**The Scientific Consulting Group, Inc.**

# Facility and Systems Access Policies and Procedures

for the

# SCG Secure Cloud System

***Version 1.7***

***June 13, 2016***

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

# Facility and Systems Access Policies and Procedures Approval

We, the undersigned, approve the content of this Facility and Systems Access Policies and Procedures for the SCG Secure Cloud (SCGSC) system located at The Scientific Consulting Group, Inc. (SCG), 656 Quince Orchard Road, Suite 210, Gaithersburg, Maryland. These policies and procedures will be reviewed annually and revised as often as deemed necessary by the undersigned to ensure that SCG's facilities and the SCGSC system are protected and secure.

6/13/16

Beverly J. Campbell
President

DATE

6/13/16

Stacy E. Philipson
Vice President of Administration

DATE

6/13/16

Chuck C. Lee
IT Director

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 History | | | |
|---|---|---|---|
| **Revision** | **Date** | **Author** | **Comments** |
| 1.0 | 1/29/15 | B. Campbell | Initial draft of Facility and Systems Access Policies and Procedures for SCGSC |
| 1.1 | 2/16/15 | E. Ransom<br>C. Berry<br>K. Martinez | Updated section titles to generate Table of Content. Updated references. Minor modifications throughout document. |
| 1.2 | 2/17/15 | B. Campbell | Reviewed changes and made minor formatting changes throughout document. |
| 1.3 | 2/24/15 | B. Campbell | Minor revisions to document |
| 1.4 | 2/25/15 | B. Campbell | Revisions throughout document |
| 1.5 | 2/26/15 | B. Campbell | Revisions throughout document |
| 1.6 | 5/19/16 | B. Campbell | Revisions throughout document |
| 1.7 | 6/13/16 | B. Campbell | 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

# List of Tables

## 1. Purpose and Scope

The purpose of this document is to establish The Scientific Consulting Group, Inc.'s (SCG) policy and procedures regarding accessing SCG facilities and the SCG Secure Cloud (SCGSC) system. SCG strives to create a welcoming environment, which at the same time is one that is safe and secure for our employees and visitors. This document details the policies and procedures that will be used to protect our organization, facilities, people, and assets by controlling who and what enters and leaves our facilities. The document facilitates the implementation of security control requirements for the "Access Control" and "Identification and Authentication Control" families, as identified in NIST Special Publication (SP) 800-53 Revision 4 *Security and Privacy Controls for Federal Information Systems and Organizations.*

It defines the Access Control and Identification and Authentication requirements and mechanisms to be implemented for the SCGSC. These procedures contained herein have been developed in accordance with Federal Information Security Management Act (FISMA) compliance requirements.

The scope of this document includes policies and procedures for access to SCG's offices in Gaithersburg, Maryland, where the SCGSC system is located, as well as access to the SCGSC system. These policies and procedures apply to the SCGSC and all of its administrators, developers, users, owners, and custodians. This procedure will be reviewed annually by the SCG President, Vice President of Administration, and IT Director and revised as needed.

The policies established in this document are consistent with what has been determined to be realistic and possible threats that pose a risk to SCG and the SCGSC. While certain activities such as thefts, property damage, and unauthorized entry are always possible, there may be times when it will be necessary to raise security levels. The Vice President of Administration and IT Director will monitor sources and notices and notify staff when there is a need to implement increased vigilance and heighten security operations. This policies and procedures document must be disseminated to the SCG employees who have user accounts for the SCG Secure Cloud system. It also is available to all SCG employees on the SCG Intranet.

## 2. Document Management

The Table 1 identifies who within SCG is responsible for developing and implementing and approving the access controls and identification and authentication procedure for the SCGSC. The following definitions apply:

- **Responsible Party** – the person responsible for developing and implementing the procedure.
- **Approver** – the person required to approve the final procedure implementation or amendment.

**Table 1. Responsibility for Facility and Systems Access Policies and Procedures**

| Policy | Responsible Parties | Responsibilities | Approver |
|---|---|---|---|
| Access Control and Identification and Authentication Policies | IT Director, Vice President, and SCG President | Support and approve the policy | SCG President, Vice President of Administration, IT Director, and NIDDK ISSO |
| | IT Director, Vice President, and SCG President | Develop, implement, and maintain the policy at least annually | SCG President, Vice President of Administration, and IT Director |
| | IT Director and Vice President of Administration | Enforces the policy and communicates any changes | SCG President |
| | SCG Employees | Acknowledge and comply with policy | IT Director and  Program Manager |

## 3. Building and Office Access

The SCGSC system is located at SCG's offices in Gaithersburg, Maryland. There are three entrances into the building in which SCG's offices at 656 Quince Orchard Road, Gaithersburg, Maryland, are located. The two street entrances are unlocked and accessible during regular business hours Monday through Friday. The garage entrance is accessed through the garage under the building. The garage door is closed at all times and can only be opened by individuals with garage door openers. The door from the garage to the building is unlocked during regular business hours Monday through Friday but is locked at all other times and then can only be accessed by individuals with assigned access card openers. The door from the stairwells in the building to the office floors are locked at all times, requiring a key to enter each floor. SCG provides each employee keys to the stairwell doors that allow entrance to the second and seventh floor lobby areas.

Entrances to SCG's offices on the second and seventh floors are locked at all times and programmed fobs are required to access the office space on both the second and seventh floors. When an employee swipes a fob for access to SCG offices, an electronic record is created that reports the employee's name, date, and time of entry. SCG staff also must sign in and out to ensure that the receptionist knows who is in the office and to create a hardcopy record of arrivals and departures.

The SCG receptionist is positioned by the main entrance into SCG's office space on the second floor. She has an unimpeded view of the entrance and all entrants must pass by this area. The receptionist has the responsibility for screening and granting access to all non-SCG employees, such as couriers, delivery persons, vendors, and clients. All visitors to SCG must report to the second floor, ring the doorbell, and wait to be admitted by the SCG receptionist. Visitors who enter SCG facilities must sign in the log book, indicating the date, time, purpose of the visit, and who they are visiting. All guests must sign out with the front desk when leaving. The receptionist may request a valid ID from visitors if they are unknown, unexpected, or there is reason for concern.

The bathrooms throughout the building are locked at all times and accessed using either a combination or key (second floor by combination, seventh floor by key). All SCG staff members are provided the combination/key to the bathrooms on the second and seventh floors; visitors are provided the combination/key by the receptionist as needed.

The two additional entrances to SCG's second floor offices are locked at all times and accessible only by SCG staff using the fob access, which creates an electronic log of the individual accessing the space and time of access. In addition, SCG's entrances and priority rooms are monitored by surveillance cameras that record events on a DVR when triggered by detected motion. All entrances into SCG space are equipped with alarms that will activate in the event of unauthorized access and when a door is propped open for more than 1 minute.

There is a single entrance to access the offices on the seventh floor. The door is locked at all times and requires fob authentication for access. On both the second and seventh floors, the server rooms are locked at all times and require fob authentication for access. The fobs of the personnel authorized to access the server are programmed to allow them access to these rooms.

Other offices/rooms within SCG's office space are locked to limit access and protect sensitive information. Keys to these offices and rooms are issued to appropriate employees by the Vice President of Administration. Two master keys that open all locked offices/rooms within the office space are kept secure by the Vice President of Administration and the President of SCG.

## 4. Authorized Individuals

SCG employees are granted access to the building, bathrooms, and office space. It is SCG's policy that employees are issued the least number of keys/fobs at the lowest level in the locking system hierarchy that is necessary to provide the required access. The levels of access and rules of issuance are summarized in Table 2. SCG employees are screened at a level commensurate to their intended positions before they are hired.

Clients, UPS and FedEx delivery persons, US Postal carriers, couriers, and other visitors are granted access to SCG space through the receptionist and they are accompanied within the office space by an SCG employee.

