The Scientific Consulting Group, Inc.

Media Protection Policy and Procedures

for the

SCG Secure Cloud System

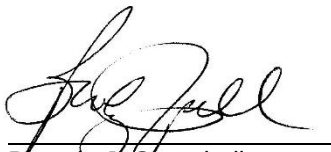
Version 1.4

May 19, 2016

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

Media Protection Policy and Procedures Approval

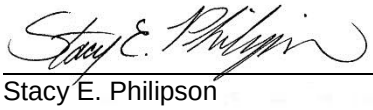
The Media Protection Policy and Procedures for the SCG Secure Cloud (SCGSC) system must be approved by the President of SCG, the Vice President of Administration, and the Information Technology (IT) Director. The undersigned acknowledge that they have reviewed the SCG Secure Cloud Media Protection Policy and Procedures and agree with the information presented in this document. This document will be reviewed annually and any changes to media protection policy and procedures deemed necessary will be coordinated with, and approved by, the undersigned or their designated representatives. The Media Protection Policy and Procedures for the SCGSC system will be reviewed at least every three (3) years and updated as required.



5/19/16

Beverly J. Campbell
President

DATE



5/19/16

Stacy E. Philipson
Vice President of Administration

DATE

5/19/16

Chuck C. Lee
Director of Information Technology

DATE

Document Information and Revision History

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

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
1.0	1/30/15	B. Campbell	Draft Policy
1.1	2/16/15	C. Berry/K. Martinez	Document review, minor modifications
1.2	2/17/15	B. Campbell	Document review, minor modifications
1.3	2/27/15	B. Campbell	Minor modifications throughout document
1.4	5/19/16	B. Campbell	Minor modifications 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 define SCG's Media Protection Policy and Procedures for managing risks from media access, media storage, media transport, and media protection for the SCG Secure Cloud system (SCGSC). It facilitates the implementation of the security control requirements for the Media Protection control family, as identified in the National Institutes of Standards and Technology (NIST) Special Publication 800-53. The media protection program helps SCG implement security best practices with regard to the SCGSC system media usage, storage, and disposal.

2. Scope

The scope of this policy is applicable to the SCGSC system that was developed and is managed 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 users (SCG employees, contractors, vendors, or others) of SCGSC resources are responsible for adhering to this policy.

3. Intent and Distribution

The SCGSC information security policy serves to be consistent with best practices associated with information security management. It is the intention of this policy to establish a media protection capability throughout SCG to help the organization implement security best practices with regard to the SCGSC system media usage, storage, and disposal.

This document is directed primarily to the SCG personnel responsible for media storage, transport, and protection for the SCGSC system. It is disseminated to SCG's IT staff and available to all SCG employees via the SCG Intranet.

4. Policy and Procedures

SCG has chosen to adopt the Media Protection principles established in NIST SP 800-53 "Media Protection," Control Family guidelines, as the official policy for the SCGSC system. The following subsections outline the Media Protection standards that constitute SCG's policy for the SCGSC. SCG employees are bound to this policy, and must develop or adhere to a program plan that demonstrates compliance with the policy.

4.1 MP-1 Media Protection Procedures

SCG must develop, adopt, or adhere to a formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. This document fulfills this requirement.

4.2 MP-2 Media Access

SCG must restrict access to digital (e.g., disks, magnetic tapes, external/removable hard drives) media to authorized personnel using physical access controls and safeguards.

Note: *The use of non-digital media (e.g., documents, microfilm) is prohibited for the SCGSC system.*

Assessment of risk must guide the selection of media for storage, transport, backup, etc., and the associated information contained on that media requiring restricted access. Unmarked media must be protected until the media are reviewed and appropriately marked, at which time the commensurate measure will be employed.

