The Scientific Consulting Group, Inc.

SCG Personnel Security Screening Policy and Procedures

for the

SCG Secure Cloud System

Version 1.2

May 19, 2016

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

SCG Personnel Security Screening Policy and Procedures Approval

The SCG Personnel Security Screening Policy and Procedures for the SCG Secure Cloud System must be approved by the SCG President, Vice President of Administration, and Information Technology Director. The undersigned acknowledge that they have reviewed the SCG Personnel Security Screening Policy and Procedures and agree with the information presented in this document. The SCG President, Vice President of Administration, and Information Technology Director will review the policy and procedures in this document at least once every three (3) years and revise it to address system and organizational policy and procedural changes. Any changes to the SCG Personnel Security Screening Policy and Procedures will be coordinated with, and approved by, the undersigned or their designated representatives.

Beverly J. Campbell
President

5/19/16
DATE

Stacy E. Philipson
Vice President of Administration

5/19/16
DATE

Chuck C. Lee
IT Director

5/19/16
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	1/29/15	B. Campbell	Initial Draft. Based on the Personnel Security principles established in NIST SP 800-53 "Personnel Security," Control Family guidelines.
1.1	3/9/15	B. Campbell	Made revisions throughout document
1.2	5/19/16	B. Campbell	Made revisions 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

The purpose of this document is to establish The Scientific Consulting Group, Inc.'s (SCG) policy regarding the personnel security screening requirements for all employees assigned to positions that require personnel security screenings. These employees will not require or have access to classified national security information.

2. Policy

SCG has adopted the Personnel Security principles established in NIST SP 800-53 "Personnel Security," Control Family guidelines as the official company policy. Therefore, it is the policy of SCG to ensure that all employees undergo personnel security screenings if required for performance under a contract (see Part IV, Applicability).

This document has been disseminated to the SCG President, Vice President of Administration, IT Director, and senior managers. It is posted in read-only format on the SCG Intranet to facilitate easy access by SCG staff.

3. Authorization

- Executive Order 13467, Reforming Processes Related to Suitability, Fitness for Contractor Employees, and Eligibility for Access to Classified Information, July 17, 2008.
- Homeland Security Presidential Directive Number 12 (HSPD-12), "Policy for Common Identification Standard for Federal Employees and Contractors."
- Privacy Act of 1974, 5 U.S.C. 552a, as amended.
- U.S. Code Title 42, The Public Health and Welfare, Chapter 132, Subchapter V – Child Care Worker Employee Background Checks, Section 13041
- Appendix III to OMB Circular No. A-130 – Security of Federal Automated Information Resources.
- NIST FIPS 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, NIST, March 2006.
- Federal Information Security Management Act (FISMA), Title III of the E-Government Act (Public Law 107-347).

4. Applicability

All SCG employees must undergo personnel security screenings if, during the performance of the contract, they will:

- Require an ID badge granting unescorted access to government facilities;
- Require IT system access;

- Require access to unclassified sensitive information, such as Privacy Act-protected, personally identifiable, proprietary, or other sensitive information and data.

5. Procedures and Responsibilities

The Program Manager (PM) is expected to play a key role in tracking the personnel security adjudication determinations of employees working on the contract as part of the responsibility in managing the contract. The PM has the option to deny employees access to unclassified sensitive information or IT systems, until the Vice President of Administration has completed the personnel security adjudication determination. The SCG President must approve in advance exceptions to this policy.

Records of all checks conducted on personnel will be maintained by the Vice President of Administration, who will certify that SCG has engaged in screening appropriate to the responsibilities of the individuals employed under the contract. Individuals who have been employed by SCG for more than 2 years and have been working on other federal government contracts that have required screening to obtain an ID badge will not have to be rescreened to work on the new contract. In addition, if an individual has been employed by SCG for 5 or more years and has been working in positions of high and moderate risk in a trustworthy manner during that time, no investigation is required when assigned to a new contract.

5.1 Assigning Position Risk Levels

For each contract, the PM must determine the risk levels for each contractor position. The PM must maintain a current position risk level designation record for each contractor position for the contract. The three position risk levels and their investigative requirements are listed in Table 1.