SCG employees are asked to notify the receptionist when they expect a visitor, delivery, courier pickup/drop-off, etc. This prenotification simplifies and accelerates the access process. Staff members expecting visitors are required to meet and escort their guests while they are in SCG office space.

Vendors, couriers, and other companies servicing SCG offices on a regular basis are expected to subject their employees to background checks. The receptionist maintains a list of all regular vendors/companies on hand and she requests business-specific identification from these visitors.

**Table 2. Levels of Access and Rules of Issuance**

| Access Point | Type of Control | Level of Access | Authorized Users | Rules of Issuance |
|---|---|---|---|---|
| Building/ Garage | Building Door Access Card/ Garage Remote | Office building entrances are locked before and after regular business hours and on weekends/holidays; garage access closed at all times. | SCG employees | Issued by Vice President of Administration. |
| Elevator Access/ Control | Access Card | Elevator access/control before and after regular business hours and on weekends/holidays; access to elevator from parking garage. | SCG employees | Issued by Vice President of Administration. |
| Stairwell Access | Key | Access to the 2nd and 7th floors from the stairwell at all times. | SCG employees | Issued by Vice President of Administration. |
| SCG Office Suite (2nd and 7th floors) | Fob | Employee-specific fob required for access. | SCG employees | Programmed authorized by and fobs issued by Vice President of Administration. |
| Server Room | Fob | Employee-specific fob required for access. | Authorized SCG employees | Fobs are programmed to permit access only by authorized employees. Fobs are programmed and issued on as needed basis by the Vice President of Administration. |
| Locked Offices/File and Storage Rooms | Key | Certain offices are locked to protect sensitive information such as company personnel and financial records, proposals, software, equipment, etc. | Authorized SCG employees | Keys are issued to authorized employees such as office occupants by the Vice President of Administration. |
| Mechanical Room | Key | Mechanical room door (locked at all times) to access electrical panels, cabling, water shutoff, etc. | Authorized SCG employees | Key secured and issued on as needed basis by IT Director. |
| All key access locked offices and rooms | Master Key | Master key opens all locked offices/rooms within SCG's suites. | Vice President of Administration and SCG President | Key secured and used on an as needed basis by the Vice President of Administration and President. |

Visitor logs are reviewed by the Vice President of Administration and IT Director on an annual basis before they are scanned and electronically archived.

The IT Director monitors and controls all deliveries of equipment, system components, and other items to server rooms and maintains records of those items and the dates they were placed in the room.

## 5. Master Key Control System

The Vice President of Administration is responsible for monitoring the distribution of keys, fobs, and duplicates, and maintaining accurate, up-to-date records. These records will be updated as soon as changes occur (e.g., issuing of a fob to a new employee, deactivating a fob of a departing employee, replacing a lost fob, duplicating a key). Keys/fobs are issued in the strict trust that proper measures will be taken to ensure their safekeeping and authorized use. Loss of keys/fobs can expose SCG and SCG employees to unnecessary risk. If an employee loses a fob/key or it is stolen, the employee must report it immediately upon discovery to the Vice President of Administration. The Vice President of Administration will deactivate the missing fob and make arrangements to replace any locks accessed by the key. Employees are responsible for the cost incurred by SCG to replace their lost keys/fobs and to replace any locks. Loss, misuse, or unauthorized duplication of keys/fobs will result in disciplinary action. Any formal sanctions taken will be communicated to the employee by his/her supervisor and the sanctions and reason(s) for those sanctions will be noted in the employee's personnel file.

Only authorized employees will have keys/fobs that offer access to specified areas of the building. Each fob is programmed specifically to grant appropriate access to the employee to which the fob is assigned. Accordingly, employees will obtain keys/fobs that are relevant to their position (e.g., a science writer does not need access to the server room or the mechanical room). All keys are made with non-duplicative features and it is a violation of SCG policy for any individual to duplicate any key/fob issued by SCG. Only the Vice President of Administration and President have authority to approve duplication of keys/fobs and a record of duplications must be maintained. Anyone receiving keys/fobs will sign them out upon receipt. All keys/fobs are the property of SCG and must be returned upon termination of employment. Obsolete or unneeded keys/fobs must be returned to the Vice President of Administration. When employees are terminated, either voluntarily or involuntarily, the Vice President of Administration collects their keys/fobs and the IT Director disables information system access and terminates/revokes any authenticators/credentials associated with the individual. Only the President and Vice President of Administration have access to the Master Key, which they make available to emergency personnel as needed.

## 6. SCGSC System Access

This section establishes SCG's Information System Access Control Policy for managing risks from user account management, access enforcement and monitoring, separation of duties, and remote access through the establishment of an access control program for the SCGSC system. The access control program helps SCG implement security best practices with regard to logical security, account management, and remote access for the SCGSC. This document section specifically addresses the identification and authentication policies and procedures employed by SCG for the SCGSC system.

The scope of this policy is applicable to the SCGSC system, which was developed and is maintained and operated by SCG. Any information, not specifically identified as the property of other parties, that is transmitted or stored on SCGSC resources is the property of SCG. All SCGSC users are responsible for adhering to this policy.

SCG's SCGSC Information Security policy serves to be consistent with best practices associated with organizational information security management. It is the intention of this policy to establish an access control capability for SCGSC that implements security best practices with regard to logical security, account management, and remote access.

SCG has chosen to adopt the Access Control principles established in NIST SP 800-53 "Access Control," Control Family guidelines, as the company's official policy for the SCGSC system. This section outlines the Access Control standards that constitute SCG policy for SCGSC. SCGSC users are bound to this policy, and must develop or adhere to a program plan that demonstrates compliance with the policy and standards documented.

- **AC-1 Access Control Procedures:** SCG has developed, adopted, and adheres to a formal, documented access control procedure that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
- **AC-2 Account Management:** SCG must
    - Identify account types (i.e., Developer, Domain Administrator).
    - Establish conditions for group membership.
    - Identify authorized users of the information asset and specify access privileges.
    - Require appropriate approvals for requests to establish accounts.
    - Establish, activate, modify, disable, and remove accounts.
    - Specifically authorize and monitor the use of all accounts.
    - Notify account managers when any account is created, when any account is modified, when any account is no longer required, and when information asset users are terminated, transferred, or information assets usage or need-to-know/need-to-share changes.
    - Deactivate all accounts that are no longer required and accounts of terminated or transferred users.
    - Grant access to the system based on (1) valid access authorization, (2) intended system usage, and (3) other attributes as required by SCG or SCG's client.
    - Review accounts on a **quarterly basis.**
- **AC-3 Access Enforcement:** SCG must enforce approved authorizations for logical access to the system in accordance with applicable policy. Only the

Domain Administrators are authorized to create new accounts, modify existing accounts, and disable existing accounts.

- **AC-4 Information Flow Enforcement:** SCG must enforce approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.
- **AC-5 Separation of Duties:** SCG must
  - Separate duties of individuals as necessary to prevent malevolent activity without collusion.
  - Document separation of duties.
  - Implement separation of duties through assigned information asset access authorizations.
- **AC-6 Least Privilege:** SCG must employ the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) that are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. Only Domain Administrators are authorized to make changes to system settings and software. The IT Director is authorized to make changes to the system hardware and to oversee his staff assisting with those changes. There are only privileged users for SCGSC; user privileges are appropriate for each account type (i.e., Domain Administrators have full privileges and Developers have limited privileges).
- **AC-7 Unsuccessful Logon Attempts:** SCG employs automatic controls to manage unsuccessful logon attempts.
  - The system locks out the user after 3 consecutive unsuccessful attempts at logon within 20 minutes.
  - The user account must be unlocked by the Domain Administrator for the user to access the system.
- **AC-8 System Use Notification:** SCG must
  - Display an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with regulations, standards, and policies.
  - Retain the notification message or banner on the screen until users take explicit actions to logon to or further access the information asset.
- **AC-11 Session Lock:** SCG must prevent further access to the information asset by initiating a session lock after 30 minutes of inactivity or upon receiving a request from a user. In addition, SCG must retain the session lock until the user reestablishes access using established identification and authentication procedures.