SCG is required to document the processes required to ensure media and the information on the media of the SCGSC system are protected from unauthorized access. This includes, but is not limited to, backup media such as tapes or disks. Only approved SCG removable digital media must be used to store data. The SCGSC backup tapes to be transported to and stored at the alternate site in Staunton, VA, are encrypted (128-bit AES encryption with an 8-character pass phrase key) to protect the Personally Identifiable Information (PII) contained on the tapes.

Note: *The backup tapes contain no financial or medical records, Social Security numbers, or similar highly sensitive PII; only names and mailing and email addresses are contained in the SCGSC system and these are purged every 30 days.*

All digital backup media at SCG's Gaithersburg facility are stored in the locked fire safe located in the IT Director's office and are accessed and transported only by SCG IT staff with the knowledge and authorization of the IT Director. The digital backup media at Frederick are stored in a locked fireproof safe in the facility. In addition, monthly digital backup media for SCGSC are stored in Staunton, VA (about 185 miles from Gaithersburg). Backups of SCGSC will be stored at all three locations (Gaithersburg and Frederick) a minimum of 3 years or for the life of the contract with the National Institute of Diabetes and Digestive and Kidney Diseases (NIDDK), whichever is longer.

4.3 MP-3 Media Marking

SCG must mark all removable digital media (i.e., backup tapes, hard drives) containing private information indicating the distribution limitations, handling caveats, and applicable security markings. There are no exceptions to the marking requirement for the SCGSC system. The assessment of risk must guide the selection of media requiring marking. For the SCGSC system backup tapes, each tape is labeled with the following:

- SCGSC Backup Tape
- Date of Backup – for example, 3/31/16 (monthly)
- Sensitive But Unclassified Data – To be handled and opened only by authorized SCG IT staff

Digital media must be marked to the most restrictive protection level of the information contained on the media. All marking requirements and guidelines are approved by the IT Director and the System Owner.

4.4 MP-4 Media Storage

SCG must physically control and securely store digital media (e.g., disks, magnetic tapes, external/removable hard drives) within secure areas using physical security controls and

safeguards. Only the SCG IT staff are authorized to store, retrieve, and use backup tapes for the SCGSC system.

The assessment of risk must guide the selection of media and associated information contained on that media requiring physical protection. “Sensitive but Unclassified” information stored by SCG for the SCGSC system must be physically controlled, and safeguarded in the manner prescribed for the highest classification level of the information contained on the media until the media is sanitized or destroyed. SCG stores all digital media associated with the SCGSC system is physically secure locations. The media are stored in locked rooms inside locked cabinets accessible only by authorized SCG IT staff.

Any digital media (i.e., backup tapes) for the SCGSC system transported outside the secure facility at Gaithersburg are encrypted to protect the sensitive information. The cryptographic mechanism used maintains the confidentiality and integrity of the information, and it is commensurate with the sensitivity of the information. SCG uses 128-bit AES encryption with an 8-character pass phrase key to protect tape backups transported to the Staunton, VA facility for storage.

Digital media must be protected until the media are destroyed or sanitized using approved equipment, techniques, and procedures. (Refer to MP-6 Media Sanitization and Disposal.)

A secure, environmentally appropriate, secure storage area must be available for archiving digital media for the SCGSC system. SCG has designated storage space at both the Gaithersburg and Frederick facilities that meet these requirements. Archived data for the SCGSC system must be retained for a minimum of three (3) years, but may be retained for up to seven (7) years. Upon reaching the seven (7)-year timeframe for archived digital media, the media are automatically released to the SO for disposition in accordance with retention schedules related to the SCGSC system. The SO is responsible for overseeing the proper disposal of digital media that are no longer needed.

At least semi-annually, SCG IT personnel must test a statistical sample of SCGSC archived digital media, to ensure that the digital media are in good condition and are readable.

4.5 MP-5 Media Transport

SCG must protect and control digital (i.e., backup tapes) for the SCGSC system during the transport outside of controlled areas. In addition, SCG must restrict access to such media to authorized personnel, and maintain accountability for information asset media during transport outside of controlled areas.

