The Scientific Consulting Group, Inc.

Information Security Awareness and Training Policy and Procedures

for the

SCG Secure Cloud System

Version 1.2

June 13, 2016

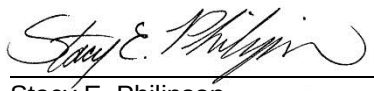
The Scientific Consulting Group, Inc.
656 Quince Orchard Road
Suite 210
Gaithersburg, MD 20878

Information Security Awareness and Training Policy and Procedures Approval

The Information Security Awareness and Training Policy and Procedures for the SCG Secure Cloud system must be approved by the SCG President, Vice President of Administration, and the Information Technology Director. The undersigned acknowledge that they have reviewed the SCG Information Security Awareness and Training Policy and Procedures and agree with the information presented in this document. The SCG President and Information Technology (IT) Director will review the Information Security Awareness and Training Policy and Procedures on an annual basis and revise the plan to address system/organizational changes or changes to policy or procedures. Any changes to the document will be coordinated with, and approved by, the undersigned or their designated representatives.

Beverly J. Campbell
President

6/13/16
DATE



Stacy E. Philipson
Vice President of Administration

6/13/16
DATE

Chuck C. Lee
Information Technology Director

6/13/16
DATE

Document Information and Revision History

Document Owners	
SCG President	
Name	Beverly J. Campbell
Contact Number	301-670-4990 (W); 301-461-1109 (C)
E-mail Address	bcampbell@scgcorp.com
SCG Vice President of Administration	
Name	Stacy Philipson
Contact Number	301-670-4990 (W); 301-742-5954 (C)
E-mail Address	bcampbell@scgcorp.com
SCG Information Technology Director	
Name	Chuck Lee, Information Technology Director
Contact Number	301-670-4990 (W); 301-366-3273 (C)
E-mail Address	clee@scgcorp.com

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
1.0	2/28/15	B. Campbell	Draft document
1.1	5/19/16	B. Campbell	Changes throughout document
1.2	6/13/2016	B. Campbell	Changes throughout document

This record shall be maintained throughout the life of the document. Each published update shall be recorded. Revisions are a complete re-issue of the entire document. The version number's decimal (minor) portion here and on the cover page is updated for each revision. The version number's integer (major) portion will be updated at each time a full Security Assessment and Authorization is performed.

Table of Contents

1. Purpose, Scope, and Distribution

The purpose of this document is to define SCG's policy and procedures for security awareness and training for all staff who have access to and responsibilities for maintaining the SCG Secure Cloud (SCGSC) system. SCG understands that "people," not necessarily technology, often are the largest threat to the security of sensitive information and security awareness and training is an effective means of preventing disclosure of such information.

This document identifies SCG's policy and procedures for information security awareness and training for the SCG staff members who have access to the SCGSC system. The document is distributed to these staff members and posted on the SCG Intranet in read-only format to allow SCG staff easy access.

2. Policy

SCG will conduct an ongoing information security awareness and training program for all SCG staff responsible for the SCGSC system to explain security responsibilities and to provide training in correct practices.

Technical IT security controls are a vital part of SCG's information security framework but are not in themselves sufficient to secure all of SCGSC's information assets. Effective information security also requires the awareness and proactive support of the personnel, supplementing and making full use of the technical security controls. This is obvious in the case of social engineering attacks, for example, which specifically target vulnerable humans rather than IT and network systems.

Lacking an adequate level of awareness concerning information security, workers are less likely to recognize or react appropriately to information security threats, attacks and incidents, and are more likely to place valuable information assets in danger through ignorance and carelessness.

Whereas "awareness" implies a basic level of understanding about a broad range of information security matters, "training" generally implies more narrowly focused and detailed attention to one or more specific topics. Awareness typically provides the foundation level of knowledge for training. In other words, awareness and training are complementary approaches.

To protect information assets, all employees who have access to SCGSC must be informed about relevant and topical information security matters, and motivated to fulfill their information security obligations.