  Where applicable or specifically requested by customers, the SCGSC limits the number of concurrent sessions to one session.

  - **Windows** – Enforced by GPO, concurrent sessions are limited to one session.
  - **VMware** – N/A; Concurrent session control is not currently available.
  - **Network Devices** – Network devices are used for administration. Network administrators at times require more than one session. Therefore, concurrent sessions are not enforced on network devices.
  - **Databases** – N/A; Concurrent session control is not currently available.

- **AC-12 Session Termination:** The firewall terminates sessions after 30 minutes of inactivity. It also terminates sessions that have lost connection and are trying to reconnect after 10 minutes. Sessions also can be manually terminated by user initiated request.

- **AC-14 Permitted Actions without Identification or Authentication:** No actions can be performed on the information asset without identification or authentication.

- **AC-17 Remote Access:**

  - Only one method of remote access, through Windows Remote Desktop, is permitted for SCGSC. However, remote access for SCGSC is disabled and is only manually enabled by the Domain Administrator (by physically accessing the system in the server room) when necessary to allow him to manage the system.

  - The usage restrictions are determined by the user account type and the static IP address, and authorized by the Domain Administrator. Guidance for the allowed remote access method is provided by the IT Director.

  - Monitoring for unauthorized remote access to the information asset is not required because remote access is only manually enabled by the Domain Administrator when a remote session is activated. Remote access then is disabled by the Domain Administrator when the remote session is completed.

  - All privileged users have the authority for remote access to the SCGSC, but access must be granted manually by the Domain Administrator.

  - No cryptographic mechanisms are used to protect the confidentiality of remote sessions because remote access is manually enabled and not required as there are no live connections through VPN or Internet; the connection is direct.

  - There is only one port (i.e., 3389) to connect through remote access to SCGSC and that must be manually enabled.

  - Remote connection requirements to SCGSC are enforced through physical security measures (access control to server room) and usage restrictions.

  - Remote session commands are limited by user account type. Domain Administrators can change both system and application settings and Developers can change only files within the folder to which they have access and application settings. Developers cannot change system settings because they do not have administrative privileges.

- **AC-18 Wireless Access:** SCG prohibits wireless access to SCGSC.
- **AC-19 Access Control for Mobile Devices:** SCG prohibits mobile device access to SCGSC.
- **AC-20 Use of External Information Systems:** External information systems are not supported by SCGSC.
- **AC-22 Publicly Accessible Content:** Public dissemination of publicly accessible content is not supported by SCGSC, nor is it the responsibility of SCG.

It is SCG's policy to develop and document access agreements for organizational information systems. SCG employees requiring access to the SCG Secure Cloud system must sign appropriate access agreements (see the access request form Appendix A) prior to being granted access. These access accounts for the SCG Secure Cloud System are reviewed quarterly by the IT Director (see the review form in Appendix B). Failure to comply with SCG's information system access and security policies will result in disciplinary action. Any formal sanctions taken will be communicated to the employee by his/her supervisor and the sanctions and reason(s) for those sanctions will be noted in the employee's personnel file. SCG employees accessing the SCGSC system are required to acknowledge in writing their receipt and understanding of the rules of behavior for SCGSC access (see Appendix C). The rules of behavior are updated annually and the acknowledgements must be re-signed annually. In addition, staff must participate in the annual incident response, disaster response, and contingency planning test, training, and exercise (TT&E) event and complete required information security awareness and privacy training courses.

# 7. SCGSC Identification and Authentication

This section of the document pertains to the SCGSC Identification and Authentication Procedure.

SCG has developed, documented, and disseminated this document, which addresses SCG's identification and authentication policy and procedures for the SCG Secure Cloud system, to privileged users of the SCGSC system. These procedures and this document are reviewed and updated annually by the SCG President and IT Director. The document is distributed to SCG employees who have access to the SCGSC and are responsible for its maintenance and security. It is available in a read-only format to SCG employees on the SCG Intranet. (**IA-1 Identification and Authentication Policy and Procedures)**

## 7.1 Federal Compliance Requirements

Federal Information Processing Standards (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013.

## 7.2 Other References

E-Government Act of 2002, *Title III—Information Security, cited as the Federal Information Security Management Act of 2002 (FISMA), Public Law 107-347*, December 17, 2002.

Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources*, November 28, 2000.

Privacy Act of 1974, *as amended, Public Law 93-579*, December 31, 1974.

National Institute of Standards and Technology (NIST) Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995.

## 7.3 Maintenance

SCG is responsible for updating this procedure and all supporting documents at least annually and after any significant change, including:

- Procedure or rules change
- Approver or procedure owner leaves the company or changes roles
- Significant change to the definitions
- Introduction of new systems/hardware
- Identification and remediation of security vulnerabilities
- Regulatory changes
- Changes to the risk profile.

The change management process and weekly team meetings should be monitored to identify significant changes that would require a procedure update.

Each document will be assigned an owner that is responsible for updating and maintaining the applicable procedure. The responsible party for this document is listed in the Responsibilities section.

## 7.4 Identification and Authentication Control Procedure

### *7.4.1 Identification and Authentication*

*Unique User Access*

All SCGSC users must be uniquely identified within the information system. SCG uses the following solution(s) and techniques on the system and application components to enforce unique identification and authentication:

- Information system: SCGSC Active Directory Server
- Cisco 5512-X Firewall: Restricts the types of remote operations

- Remote access: Unique UserID and password authentication
- Kerberos: Uses DES encryption to authenticate a user when logging into the system

SCG assigns individual accounts within the SCGSC system that are accessible only by that individual. Employees requiring access to the SCGSC must submit a request for access form, which is reviewed and approved by the SCG President and IT Director. The access accounts are reviewed quarterly by a System Administrator and renewed on a quarterly basis. These forms are scanned by the System Administrator and stored on the secured T drive. **(IA-2 Identification and Authentication (Organizational Users))**

Shared accounts are not permitted per SCG policy. Authentication to SCGSC requires the user to logon and provide his/her unique UserID and password to obtain access to the system. SCG uses Active Directory for identification and authentication of users accessing the SCGSC system.

The SCGSC system utilizes Microsoft Authentication capabilities that leverage Kerberos services. Utilization of this authentication framework allows for ticket granting services that resist replay attacks to the environment. Additional security can be configured when the NIDDK determines it is necessary for this system. The IT Director has set the FIPS local/group security policy flag in Windows Group Policy to ensure consistency with FIPS 140 Security Policy. The IT Director would alter the Group Policy settings if the FIPS policy changes to ensure compliance. **(IA-2 (8) Identification and Authentication (Organizational Users))**

*Multifactor Authentication*

No multifactor authentication is used for SCGSC system privileged accounts. The ISSO does not consider multifactor authentication necessary based on the assessment of associated risk. There are only four employees with system access accounts, which limits the risk and there is no sensitive PII (such as Social Security numbers, health/medical information, financial or payment information) contained or accessed through the system. The PII accessed through the system is limited to names, mailing addresses, phone numbers, and e-mail addresses, most of which is available through numerous other publically available sources. **(IA-2 (1) Identification and Authentication (Organizational Users))**

Non-privileged accounts are not permissible in the SCGSC system per SCG policy. **(IA-2 (2) Identification and Authentication (Organizational Users))**

No multifactor authentication is used for SCGSC system local access to privileged accounts. **(IA-2 (3) Identification and Authentication (Organizational Users))**

SCG does not implement multifactor authentication for remote access to privileged accounts for the SCGSC. Content that is provided by the applications that are hosted in the SCG Secure Cloud system is offered through a web connection to the public Internet, and is subject to the individual security models of the applications. These authentication capabilities are supported in the manner that the applications demand

and are restricted in nature to the applications that allow for public domain access. Non-privileged accounts are not supported in the SCGSC system by organizational policy. **(IA-2 (11) Identification and Authentication (Organizational Users))**

*Unique Device Access*

The SCGSC system uniquely identifies and authenticates the virtual machines before establishing a local connection. SCG uses Active Directory to support machine level authentication to the SCG Secure Cloud system environment. Machines are loaded with certificates from an AD central management capability using auto-enrollment. Each user and device account is assigned a unique Microsoft identification number, the Security Identifier (SID). **(IA-3 Device Identification and Authentication)**

Access to SCGSC is restricted to connections originating from designated IP addresses that use a specified port. All devices included in the SCGSC configuration are assigned device IDs by the IT Director, who identifies the device, location, connection required, and permissions needed. Unique identifiers are not to be reused for all types of devices, users, and operating systems for at least three (3) years after decommission status. All configuration items must be stored and managed by the Configuration Manager for compliance. System controls are in place to prevent the re-use of identifiers.