For moderate information systems, such as the SCGSC system, all digital media must be protected and controlled during transport outside of controlled areas using defined security measures (i.e., cryptography). Accountability for information system media must be maintained during transport outside of controlled areas using defined security measures (i.e., cryptography) that are SCG-approved, FIPS 140-2 validated, or compliant encryption technologies. Activities associated with transport of information system media must be restricted to authorized personnel. For the SCGSC, the only digital media transported are the backup tapes, which are transported on a monthly basis from SCG Gaithersburg to the Staunton, VA facility. The SCG President transports the backup tapes to the secure storage area in Staunton, VA. The tapes are encrypted using 128-bit AES

encryption with an 8-character pass phrase key to protect the “Sensitive but Unclassified” information on the tapes.

The physical and technical security measures for the protection of digital media for the SCGSC must be approved by the SO, commensurate with the sensitivity of the information residing on the media, and consistent with any federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The SO, SCG’s President, has approved the physical and technical security measures outlined in this policy and procedures document to protect the digital media for the SCGSC when it is transported.

4.6 MP-6 Media Sanitization

All SCGSC system digital media must be sanitized by using approved equipment, techniques, and procedures prior to disposal, release out of organizational control, or release for reuse. Sanitization is the process used to remove information from information system media such that there is reasonable assurance that the information cannot be retrieved or reconstructed. All electronic information and licensed software must be removed when disposing of computers with hard drives. IT resources and digital storage media must be cleaned of all information.

Sanitization mechanisms with the strength and integrity commensurate with the sensitivity of the information must be employed. For sanitizing SCGSC backup tapes for reuse, SCG performs Long Erase on the digital media using Symantec BackupExec, which ensures that the information on the media cannot be recovered. This sanitization method has been approved by the SO and the IT Director, who deem them appropriate for the sensitivity of the information contained on the digital media for the SCGSC system.

SCG sanitizes hard drives using low-level formatting. This writes 0s to all sectors on the hard drive making rendering recovery of the data infeasible.

Note: After overwriting, the hard drive is still physically functional and can accept formatting. Therefore, the media can be reissued and used within SCG.

SCG accomplishes digital media destruction by shredding the media (i.e., backup tape) when it is no longer needed. Before any digital media or hard drive is destroyed the IT Director confirms with the SO that the media is no longer needed and has been approved for destruction. The IT Director may request such confirmation in writing (e.g., e-mail message).

4.7 MP-7 Media Use

SCG prohibits the use of portable storage devices in the SCGSC environment.

5. Roles and Responsibilities

5.1 IT Director

The IT Director has the following responsibilities with respect to media protection:

- Ensure that an assessment of risk guides the selection of media and associated information contained on that media requiring protection and restricted access.

- All backup tapes are marked before they are used in the Tandberg tape backup device. Once the backup is complete the IT Director confirms the markings are correct before the tape is stored.
- Document the processes required to ensure media and the information on the media of the SCGSC system are protected from unauthorized access.
- Ensure data can be stored only on approved SCG removable digital media.
- Physically control and securely store SCGSC system media within controlled areas.
- Document in policy and procedures the specific measures taken to protect media based on requirements of the information it holds.
- Protect information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.
- Maintain a secure, environmentally appropriate facility for archiving digital media for the SCGSC.
- Document in policy and procedures the media requiring protection during transport and the specific measures taken to protect such transported media.
- Employ cryptography as needed to protect information stored on digital media during transport outside of controlled areas.
- Restrict activities associated with transport of digital media to authorized personnel.
- Consult with appropriate IT and programmatic staff to determine if and when digital media and/or hard drives should be destroyed.
- Prior to sanitization of media, ensure that all SCGSC records are properly identified, retrieved from the media, and processed in accordance with company policy.
- Prior to sanitizing, disposing of, or destroying media, ensure that the media and information are approved for destruction and confirm they are no longer needed.
- Track, document, and verify media sanitization and disposal actions.
- Create and retain a log of all media destroyed.
- Develop policy and standard operating procedures (SOPs) for SCGSC media sanitization.
- Ensure that users are trained on these policies and SOPs.
- Ensure that sanitization equipment and procedures are tested to verify correct performance.

