure before connecting to CMG information assets. Users must promptly report the loss or theft of any device, which grants access to a CMG system regardless of ownership or electronic information (passwords or other credentials) to CMG resources.

Published Information: Users who publish or maintain information on CMG information assets are responsible for ensuring that the information they post complies with applicable laws, regulations, policies concerning copyrighted material and fair use of intellectual property. Software must be used in a way that is consistent with the relevant license agreement. Unauthorized copies of licensed or copyrighted software may not be created or distributed.

Email & Stored Files: Users must not browse, monitor, alter, or access email messages or stored files in another user's account unless specifically authorized by the user. However, such activity may be permitted by an administrator with approval of an executive committee member to comply with applicable law, regulations or under the guidance of law enforcement or legal counsel.

User Credentials: Users who act as a custodian of credentials, such as a username and password, that permit access to a CMG information system or network resource is responsible for all activity initiated by the user and performed under his/her credentials. The user shall assist in the investigation and resolution of a security incident regardless of whether the activity occurred without the user's knowledge and because of circumstances outside his or her control.

Users must take reasonable steps to appropriately protect their credentials from becoming known by or used by others. Users who have been authorized to use a password-protected account must follow established procedures for setting, maintaining, and changing passwords. With exception of system administrators, users are prohibited from using or attempting to use the account to access, modify, or destroy any information assets for which a user is not normally authorized, from disclosing passwords to any party or including passwords in documentation, or embedding passwords in software code.

Third Party Transmission: Except for publicly accessible CMG information assets, users must not transfer or provide access to CMG information assets to outside individuals or groups without proper authorization. Users of CMG information assets must not purposefully misrepresent their identity, either directly or by implication, with the intent of using false identities for inappropriate purposes.

Personal Use: CMG assets are provided to further the mission of the organization by its members, volunteers, and leaders. Personal or non-CMG business use is acknowledged and permissible to the extent allowed by service providers and provided that such use doesn't violate the law, interfere with operation, maintenance or use of its assets, does not oppose its mission or core values, and does not result in a loss to the organization.

CMG Responsibilities

The CMG has broad responsibilities with respect to protecting its information assets. These include but are not limited to controlling access to information, responding to and addressing information security incidents, complying with laws and regulations, and ensuring the logical and physical security of the underlying technology used to store and transmit information.

The CMG gives broad discretion to users as to whether communication or data information is to be saved in their account storage or to make it available as shared information to others in the organization. Officers of the organization particularly have both an interest in maintaining privacy of records, being transparent about their activities and transferring of information to a succeeding office holder. When users choose to collaborate on documents they may share those files to others with credentials in the organization or outside users and guests who are contributing to documentThe CMG retains ownership or stewardship of information assets owned (or managed) by or entrusted to the CMG. The CMG reserves the right to limit access to its information assets and to use appropriate means to safeguard its data, preserve network and information system integrity, and ensure continued delivery of services to users. This can include but is not limited to: monitoring communications across network services; monitoring actions on information systems; checking information systems attached to the network for security vulnerabilities; disconnecting information systems that have become a security hazard; or, restricting data to/from information systems and across network resources. These activities are not intended to restrict, monitor, or utilize the content of legitimate organizational communications.

Enforcement

The CMG respects the rights of its members, volunteers, and leaders. Any enforcement of these terms should uphold the dignity of individuals to the extent possible and must comply with appropriate laws and regulations. The CMG reserves the right to temporarily or permanently suspend, block, or restrict access to information assets, when it reasonably appears necessary to do so to protect the confidentiality, integrity, availability, or functionality of CMG resources or to protect the organization from liability. The CMG may also refer suspected violations to appropriate law enforcement agencies.

How to Contact Us

You may contact the California Men's Gatherings

By mail: 1049 Havenhurst Dr., Unit #123, West Hollywood, CA 90046

By email: question@thecmg.org

Or by using any of the submission forms under "Contact the CMG" on our website.