*Adding New Users/Devices*

New users and devices must follow SCG's access control procedures for the SCGSC. The process should include a formal request with approval and specification of privileges, assigning the user with a unique user ID, and ensuring that the new user ID is not a duplicate or a repeat. It is ***against*** SCG's policy to issue or generate shared user IDs.

*User Status*

Screening criteria for employees is outlined in the *Personnel Security Screening Policy* document. All employees who will access the SCGSC, must undergo a background security investigation (which includes fingerprinting) that is conducted by the NIH before the employee can received an ID badge and be granted access to NIH computer systems. If an employee has been screened by NIH for another contract, they will not have to be rescreened to obtain access to the SCGSC system. Prior to offering an applicant a position at SCG, the Human Resources Department reviews the applicant's employment application, verifies previous employment and other information on the application, and contacts references for the candidate. The applicant is informed that they will have to undergo fingerprinting and a background check as a condition of hire to work on the SCGSC system.

### *7.4.2 Identifier Management*

All privileged users are required to request access to the SCGSC using a request form that is approved by the SCG President/Business Owner and IT Director. Once approved, the forms are scanned by the System Administrator and stored on the secure T drive. All privileged users are provided unique accounts that permit access to the SCGSC system. Accounts must be unique as part of the Windows Operating System enforcement models. The System Administrator disables accounts as part of the offboarding process for the SCGSC system. When an employee who has access to the SCGSC resigns, the HR Manager notifies the System Administrator within 1 hour of the resignation, and the System Administrator disables the account. If an employee who has access to the SCGSC is transferred from the contract, the Program Manager notifies the System Administrator of the employee's change in status and requests that the account be disabled. Accounts are disabled rather than removed or deleted to prevent account reuse. The System Administrator runs a script on AD on a monthly basis to identify inactive accounts and then disables those accounts that have been inactive for 30 days. **(IA-4 Identifier Management)**

The four virtual machines in SCGSC are assigned unique device names and a unique SID. Devices are disabled rather than removed when they are no longer part of the system. User accounts are disabled after 30 days of inactivity.

### *7.4.3 Authenticator Management*

For all user identifiers, authenticator content must be applied.

*Initial Authenticator Content*

1. Verify the identity of the individual or device receiving the authenticator content.
   a. Users: Confirm the employee's UserID.
   b. Devices: Access policies restricting all access not originating from a designated IP address through a specified port.
2. Configure the initial authenticator content.
   a. Users: Assign a temporary password for new users that must be changed upon first access.
   b. Devices: Designated IP address through specified port.
3. Configure the authenticator content with sufficient strength:
   a. Users: By default, user authenticator content should meet strong complexity characteristics.
   b. Devices: By defaults, device authenticator content should be restricted to designated IP addresses through specified ports.
4. If applicable, default authenticator content must be changed for any new system components, network devices, or application features.

UserIDs are created by the IT Director and entered using Active Directory Users and Computers interface. The following format is used by the IT Director in creating UserIDs: first initial followed by last name. If there are two individuals with the same first initial and last name, the IT Director assigns a number to each of these UserIDs (e.g., jdoe1 and jdoe2).

Users are provided an account by the IT Director after the request for access is approved by the SCG President and IT Director. The initial account authenticator (password) is provided by the IT Director to the individual in person. The individual must change the password at first logon. The subsequent password is known only by the individual user, who is required by the signed rules of behavior agreement to keep it confidential.

The Windows Group Policy settings ensure that passwords adhere to policies that are implemented for the SCG Secure Cloud system.

The authenticator (password) rules are established in the Windows Group Policy settings by the IT Director and are enforced by this commercial off-the-shelf (COTS) system.

The IT Director personally manages these processes with in-person validation of identity and ensures that authenticators adhere to organizational policy. The default passwords for the SCG Secure Cloud system were all changed during installation by the System Administrator. The SCG IT Director conducts an in-person exchange of information to register and establish a user for accessing the SCGSC system. He also issues the username and temporary password to each employee approved for system access. The system is set to require that the password be changed upon first logon. **(IA-5 (3) In-Person or Trusted Third-Party Registration)**

The use of an initial/temporary password for system logons is permitted with an immediate change to a permanent password at first logon. **(IA-5 Authenticator Management)**

The SCGSC system uses Entrust and DigiCert SSL certificates to support PKI-based authentication. **(IA-5 (2) Authenticator Management)**

The SCG Secure Cloud system uses the Microsoft Kerberos authentication solution that effectively masks and encrypts password information, which meets this control. **(IA-6 Authenticator Feedback)**

The SCGSC system uses Entrust and DigiCert SSL certificates to support Cryptographic Module Authentication. **(IA-7 Cryptographic Module Authentication)**

*Forgotten/Compromised or Revoking Authenticators*

The IT Director implements administrative procedures for forgotten/compromised authenticators, and for revoking authenticators. If an employee forgets his/her password, he/she must contact the System Administrator and request a password change. A new temporary password would be provided to the employee by the System Administrator and the employee would be required to change the password upon system access.

1. In the event a password has been forgotten or compromised, users should contact the IT Director immediately.
2. Upon notification of a forgotten or compromised authenticator, the System Administrator should disable the account if needed and assign the user a new password.
3. If the authenticator needs to be revoked, the System Administrator must immediately disable the account or revoke the credential from the specified user.
4. For all authenticator content, instruct users on how to protect and safeguard authentication content from unauthorized disclosure or modification. As a rule, users must not:

a. Write down passwords.
b. Share passwords with anyone.
c. Store passwords on unencrypted and unprotected systems.

### *7.4.4 Authenticator Content*

Initial passwords are generated by the IT Director and provided in person to the privileged user following approval of the request for access. Users must change the password upon first access and the password must meet the rules for complexity enforced by the Windows Group Policy.

The SCG Secure Cloud system utilizes a Windows-based mechanism for password change that is secure and enforceable through Windows Group Policy settings.

Passwords are known only to the account holder and are encrypted by Microsoft to keep them from being discovered. The passwords are masked on the monitor and presented as a secure hash to the Operating System utilizing a symmetric key exchange style of approach, which adequately protects from password discovery.

Individuals are required to protect the confidentiality of their authenticators (passwords) as specified in the rules of behavior agreement. When a user logs on, the authenticator (password) remains encrypted and only a secure hash is exchanged with the MS Kerberos service protecting the password from discovery.

Passwords are not assigned by group or role. They are unique to each user. Therefore, group and membership changes are not applicable to the SCGSC system. A minimum password length of 8 characters for all users has been established for the Windows OS environment. There are no non-privileged users of the SCGSC. At least 75% of the characters must be changed when new passwords are created.