5.2 SCG IT Personnel

The IT personnel have the following responsibilities with respect to SCGSC media protection:

- Mark SCGSC digital media (i.e., backup tape) appropriately in accordance with the policies and procedures set forth by SCG in this document.
- Affix printed label to each backup tape with the required information. Also affix printed label to the tape jacket with the required information to identify and retrieve the tape and to designate the sensitivity of the data it contains.
- Release archived digital media that have reached the seven (7)-year timeframe to the NIDDK System Owner for disposal.
- Semi-annually test a statistical sample to ensure that archived digital media are in good condition and are readable.
- Protect and control media during transport outside of controlled areas.
- Restrict activities associated with transport of media to authorized personnel.
- Sanitize all media prior to disposal or release for reuse.
- Use approved equipment, techniques, and procedures for sanitizing and disposing of media.
- Abide by documented procedures and standards for media sanitization and disposal.
- Test sanitization equipment procedures annually to verify correct performance.

6. Definitions

- **Authentication** – the process of verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
- **Availability** – ensuring timely and reliable access to and use of information.
- **Confidentiality** – preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.
- **Controlled Access Area** – any area or space within a facility for which SCG has confidence that the physical and procedural protections provided are sufficient to meet SCG's authorized access requirements established for protecting the information and/or information system (generally a controlled area is within a facility not owned or managed solely by SCG). This area may be within a publicly accessible facility or a controlled access facility.
- **Controlled Access Facility** – a facility where access is physically or procedurally controlled at the facility entrance and is limited to individuals authorized to access the facility. This may include organizations that inhabit the facility other than SCG.
- **Controlled Area** – any area or space for which SCG has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system.
- **Controlled Limited Access Area** – an area or office space, generally within a controlled access area, that further restricts access to a smaller subset of authorized individuals.

- **Information Security** – the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
- **Information Security Policy** – an aggregate of directives, regulations, rules, and practices that prescribe how an organization manages, protects, and distributes information.
- **Information System** – a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
- **Information Type** – a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation.
- **Integrity** – guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity.
- **Labeling** – the application or use of security attributes with regard to internal data structures within the information system.
- **Marking** – the application or use of human-readable security attributes.
- **Media** – physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, printouts (but not including display media) onto which information is recorded, stored, or printed within an information system. Digital media include diskettes, tapes, removable hard drives, flash/thumb drives, compact disks, digital video disks; examples of non-digital media are paper or microfilm. This term also applies to mobile computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices).
- **Media Sanitization** – actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.
- **Overwriting [media]** – writing to the entire media storage space with a predetermined pattern of meaningless information, usually 0s, 1s, and random or pseudo-random data, effectively rendering any data unrecoverable. Reformatting media is neither sufficient or nor equivalent to overwriting.
- **Protection Level Markings** – SCG has three basic protection level markings related to data or information confidentiality. These protection levels can be augmented in marking to include the content and/or governing statute (e.g., “Restricted – PII,” “Restricted – Privacy Act,” “Restricted – Controlled Unclassified Information”). The three protection levels and associated markings are as follows:
    - **Unrestricted:** Unrestricted data are accessible to anyone for any reason.
    - **Restricted:** Restricted data are not accessible to the general public. Restricted data are accessible to data subjects or data suppliers. Restricted data is accessible only to authorized users.

  - **Protected:** Protected data are not accessible to the general public. Protected data are accessible only to authorized users.