Table 1. Position Risk Level Descriptions and Requirements

Risk Level	Position Descriptions
HIGH RISK (HR)	Positions with the potential for exceptionally serious impact on the efficiency of SCG. This includes access to IT systems that allows the bypass of security controls or access that, if taken advantage of, could cause serious harm to the IT system or data. A background investigation is the type of investigation required.
MODERATE RISK (MR)	Positions with the potential for moderate to serious impact on the efficiency of SCG, including all positions that require access to unclassified sensitive information, such as Privacy Act-protected, personally identifiable, proprietary or other sensitive information and data. A background check using an agency such as HireRight, and a credit check, is the type of investigation required. The investigation may be expanded if the background and/or credit check investigation develops information that SCG managers consider potentially actionable.
LOW RISK (LR)	Includes all other positions to which this policy applies (see applicability in Section IV). A background check using an agency such as HireRight is the type of investigation required.

The PM must assign a position risk level to each applicable contractor employee position, consistent with Appendix A of this document. This information will be recorded on the Position Designation Record for Contractor Positions form (see Appendix B). These records are maintained on file with the Vice President of Administration and the Program Manager. The SCG President, Vice President of Administration, and IT Director must concur in writing with the designated risk level. If the duties of a position involve more than one risk level, the higher of the two risk levels will be assigned to the position. The PM must maintain status update on contractor duties as they change (e.g., from Moderate Risk to High Risk), and is responsible for commensurate paperwork and elevation of position risk level and commensurate background investigation requirement.

5.1.1 High Risk Level Positions

For High Risk level positions, each PM must deny the employee High Risk level access to IT systems, or sensitive or Privacy Act-protected information, until the Vice President of Administration notifies the PM that the preliminary security screening was completed favorably.

Employees for High Risk level positions should be U.S. citizens. SCG may consider a non-U.S. citizen only when the individual possesses unique or unusual skills/expertise not available elsewhere and provided the employee is a Lawful Permanent Resident of the United States; has resided continuously in the United States for a minimum of three (3) years; the government agency issuing the contract approves the assignment in writing; and the written approval is filed with the Contracting Officer before requesting the preliminary personnel security screening and/or investigation is initiated.

Preliminary personnel security screening is required for High Risk IT level system access. All employees assigned or transferred into positions determined to be at the High Risk IT level must undergo a preliminary personnel security screening before: (1) they are authorized to bypass significant technical and operational security controls of general support IT systems, or major applications; or (2) they are authorized to access applications where controls such as separation of duties, least privilege, and individual accountability cannot adequately protect the application or the information in it. The preliminary personnel security screening may include a review of completed security forms, credit check, record checks, and file reviews. The PM must deny the employee High Risk level access to IT systems until the Vice President of Administration notifies the PM that the preliminary personnel security screening was completed favorably. The inquiries for the preliminary personnel security screening will be initiated within 5 working days after receipt of the completed security forms. Within 5 working days after receiving the results of those inquiries, a determination will be made regarding an employee's acceptability. As necessary, a background investigation will be conducted following the completion of the preliminary personnel security screening. Employees occupying High Risk level IT positions must undergo reinvestigation every 5 years for the duration of the contract, or if there is a break-in-service with SCG of 365 days or more.

5.1.2 All Other Risk Level Positions

Employees occupying Moderate or Low Risk level positions must undergo the appropriate level of investigation specified in the table above. No employees are permitted unescorted/unsupervised access to government facilities, unclassified sensitive information, or IT systems, until they have submitted applicable investigative forms.

5.2 Employee Screening and Findings

The Vice President of Administration will keep the PM informed during the employee screening process, including notification of the screening determination.

The Vice President of Administration will notify the PM of the personnel security adjudication determination and maintain a copy in the employee's personnel file. If any attributes of the position change, including the need for a higher risk level, the PM will work with the Vice President of Administration to determine if additional investigation is warranted for the employee to meet the investigative requirements for the higher position risk level.

When a security investigation returns negative findings, the Vice President of Administration will notify the PM and IT Director that an employee is deemed not acceptable for reasonable cause and such finding(s) makes the individual ineligible for access to government facilities or IT systems.

The PM and IT Director must immediately deny an employee access to all IT systems, facilities, and information, when notified by the Vice President of Administration that an employee is deemed not acceptable for reasonable cause.

5.3 Recordkeeping

The PM must maintain an up-to-date list of all contract positions and risk level designations covered by these policies and procedures. The list must include the employee's name, the risk level designation of the employee's position, the date the employee's investigation was initiated, the date of the final personnel security screening determination, and the final determination. The PM also must ensure that an employee is not placed in a more sensitive position than that for which he or she was previously approved, without the approval of the SCG President, Vice President of Administration, and IT Director.

5.4 Employee Reassignment/Departure

The PM must notify the Vice President of Administration and IT Director immediately of the immediate or eminent departure of an employee, either voluntary or involuntary, and furnish the reason(s) and the date of the departure. The PM must obtain any government-issued IDs from the employee prior to departure.