Only encrypted representations of passwords are stored in the SCGSC system. Passwords are masked when entered to maintain password protection. The System Administrator enforces password minimum and maximum lifetime restrictions of 1 and 60 days, respectively. Passwords cannot be reused for at least 24 generations per the settings in the Windows OS environment.

*Parameters*

Per SCG policy, password authentication must be enforced for the following systems, devices, and application components and meet the following password criteria:

- Information system
- Firewall
- Test systems
- Remote access

| Account Password Policy | Setting |
|---|---|
| Enforce password history | 24 passwords remembered |

| Account Password Policy | Setting |
|---|---|
| Maximum password age | 60 days |
| Minimum password age | 1 days |
| Minimum password length | 8 characters |
| Passwords must meet complexity requirements | Enabled |
| Passwords must contain at least 3 of the following | Uppercase, lowercase, number & special character |

| Account Lockout Policy | Setting |
|---|---|
| Account lockout duration | Until administrative reset |
| Account lockout threshold | 3 invalid logon attempts |
| Reset account lockout counter after | Locked until administrative reset |
| Inactive session timeout | 30 minutes |

Where applicable, authenticators must include the following:

- Uppercase characters of the English language (A through Z)
- Lowercase characters of the English language (a through z)
- Base 10 digits (0 through 9)
- Non-alphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;"'<>, ?/

The rules for password complexity, expiration, reuse frequency, and compromise are presented in Table 3.

**Table 3. Rules for SCGSC Access Passwords**

| SCGSC Access Password Rules | | |
|---|---|---|
| **Item** | **Description** | **System Setting** |
| Password Complexity (applies to both initial and subsequent passwords) | Passwords must have sufficient complexity to prevent other users from guessing them. Passwords are case sensitive. Passwords entered that do not meet these minimum requirements will not be accepted. | Password complexity requirements enabled; enforces minimum password complexity of at least one (1) character from each of the four character categories (A-Z, a-z, 0-9, and special characters), minimum length of 8 characters for all users |
| Initial Password Expiration | Initial password expires at the first logon when the user will be prompted to change the password | Enforce change of password at first logon |

| SCGSC Access Password Rules | | |
|---|---|---|
| **Item** | **Description** | **System Setting** |
| Subsequent Password Expiration | Password expires within 60 days of the date it was changed | Maximum password age = 60 days |
| Reuse of Old Passwords | Users cannot reuse old passwords within 24 generations | Enforce password history = 24 |
| Number of Password Entry Attempts Allowed | Users entering 3 consecutive incorrect passwords in 20 minutes will be locked out until the System Administrator releases the lock | Account lockout threshold = 3 invalid logon attempts<br>Account lockout duration = until System Administrator releases the lock |
| Account Lockout Policy | Accounts remain locked out until the System Administrator resets the account | Until Administrative reset |
| Inactive Session Timeout | Session times out after 30 minutes of inactivity | 30 minutes |
| Compromised Password | Users who lose or suspect their passwords are compromised must notify the IT Director and the Program Manager immediately. The IT Director will reset the password and enforce password change at first logon. | NA |

Additional guidelines for passwords include:

- First time passwords are set to a unique value for each user and must be changed by the user immediately after first login.
- Group, shared, or generic passwords are prohibited.
- Passwords may not contain the UserID.
- Passwords may not include the user's own (to the best of his or her knowledge) or a close friend or relative name, employee number, social security number, birth date, telephone number, or any information about him or her that the user believes could be readily learned or guessed.
- Passwords may not (to the best of the user’s knowledge) include common words from an English dictionary or a dictionary of another language with which the user has familiarity.
- Passwords may not (to the best of the user’s knowledge) contain commonly used proper names, including the name of any fictional character or place
- Passwords may not contain any simple pattern of letters or numbers such as "qwertyxx" or "xyz123xx".
- Passwords must not be written down and left in a place where unauthorized persons might discover them.

- User passwords should not be shared or revealed to anyone else including IT staff. Sharing passwords exposes the authorized user to responsibility for actions that the other party takes with the disclosed password. Similarly, except as otherwise provided by applicable policies, users should not perform any activity with passwords belonging to others.
- All passwords must be immediately changed if they are suspected of being disclosed or known to have been disclosed to anyone besides the authorized user.
- Passwords must not be stored in readable form in login scripts, application programs, Windows, programmable function keys, macros, or in other locations where unauthorized persons might discover them. Furthermore, users should not configure their software, including remote access software to retain their password for automatic log in, except by means of a company approved security device.
- Passwords expire after 60 days and accounts are disabled after 90 days of inactivity, where applicable. The Windows Group Policy settings establish the rules for a maximum of 60 days for password longevity.

*Use of Authenticator Content*

It is the responsibility of the IT Director and the System Administrators to verify that unencrypted static authenticator content is not embedded in applications or access scripts or stored on function keys. The following steps should be taken:

1. Review a sample of applications, access scripts, or functions.
2. Look for any authenticator content or references to authenticator content.
3. If authenticator content is identified, notify the IT Director immediately to remove it.

SCG does not issue HSPD12 smart cards as authenticator content.

### 7.5 Roles and Responsibilities

| Roles | Responsibilities |
|---|---|
| SCG Secure Cloud System Administrator | • Assisting information owners with controlling access to their resources.<br>• Promptly removing access from the system when requested.<br>• Reporting any unauthorized accesses that they discover. |
| Users | • Understanding responsibilities for safeguarding UserIDs and passwords, and immediately notifying the IT Director if they suspect that a password or other system credential has been compromised. |
| NIDDK SCGSC Management Team | • Ensuring that appropriate identification and authentication methods are implemented for the resources that they own, based on the classification and level of risk assigned to the resource.<br>• Confirming that appropriate identification and authentication methods for the information resources in their care are being used, instructing |

| Roles | Responsibilities |
|---|---|
| | users as to their usage, and reporting any compromises of these resources to the appropriate federal contacts. |
| IT Director | • Preparing guidelines and standards for user credentials; issuing and approving administrator credentials.<br>• Assigning responsibilities to specific information owner or delegate to ensure that proper authenticator management control is implemented.<br>• Verification for disabling and removing accounts. |
| Program Manager and IT Director | • Ensuring that SCG personnel understand and comply with the guidelines contained in this policy; promptly notifying information custodians of accounts that should be deactivated; and reporting any suspected violations or compromises of credentials to the IT Director, who notifies the NIDDK system owner and ISSO as required. |
| Developer | • Ensuring that his systems support the procedures and guidelines specified in this document. |

## 8. Employee Computer Security and Awareness Training

For SCG's access policies to provide effective security, all employees must recognize the importance of following and adhering to the developed security procedures. All staff will be informed of SCG's security policies through this document, which is issued to each new employee during orientation. Following an event or when heightened security measures are necessary, SCG will hold staff meetings to discuss access security controls and their importance in safeguarding SCG employees, facilities, equipment, information systems, and other assets. During orientation and trainings/meetings, SCG emphasizes the importance of reporting any suspicious activity, packages, and persons that might threaten the security of SCG, its employees, and its assets. All SCG employees who have access to the SCGSC system must complete annual Information Security and Privacy Awareness training offered by the National Institutes of Health (NIH). In addition, they must participate in the annual TT&E event for the SCGSC. Training requirements are detailed in the *Security Awareness and Training Policy and Procedures for the SCG Secure Cloud System* document.

