The Scientific Consulting Group, Inc. Acceptable Use Policy

1.0 Overview

The Scientific Consulting Group, Inc.'s (SCG) intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to SCG's established culture of openness, trust and integrity. SCG is committed to protecting SCG's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and FTP, are the property of SCG. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers, in the course of normal operations.

Effective security is a team effort involving the participation and support of every SCG employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at SCG. These rules are in place to protect the employee and SCG. Inappropriate use exposes SCG to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at SCG, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by SCG.

4.0 Policy

4.1 General Use and Ownership

1. While SCG's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of SCG. Because of the need to protect SCG's network, management cannot guarantee the confidentiality of information stored on any network device belonging to SCG.
2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
3. For security and network maintenance purposes, authorized individuals within SCG may monitor equipment, systems and network traffic at any time.
4. SCG reserves the right to audit networks and systems on a periodic basis and at any time to ensure compliance with this policy.

4.2 Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly, user level passwords should be changed every six months. Passwords should have at least 6 characters and include numbers or other characters rather than simple words.
3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the host will be unattended.
4. All hosts used by the employee that are connected to the Internet/Intranet/Extranet, whether owned by the employee or SCG, shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.
5. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.
6. Employee also should be aware of phishing and other fraudulent internet schemes to obtain passwords and other confidential information.

4.3. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of SCG authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing SCG-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities that fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by SCG.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which SCG or the end user does not have an active license.

3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate manager should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using any SCG computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any SCG account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior notification and approval by SCG.
11. Executing any form of network monitoring that will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee's host (e.g., denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with or disable a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
15. Providing information about, or lists of, SCG employees to parties outside SCG.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam - unauthorized and/or unsolicited electronic mass mailings).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within SCG's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by SCG or connected via SCG's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

5.0 Personal Use

The computers, electronic media and services provided by SCG are primarily for business use to assist employees in the performance of their jobs. Limited, occasional, or incidental use of electronic media (sending or receiving) for personal use, non-business purposes is understandable and acceptable, and all

such use should be done in a manner that does not negatively affect the systems' use for their business purposes. However, employees are expected to demonstrate a sense of responsibility and not abuse this privilege. In addition, time engaged for personal use of SCG resources should not be billed to SCG or to SCG clients. All personal use of SCG resources is subject to the restrictions and policies stated herein. Employees who violate these restrictions and policies will be acting on their own and not as an employee of SCG and they will be subject to disciplinary actions by SCG and SCG will cooperate with authorities dealing with related investigations and/or violations.

6.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

7.0 Acknowledgement

Employee Name: _____

- I hereby acknowledge that I have received and read the information regarding The Scientific Consulting Group, Inc.'s (SCG) Acceptable Use Policy and I understand that this publication provides guidelines on the policies, procedures, and programs affecting my employment with SCG.

- I acknowledge that any changes made by SCG with respect to these policies, procedures, or programs can supersede, modify, or eliminate any of the policies, procedures, or programs outlined in this policy.

- I accept responsibility for familiarizing myself with the information in this policy, and will seek clarification and/or guidance if questions arise concerning the information presented.

_____ _____

Signature Date