SCG's security awareness policy details include the following:

- Initial security awareness and training must be completed before an SCG employee is granted access to the SCGSC system. The awareness and training activities should continue on an annual basis thereafter or when required by

system changes to maintain a reasonably consistent level of awareness and training.

- The information security awareness program ensures that SCG employees achieve and maintain a basic level of understanding on a broad range of information security matters, including their obligations under various information security policies, standards, procedures, guidelines, laws, regulations, and contractual terms and generally held standards of ethics and acceptable behavior.
- Additional training is appropriate for employees with specific obligations towards information security that are not satisfied by basic security awareness, for example information security management, security administration, site security, and IT personnel. The particular training requirements will reflect workers' relevant prior experience, training and/or professional qualifications, as well as job needs.
- Where necessary and practicable, security awareness and training materials should suit their intended audiences in terms of their styles, formats, complexity, technical content, etc. For example, some people prefer to read written descriptions and instructions while others prefer to be shown things or have them demonstrated. Some like to read words, others prefer diagrams and pictures. Non-technical workers are unlikely to understand or appreciate highly technical awareness content, while their technical colleagues may well need the full details in order to understand exactly what they are being asked to do.

3. Procedures

SCG's President and IT Director are responsible for developing, implementing, and maintaining the information security awareness and training program for SCG employees responsible for the SCGSC. All IT staff who have access to the SCGSC must participate in the program to ensure that they are knowledgeable about information security policies, and comply with the procedures and instructions provided in the training.

4. Information Security Awareness Training

SCG requires that all staff responsible for the SCGSC system receive information security awareness training. This training instructs employees on information security policies, procedures, and responsibilities. All SCG employees responsible for the SCGSC system are required to take annual security awareness training and when changes to the system occur.

The security awareness training will: (1) improve employees' awareness of the need to protect the SCGSC information resources, (2) ensure that the employees clearly understand their responsibilities for protecting the SCGSC information resources, (3) ensure that employees are knowledgeable about SCG's and the National Institute of Diabetes and Digestive and Kidney Diseases' (NIDDK's) (the client for the SCGSC

system) information security policies and practices, and (4) develop skills and knowledge so employees can perform their jobs correctly and effectively protect the security of the SCGSC.

The information security awareness training will address information security policy and governance, physical access controls, e-mail and internet security, security outside the office, privacy, incident reporting, and rules of behavior. All SCG personnel with access to SCGSC must complete the National Institutes of Health (NIH) Information Security Awareness Course, which addresses internal as well as external threats, and includes training on recognizing and reporting potential indicators of insider threat, annually. They also must complete the NIH Privacy Awareness Course before they are granted access to the SCGSC. Each employee completes the information security awareness training annually by logging onto the NIH security training website (http://irtsectraining.nih.gov/) and completing the two courses. If the employee has already taken the courses, they must complete the annual refresher course. . Once the employee completes each training course, he or she prints out the certificate, notifies the Program Manager via e-mail, and provides the training certificate to the SCG Human Resources Manager, who maintains the certificates in the secured personnel files. The Program Manager is responsible for maintaining the *SCGSC Technical Training Checklist*, which identifies the type of training required for each employee accessing the SCGSC, the frequency of the training, and when the training was completed.