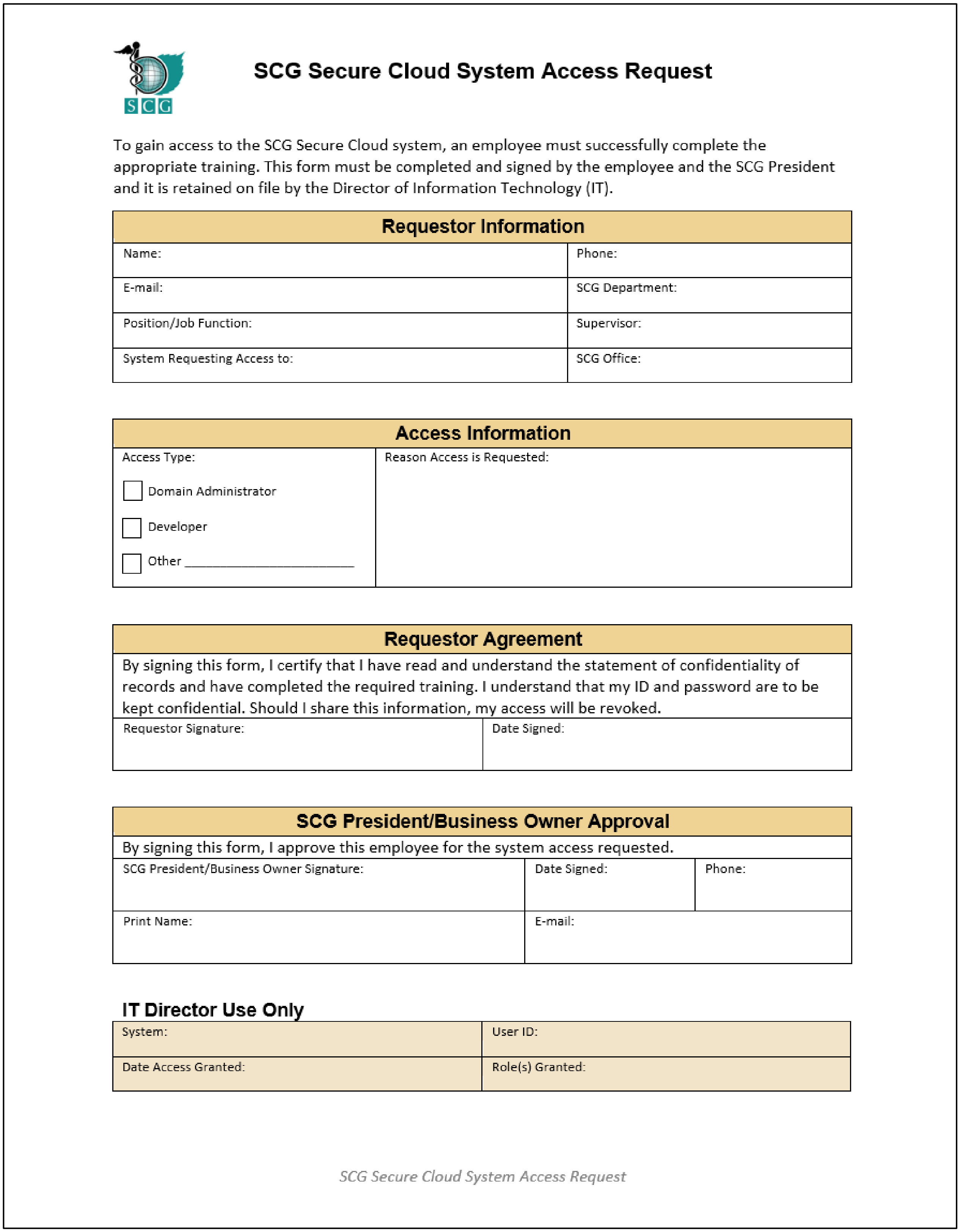
## 9. Unauthorized Access Response

If an unauthorized individual enters SCG's facility during business hours, whether by deceptive means or forceful entry, the receptionist and/or any SCG employee witnessing the access will immediately contact building security and the Vice President of Administration. Law enforcement will be contacted if necessary and actions will be taken to remove the individual from SCG's facility. If an unauthorized individual enters SCG's facility outside of business hours, the alarm will activate and e-mail an alert to the Vice President of Administration and the IT Director. The Vice President of Administration will contact law enforcement to investigate the intrusion. The Vice President of Administration and IT Director will enter the facility as soon as allowed by law enforcement to assess the damage, if any, to SCG's facilities, equipment, systems, and other assets. SCG will cooperate fully with law enforcement to investigate the crime and provide video footage of the perpetrator captured on our surveillance system.

Access logs and surveillance videos will be reviewed by the Vice President of Administration and the IT Director if a security breach is suspected.

SCG takes numerous measures to prevent unauthorized access to the SCGSC, including physical safeguards (e.g., facility and system access controls) and technical safeguards (e.g., access control, audit controls, user authentication). These controls allow SCG to restrict, monitor, and protect the confidentiality, integrity, and availability of the SCGSC information. In the event of an incident of unauthorized access, SCG has a plan to respond to the incident that will define and document the nature and scope of the computer security incident response, measures taken to prevent future incidents, and restoration of the system. These procedures are detailed in the *Incident Response Plan for the SCG Secure Cloud System* document.

# Appendix A: SCGSC System Access Request Form



SCG

## SCG Secure Cloud System Access Request

To gain access to the SCG Secure Cloud system, an employee must successfully complete the appropriate training. This form must be completed and signed by the employee and the SCG President and it is retained on file by the Director of Information Technology (IT).

| Requestor Information | |
|---|---|
| Name: | Phone: |
| E-mail: | SCG Department: |
| Position/Job Function: | Supervisor: |
| System Requesting Access to: | SCG Office: |

| Access Information | |
|---|---|
| Access Type:<br>□ Domain Administrator<br>□ Developer<br>□ Other ___________________ | Reason Access is Requested: |

| Requestor Agreement | |
|---|---|
| By signing this form, I certify that I have read and understand the statement of confidentiality of records and have completed the required training. I understand that my ID and password are to be kept confidential. Should I share this information, my access will be revoked. | |
| Requestor Signature: | Date Signed: |

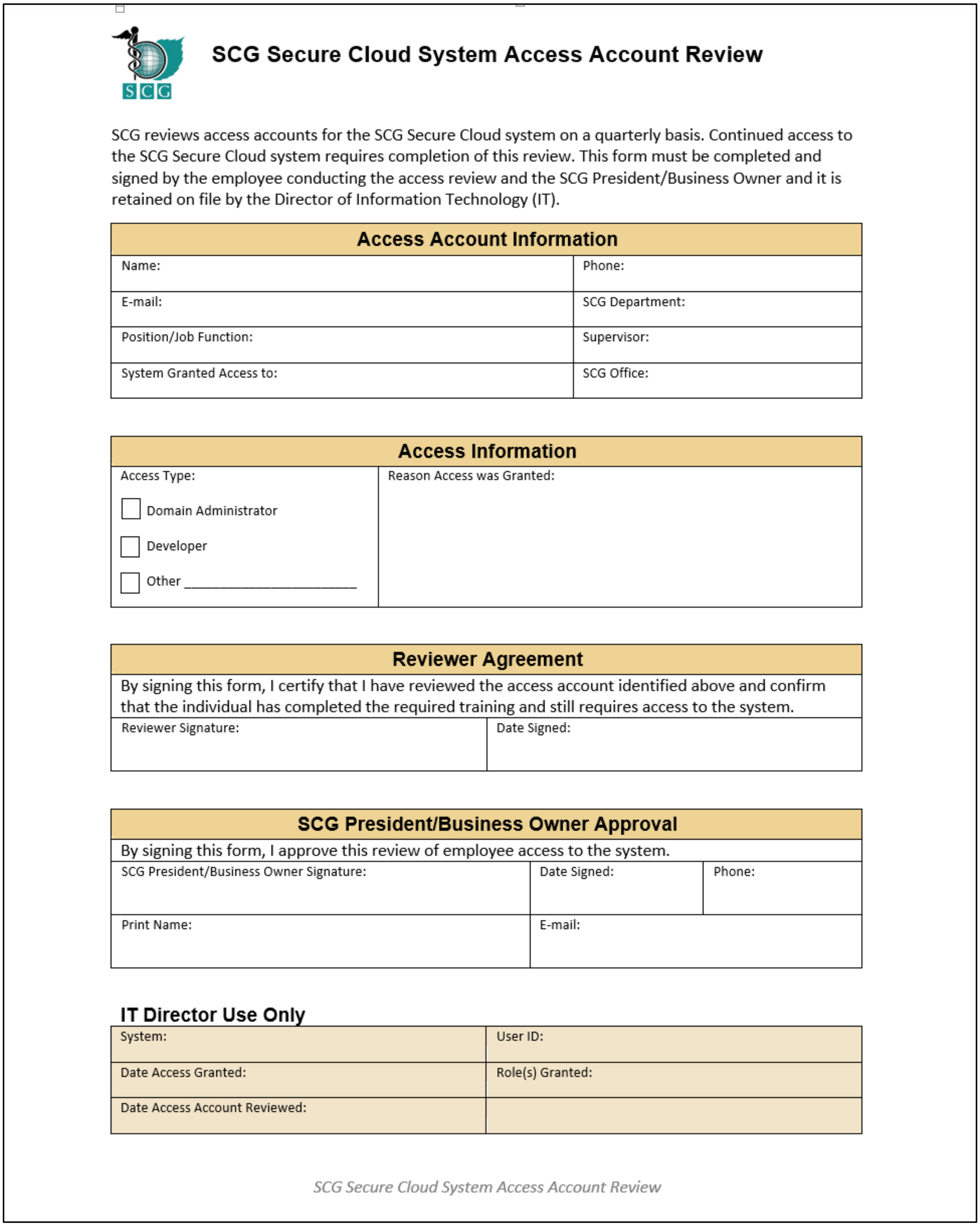
| SCG President/Business Owner Approval | | |
|---|---|---|
| By signing this form, I approve this employee for the system access requested. | | |
| SCG President/Business Owner Signature: | Date Signed: | Phone: |
| Print Name: | E-mail: | |