For employee transfers/reassignments, the Vice President of Administration must notify the PM and the IT Director immediately upon approval of the transfer/reassignment. Within the 2-week transition period, the Vice President of Administration must collect IDs, fobs, keys, and similar property no longer required by the employee and issue any

new IDs, fobs, keys, etc., required for the new assignment. In addition, the IT Director must disable any system credentials/authenticators for accounts no longer required by the employee and create new accounts required for the new assignment. The Vice President of Administration and IT Director must notify the SCG President when transfer/reassignment tasks are completed within 1 day or completion.

For involuntary terminations, the IT Director immediately disables information system access and terminates/revokes any authenticators/credentials associated with the individual and the account is disabled within 7 days; for voluntary terminations, the IT Director and PM determine the appropriate date to disable information system access and disable/revoke any authentications/credentials and the account is removed 7 days following that date.

The Vice President of Administration conducts exit interviews that include a discussion of security and other topics and retrieves all security-related property issued by SCG such as keys, fobs, and garage opener. The Vice President of Administration also confirms that the PM has retrieved all government-issued security-related property such as ID badges, tokens, etc. The PM also notifies the government client to close all e-mail accounts and access privileges to government systems for the employee.

The IT Director retains access to organizational and information systems formerly controlled by the terminated employee and notifies the Vice President of Administration and PM as soon as control is verified.

5.5 Reporting of Incidents/Concerns

The PM and IT Director must report to the SCG President and Vice President of Administration all instances of employees seeking to obtain unauthorized access to any IT system or unclassified sensitive and/or Privacy Act-protected information.

The PM and IT Director must report to the SCG President and Vice President of Administration any information that would raise a concern about whether an employee's continued employment would jeopardize the contract and/or violate the public trust.

Appendix A: Position Risk Designation for Contract Positions

Risk Level	Criteria for Determining Risk Level
High Risk	Position involves one or more of the following attributes: • Responsibility for the development, direction, implementation, and administration of computer security programs, including direction and control of risk analysis or threat assessment. • Significant involvement in mission-critical IT systems. • Responsibility for preparing or approving data for input into an IT system that does not necessarily involve personal access to the IT system, but which creates a high risk for effecting grave damage or realizing significant personal gain. • Major responsibility for the direction, planning, design, testing, maintenance, operation, monitoring, or management of the IT systems hardware and software. • Access to an IT system during the operation or maintenance in a way that bypasses incorporated controls, to permit high risk for causing grave damage or realizing a significant personal gain. • Any other positions that involve high risk for effecting grave damage or significant personal gain.
Moderate Risk	A position whose work is technically reviewed by a higher authority at the High Risk level to ensure the integrity of the information or IT system. Position involves one or more of the following attributes: • Access to or processing of proprietary data or information protected under the Privacy Act of 1974. • Other positions that involve a degree of access to an IT system that creates a significant potential for damage or personal gain less than that in High Risk positions.
Low Risk	Includes all other positions to which this policy applies (see Part IV, Applicability) that do not fall within the High and Moderate Risk levels above.

Appendix B: Position Designation Record for All Applicable Contractor Positions

Contractor Name: _____

Contract Title & Number: _____

Contract Position Title: _____

1. INFORMATION TECHNOLOGY (IT) RISK LEVEL: _____

   JUSTIFICATION: _____

   _____

   _____

   Reminder: Be sure you have considered all pertinent access controls of the relevant IT system when determining the position risk level, such as separation of duties, least privilege and individual accountability.

   If the position is Moderate or High Risk from an IT standpoint, you do not need to perform the next step. If the position is Low Risk from an IT standpoint, Step 2 below may adjust the final position risk level to a Moderate Risk level position.

2. This is a Moderate Risk Level position because the employee will require access to: (Please check if applicable)

   _____ Unclassified sensitive information, such as Privacy Act-protected, personally identifiable, proprietary, or other unclassified sensitive information or data.

3. This is a Low Risk Level position because the employee will require:

   _____ A government ID badge granting unescorted access to government facilities.

   _____ No access to unclassified sensitive information, such as Privacy Act-protected, personally identifiable, proprietary, or other unclassified sensitive information or data.

4. _____ No risk level required for this position.

5. FINAL POSITION RISK LEVEL PLACEMENT: _____
   (Where the duties of the position involve more than one risk level, the higher of the two risk levels will be assigned to the position.)

Signature Vice President of Administration	Signature IT Director	Signature Program Manager
Printed Name & Date	Printed Name & Date	Printed Name & Date
Telephone No.	Telephone No.	Telephone No.
E-mail	E-mail	E-mail