These 5. Targeted Training

Certain SCG IT personnel may require training that is more advanced or specialized than general awareness training in order to best support the security goals for the SCGSC system. SCG requires personnel assigned security roles and responsibilities for the SCGSC system to complete the appropriate HHS' role-based training course. HHS offers Information Security for Executives, Information Security for IT Administrators, and Information Security for Managers (http://www.hhs.gov/ocio/securityprivacy/awarenesstraining/awarenesstraining.html). The System Administrators for the SCGSC are required to complete the HHS Information Security for IT Administrators training course within three (3) months of entering this position and gaining SCGSC access, when changes to the system occur, and at least annually. As with the NIH information security and privacy awareness training, the employee completes the HHS role-based training, prints the certificate, notifies the Program Manager, and provides the certificate to the HR Manager. The HHS Information Security for IT Administrators course covers information security program management, development phase security, implementation and assessment phase security, operations and maintenance phase security, and disposition phase security. Annual incident response, disaster recovery, and contingency planning training, testing, and evaluation also is required for all employees with SCGSC access. This training is conducted by the IT Director. Once the training is completed, the IT Director notifies the Program Manager and sends an e-mail to the HR Manager certifying the completion of the annual training for the employees, who adds the information to the personnel files. The SCG personnel who have access to the SCGSC

must participate in incident response, disaster recovery, and contingency planning testing, training, and exercises (TT&E) on an annual basis, as outlined in the Disaster Recovery Plan (DRP), Incident Response Plan (IRP), and Contingency Plan (CP) for the SCGSC system. Such TT&E also will be conducted as needed after system changes, the issuance of new guidance or procedures, or similar events. Execution of TT&E assists in determining the effectiveness of the DRP, IRP, and CP, and that all personnel know their specific roles with regard to implementing each of the SCGSC plans.

The provisions of the IRP and DRP will be incorporated into the security training program to familiarize all SCG personnel with the plans and their responsibilities if a cyber-incident or disaster occurs. During training activities, the IT personnel will be made aware of policies and procedures regarding appropriate use of the SCGSC system and applications. Applicable lessons learned from incidents that have occurred will be documented and shared during training sessions so that trainees can see how their actions could affect the SCGSC. Improving staff awareness regarding incidents should reduce the frequency of incidents. The training will ensure that the IT staff can maintain and protect the SCGSC system and applications in accordance with SCG's and NIDDK's security standards.

SCG is required to conduct TT&E events periodically, following organizational or system changes, the issuance of new TT&E guidance, or as otherwise needed. In addition, SCG personnel accessing federal government systems are required to complete annual computer security and awareness training. The IT Director is responsible for scheduling and conducting the annual TT&E events.

6. Roles and Responsibilities

The IT Director and SCG President are responsible for establishing and enforcing the SCGSC security awareness and training program. The IT Director and SCG President specify the types and frequency of training required, ensure that the training is conducted as scheduled, and verify that the staff who are required to take the training do so. The IT Director and SCG President also identify the IT staff members who need targeted additional training, such as the HHS Information Security for IT Administrators course. For security awareness and privacy training, SCG relies on the NIH courses mentioned above.

For incident response and disaster recovery TT&E, the IT Director works with IT staff to develop tests, training, and exercises for SCGSC incident response and disaster recovery to verify the preparedness of the team, ensure that each member knows and can perform his/her role, and assess the effectiveness of the DRP and IRP for the SCGSC system.

The SCG IT personnel who have access to the SCGSC must complete the NIH security awareness and privacy awareness course or refresher course annually. They also are responsible for participating in the TT&E events scheduled by the IT Director as needed. Some SCG IT personnel may be responsible for taking additional security

training as determined by the IT Director. Upon completion of the annual NIH and HHS training, each employee must submit a copy of the training completion certificate to the Human Resources Manager (Ava Wilt), who adds the certificate to the employee's secure personnel file. These certificates will be retained by HR for the duration of the contract or until there is a status for the SCG personnel. The employee also must notify the Program Manager (Susie Warner) by e-mail that he/she has completed the training, and the Program Manager will update the *SCGSC Technical Training Checklist* to indicate the date the training was completed. This checklist will be maintained by the Program Manager throughout the duration of the contract.