### IT Director Use Only

| | |
|---|---|
| System: | User ID: |
| Date Access Granted: | Role(s) Granted: |

*SCG Secure Cloud System Access Request*

# Appendix B: SCGSC System Access Account Review Form



## SCG Secure Cloud System Access Account Review

SCG reviews access accounts for the SCG Secure Cloud system on a quarterly basis. Continued access to the SCG Secure Cloud system requires completion of this review. This form must be completed and signed by the employee conducting the access review and the SCG President/Business Owner and it is retained on file by the Director of Information Technology (IT).

| Access Account Information | |
|---|---|
| Name: | Phone: |
| E-mail: | SCG Department: |
| Position/Job Function: | Supervisor: |
| System Granted Access to: | SCG Office: |

| Access Information | |
|---|---|
| Access Type:<br>□ Domain Administrator<br>□ Developer<br>□ Other ________________________ | Reason Access was Granted: |

| Reviewer Agreement | |
|---|---|
| By signing this form, I certify that I have reviewed the access account identified above and confirm that the individual has completed the required training and still requires access to the system. | |
| Reviewer Signature: | Date Signed: |

| SCG President/Business Owner Approval | | |
|---|---|---|
| By signing this form, I approve this review of employee access to the system. | | |
| SCG President/Business Owner Signature: | Date Signed: | Phone: |
| Print Name: | E-mail: | |

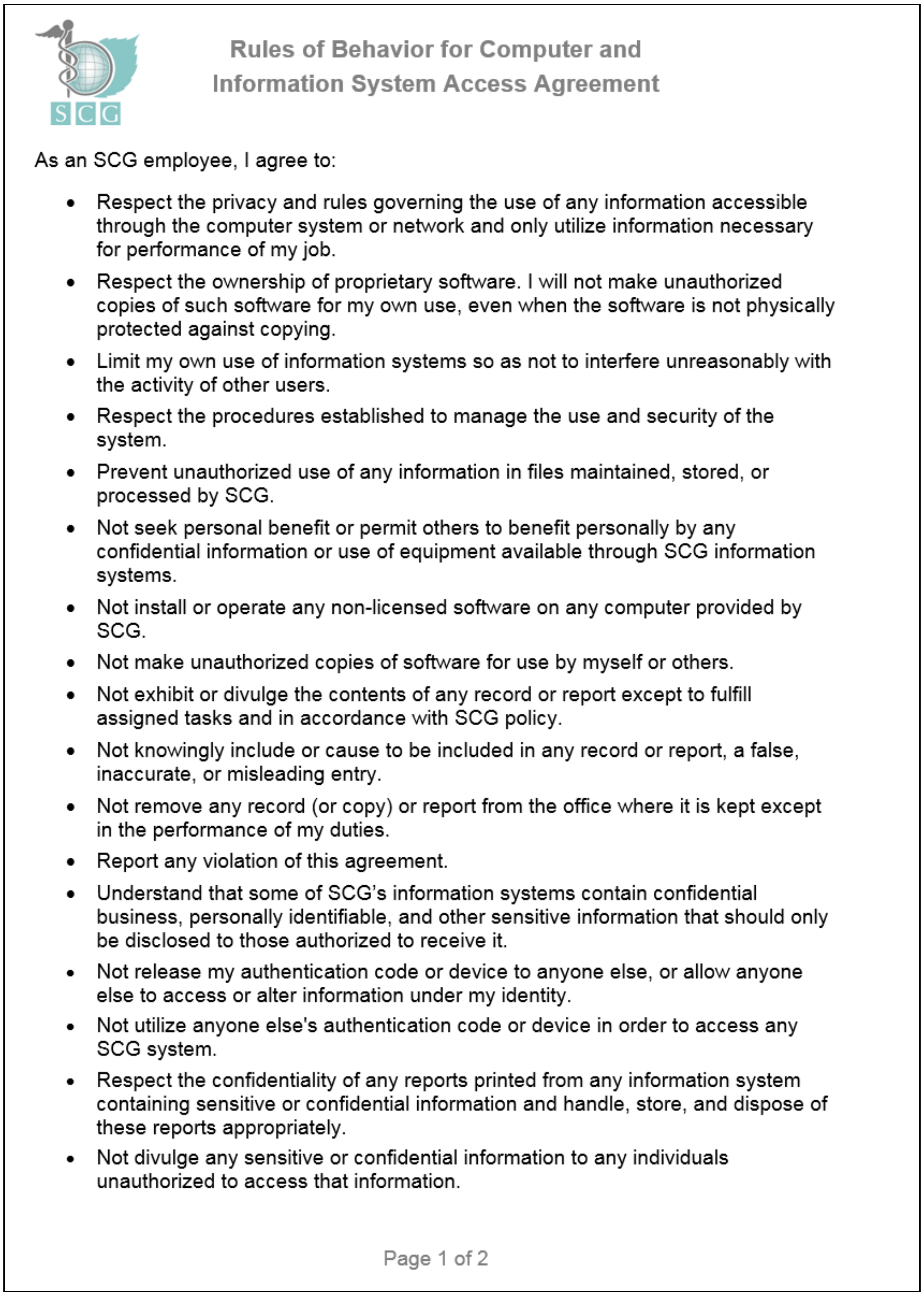
### IT Director Use Only

| | |
|---|---|
| System: | User ID: |
| Date Access Granted: | Role(s) Granted: |
| Date Access Account Reviewed: | |

*SCG Secure Cloud System Access Account Review*

## Appendix C: Rules of Behavior for Computer and Information System Access Agreement

All persons who are authorized to view data and access the SCGSC as developers or for system administration must read and comply with the Facility and Systems Access Policies and Procedures for the SCGSC, including the Rules of Behavior Agreement below.