- **Removable Media** – includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, DVDs) and non-digital media (e.g., paper, microfilm).
- **Risk** – the level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, other organizations, individuals, or the Nation resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
- **Risk Assessment** – the process of identifying risks to SCG operations (including mission, functions, image, or reputation), SCG assets, other organizations, individuals, or the Nation arising through the operation of the information system. Part of risk management, synonymous with risk analysis, incorporates threat and vulnerability analyses, and considers mitigations provided by planned or in place security controls.
- **Risk Management** – the process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, other organizations, individuals, or the Nation resulting from the operation of an information system, and includes: (1) the conduct of a risk assessment; (2) the implementation of a risk mitigation strategy; and (3) employment of techniques and procedures for the continuous monitoring of the security state of the information system.
- **Sanitization** – the process used to remove information from information system media such that there is reasonable assurance that the information cannot be retrieved or reconstructed.
- **Secured Means of Transport** – secured means of transport is determined by documented risk assessments and varies depending on the media. Secure transport of non-digital media includes, but is not limited to, media contained in marked and addressed envelopes within an “official” commercial carrier container (e.g., United Parcel Service, FedEx, etc.). Secure transport of digital media includes, as a minimum, use of encryption. Transport protections for some small handheld device type media may include, but are not limited to, password protection and electronic deactivation or erasure if control has been compromised.
- **Signature (of an individual)** – a mark or sign made by an individual to signify knowledge, approval, acceptance, or obligation. Can be accomplished manually, sometimes referred to as a “wet signature,” or electronically.
- **User** – individual or (system) process authorized to access an information system.
- **Written** – or “in writing” means to officially document the action or decision and includes a signature. The documentation can be accomplished manually or electronically.

7. Relevant References

- E-Government Act of 2002, Public Law 107-347, Title III, Federal Information Security Management Act (FISMA) as amended
- Freedom of Information Act (FOIA), 5 U.S.C. § 552, as amended by Public Law 104-231, 110 Stat. 3048, Electronic Freedom of Information Act Amendments of 1996
- Clinger-Cohen Act of 1996, Public Law 104-106
- Paperwork Reduction Act of 1995 (44 USC 3501-3519)
- Privacy Act of 1974 (5 USC § 552a) as amended
- USA PATRIOT Act of 2001, Public Law 107-56
- Code of Federal Regulations, Part 5 Administrative Personnel, Subpart C—Employees Responsible for the Management or Use of Federal Computer Systems, Section 930.301 through 930.305 (5 C.F.R 930.301-305)
- Office of Management and Budget (OMB) Memorandum M-06-16, “Protection of Sensitive Agency Information”, June 2006
- OMB Circular A-130, “Management of Federal Information Resources”, Appendix III, “Security of Federal Information Resources”, November 2000
- Federal Information Processing Standards (FIPS) 140-2, Security Requirements for Cryptographic Modules, May 2001
- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006

Appendix A: Storage Protection Guidelines

Information Confidentiality Level/Protection Level	Media Storage Protected Environment Guidelines (selection of acceptable or optimum may be risk dependent)		
	Unacceptable	**Acceptable**	**Optimum**
Moderate/ "Sensitive but Unclassified"	Anywhere in a public space	• In a controlled access facility • In locked office space • In a labeled file cabinet or encrypted (digital media)	• In a controlled access facility • In a controlled access area • In locked, labeled file cabinet or encrypted (digital media)

Appendix B: References

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

- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-60 "Guide for Mapping Types of Information and Information Systems to Security Categories" August 2008.
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-111 "Guide to Storage Encryption Technologies for End User Devices" November 2007.
- 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 800-88 "Guidelines for Media Sanitization" September 2006.

Appendix C: Acronyms

AES	Advanced Encryption Standard
DVD	Digital Video Disk
C	Mobile (or Cell) Phone
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
IT	Information Technology
LSI	Large-Scale Integration
NIDDK	National Institute of Diabetes and Digestive and Kidney Diseases
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PII	Personally Identifiable Information
SAN	Storage Area Network
SCGSC	Scientific Consulting Group Secure Cloud
SOP	Standard Operating Procedures
W	Work Phone