7. Compliance and Enforcement

The security awareness and training policy applies to all SCG staff who have access to the SCGSC and are responsible for its maintenance and protection. Persons in violation of the security and privacy rules communicated during training are subject to a range of sanctions (determined and enforced by SCG management), including the loss of SCGSC access privileges, disciplinary action, dismissal, and legal action. The IT Director, SCG President, and Program Manager are responsible for enforcing compliance with the information security, privacy awareness, incident response, disaster recovery, and contingency planning training. Employees who fail to comply with the training policies and procedures will be subject to sanctions, primarily loss of SCGSC access privileges. The IT Director, SCG President, and Program Manager also are responsible for detecting and assessing security and privacy violations and enforcing the sanctions they deem appropriate to the nature of the incident. Some violations may constitute criminal offenses and prosecution, while others may warrant loss of SCGSC access privileges or dismissal. The IT Director and Program Manager will be responsible for carrying out the sanctions and the Program Manager will report such violations to the NIDDK and appropriate authorities.

Appendix A: Key Personnel Contact List

This appendix contains a list of key personnel at SCG responsible for the SCGSC, and their contact information. Only the four individuals with an asterisk (*) next to their names have access to the SCGSC and must complete annual information security awareness training.

Title	Name	Contact Information	Emergency Role
IT Director	Chuck Lee*	301-670-4990 (W) 301-366-3273 (C) 301-637-4355 (H) clee@scgcorp.com	Damage Assessment, Incident Response/Disaster Recovery Team Leader DRP Director
SCG President	Beverly Campbell	301-670-4990 (W) 301-461-1109 (C) 540-887-9829 (H) bcampbell@scgcorp.com	Damage Assessment, CP Activation Decision, and Contingency Planning Team Leader
Vice President of Administration	Stacy Philipson	301-670-4990 (W) 301-742-5954 (C) 301-363-5707 (H) sphilipson@scgcorp.com	Damage Assessment, SCG Facilities Management, Business Continuity Plan Team Leader, Incident Response/ Disaster Recovery Team Member
Program Manager	Susie Warner	301-670-4990 (W) 301-366-3217 (C) 301-355-4388 (H) swarner@scgcorp.com	SCG Secure Cloud Contract Management, Incident Response/Disaster Recovery Team Member
IT Systems Specialist	Kenny Ying Lee*	301-670-4990 (W) 315-956-7796 (C) ylee@scgcorp.com	Incident Response/Disaster Recovery Team Member
IT Systems Specialist	John Bernheimer*	301-670-4990 (W) 410-428-1330 (C)	Incident Response/Disaster Recovery Team Member
Web Developer	Adam Mann*	301-670-4990 (W) 301-717-3273 (C) amann@scgcorp.com	Applications and Web Development, Incident Response/Disaster Recovery Team Member

Appendix B: NIDDK Contacts for the SCGSC

NIDDK System Owner: Dana Sheets, Digital Engagement Lead, Office of Communications and Public Liaison (OCPL), NIDDK/NIH, 301-496-7059, sheetsdm@mail.nih.gov

NIDDK Information Systems Security Officer (ISSO) Contact: Warren Herder, Information System Security Officer, Computer Technology Branch, NIDDK/NIH, 301-443-9292, herderjw@niddk.nih.gov

NIDDK Authorizing Official/Designated Approving Authority Contact (AO/DAA): Chandan Sastry, IT Director and CIO, Computer Technology Branch, NIDDK/NIH, 301-496-9555, sastrych@mail.nih.gov

NIDDK Privacy Officer: Kelly Yager, Management Analyst, Office of Management and Policy Analysis, NIDDK/NIH, 301-594-3056, kelly.yager@nih.gov.

Appendix C: Acronyms

AO	Authorizing Official
C	Mobile (or Cell) Phone
CP	Contingency Plan
DAA	Designated Approving Authority
DRP	Disaster Recovery Plan
H	Home Phone
IRP	Incident Response Plan
ISSO	Information System Security Officer
IT	Information Technology
NIDDK	National Institute of Diabetes and Digestive and Kidney Diseases
NIH	National Institutes of Health
OCPL	Office of Communications and Public Liaison
SCGSC	Scientific Consulting Group Secure Cloud
TT&E	Testing, Training and Exercise
W	Work Phone