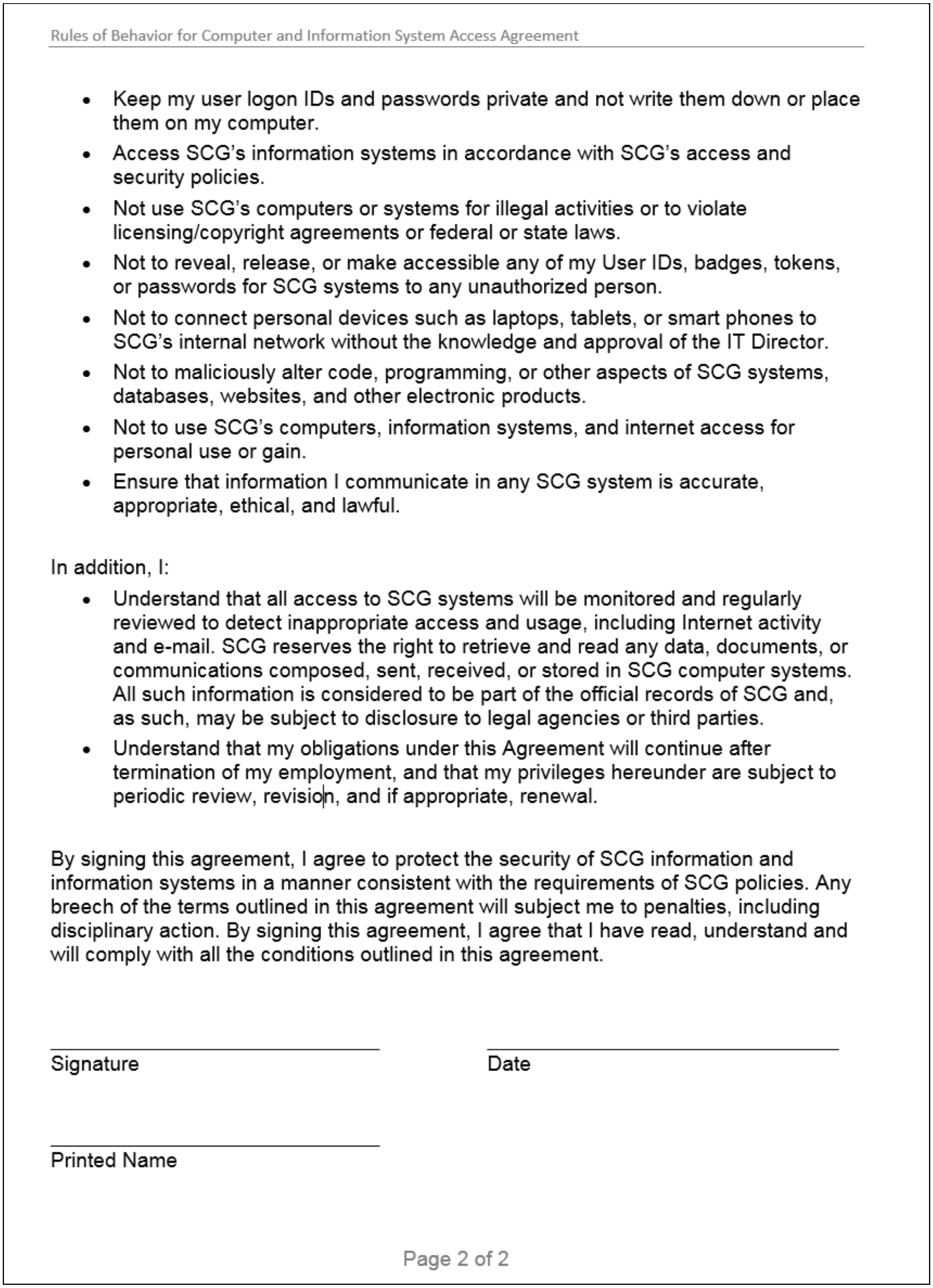
SCG

Rules of Behavior for Computer and Information System Access Agreement

As an SCG employee, I agree to:

- Respect the privacy and rules governing the use of any information accessible through the computer system or network and only utilize information necessary for performance of my job.
- Respect the ownership of proprietary software. I will not make unauthorized copies of such software for my own use, even when the software is not physically protected against copying.
- Limit my own use of information systems so as not to interfere unreasonably with the activity of other users.
- Respect the procedures established to manage the use and security of the system.
- Prevent unauthorized use of any information in files maintained, stored, or processed by SCG.
- Not seek personal benefit or permit others to benefit personally by any confidential information or use of equipment available through SCG information systems.
- Not install or operate any non-licensed software on any computer provided by SCG.
- Not make unauthorized copies of software for use by myself or others.
- Not exhibit or divulge the contents of any record or report except to fulfill assigned tasks and in accordance with SCG policy.
- Not knowingly include or cause to be included in any record or report, a false, inaccurate, or misleading entry.
- Not remove any record (or copy) or report from the office where it is kept except in the performance of my duties.
- Report any violation of this agreement.
- Understand that some of SCG's information systems contain confidential business, personally identifiable, and other sensitive information that should only be disclosed to those authorized to receive it.
- Not release my authentication code or device to anyone else, or allow anyone else to access or alter information under my identity.
- Not utilize anyone else's authentication code or device in order to access any SCG system.
- Respect the confidentiality of any reports printed from any information system containing sensitive or confidential information and handle, store, and dispose of these reports appropriately.
- Not divulge any sensitive or confidential information to any individuals unauthorized to access that information.

Page 1 of 2



- Keep my user logon IDs and passwords private and not write them down or place them on my computer.
- Access SCG's information systems in accordance with SCG's access and security policies.
- Not use SCG's computers or systems for illegal activities or to violate licensing/copyright agreements or federal or state laws.
- Not to reveal, release, or make accessible any of my User IDs, badges, tokens, or passwords for SCG systems to any unauthorized person.
- Not to connect personal devices such as laptops, tablets, or smart phones to SCG's internal network without the knowledge and approval of the IT Director.
- Not to maliciously alter code, programming, or other aspects of SCG systems, databases, websites, and other electronic products.
- Not to use SCG's computers, information systems, and internet access for personal use or gain.
- Ensure that information I communicate in any SCG system is accurate, appropriate, ethical, and lawful.

In addition, I:

- Understand that all access to SCG systems will be monitored and regularly reviewed to detect inappropriate access and usage, including Internet activity and e-mail. SCG reserves the right to retrieve and read any data, documents, or communications composed, sent, received, or stored in SCG computer systems. All such information is considered to be part of the official records of SCG and, as such, may be subject to disclosure to legal agencies or third parties.
- Understand that my obligations under this Agreement will continue after termination of my employment, and that my privileges hereunder are subject to periodic review, revision, and if appropriate, renewal.

By signing this agreement, I agree to protect the security of SCG information and information systems in a manner consistent with the requirements of SCG policies. Any breech of the terms outlined in this agreement will subject me to penalties, including disciplinary action. By signing this agreement, I agree that I have read, understand and will comply with all the conditions outlined in this agreement.

______________________________
Signature

______________________________
Date

______________________________
Printed Name

## Appendix D: References on Cybersecurity

The following references illustrate public laws that have been issued on the subject of cybersecurity and should be used to demonstrate SCG's responsibilities associated with protection of its cyber assets.

- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-53, Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations Revision 4, April 2014.
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-100 "Information Security Handbook: A Guide for Manager" October 2006.
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-46, Rev 1 "Guide to Enterprise Telework and Remote Access Security" June 2009.
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-113 "Guide to SSL VPNs" July 2008.
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-114 "User's Guide to Securing External Devices for Telework and Remote Access" November 2007.
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-121, Rev 1, "Guide to Bluetooth Security" June 2012.
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-48, Rev 1, "Guide to Securing Legacy IEEE 802.11 Wireless Networks" July 2008.
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-94 "Guide to Intrusion Detection and Prevention Systems (IDPS)" February 2007.
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-97 "Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i" February 2007.
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-124, Rev 1, "Guidelines for Managing the Security of Mobile Devices in the Enterprise" June 2013.
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-77 "Guide to IPsec VPNs" December 2005.