



**The Scientific Consulting Group, Inc.**

# **Audit and Accountability Policy and Procedures**

**for the**

## **SCG Secure Cloud System**

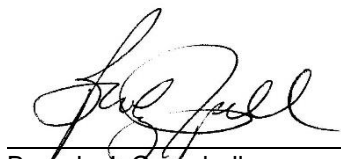
***Version 1.3***

***May 19, 2016***

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

## **Audit and Accountability Policy and Procedures Approval**

The Audit and Accountability Policy and Procedures for the SCG Secure Cloud system must be approved by the SCG President, the Vice President of Administration, and the Director of Information Technology. The undersigned acknowledge that they have reviewed the SCG Secure Cloud Audit and Accountability Policy and Procedures and agree with the information presented in this document. This document will be reviewed annually and any changes to audit and accountability policy and procedures deemed necessary will be coordinated with, and approved by, the undersigned or their designated representatives.



Beverly J. Campbell  
President

5/19/16

DATE



Stacy E. Philipson  
Vice President of Administration

5/19/16

DATE



Chuck C. Lee  
Director of Information Technology

5/19/16

DATE

## Document Information and Revision History

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

Document Revision and History			
Revision	Date	Author	Comments
1.0	2/25/15	B. Campbell	Initial draft document
1.1	2/26/15	B. Campbell	Edits throughout document
1.2	11/19/15	B. Campbell	Edits throughout document
1.3	5/19/16	B. Campbell	Edits 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

<b>1. Purpose .....</b>	<b>5</b>
<b>2. Scope and Applicability .....</b>	<b>5</b>
<b>3. Background.....</b>	<b>5</b>
<b>4. Procedures.....</b>	<b>5</b>
4.1 AU-1 – Audit and Accountability Policy and Procedures .....	5
4.2 AU-2 – Auditable Events .....	5
4.3 AU-3 – Content of Audit Records .....	15
4.4 AU-4 – Audit Storage Capacity .....	15
4.5 AU-5 – Response to Audit Processing Failures .....	15
4.6 AU-6 – Audit Review, Analysis, and Reporting .....	16
4.7 AU-7 – Audit Reduction and Report Generation .....	16
4.8 AU-8 – Time Stamps.....	16
4.8.1 AU-8 (1) – Time Stamps .....	17
4.9 AU-9 – Protection of Audit Information .....	17
4.9.1 AU-9 (4) Protection of Audit Information .....	17
4.10 AU-11 – Audit Record Retention.....	17
4.11 AU-12 – Audit Generation.....	17
<b>5. Roles and Responsibilities .....</b>	<b>18</b>
5.1 SCG President .....	18
5.2 Domain Administrators.....	18
<b>Appendix A: Definitions.....</b>	<b>20</b>
<b>Appendix B: Acronyms.....</b>	<b>21</b>

## **1. Purpose**

The purpose of this SCG Secure Cloud (SCGSC) Audit and Accountability Policy and Procedures document is to facilitate the implementation of SCG security control requirements for the Audit and Accountability control family, as identified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3: *Recommended Security Controls for Federal Information Systems and Organizations*.

## **2. Scope and Applicability**

These procedures cover the SCGSC system only. They apply to all SCG employees and contractors/consultants granted an account to access the SCGSC system.

## **3. Background**

SCG is responsible for ensuring that the SCGSC system meets the minimum security requirements through the use of security controls defined in the NIST SP 800-53, Revision 3. This document addresses the procedures and standards set forth by SCG, and in compliance with, the audit and accountability family of controls found in NIST SP 800-53, Revision 3.

## **4. Procedures**

### **4.1 AU-1 – Audit and Accountability Policy and Procedures**

This document defines SCG's audit and accountability policy and procedures for the SCGSC system. It is disseminated to all SCG employees, consultants, and contractors with user accounts for the SCGSC system. The policy and procedures are reviewed at last once every three (3) years and the document is updated as needed.

### **4.2 AU-2 – Auditable Events**

Audit logging must be determined, based on a risk assessment and mission needs, that the SCGSC system must be capable of auditing for certain events. The following events must be identified within server audit logs:

- Server startup and shutdown
- Loading and unloading of services
- Installation and removal of software
- System alerts and error messages
- User logon and logoff
- Windows Local Policy logon, access, or modification
- System administration activities
- Attempted and successful accesses to sensitive information, files, and systems
- Account creation, modification, or deletion
- Modifications of privileges and access controls

The following events must be identified within application and database audit logs:

- Modifications to the application
- Application alerts and error messages
- User logon and logoff
- System administration activities
- Accesses to information and files
- Account creation, modification, or deletion
- Modifications of privileges and access controls

The SQL Audit log includes the following events for audit log reports:

- Database Transaction Logs—These logs track every transaction within a specific database. All entries in these logs are designed to meet ACID compliance. ACID stands for atomicity, consistency, isolation, and durability. All the transactions must fulfill these characteristics:
  - An **atomic transaction** is either fully completed, or is not begun at all
  - A transaction enforces **consistency** in the system state by ensuring that at the end of any transaction the system is in a valid state
  - When a transaction runs in **isolation**, it appears to be the only action that the system is carrying out at one time
  - A transaction is **durable** meaning that once it has been successfully completed, all of the changes it made to the system are permanent
- Login Audit
  - Failed logins only
  - Successful logins only
  - Both failed and successful logins
- Server Audit – Table 1 shows the Audit Action Groups that can be logged in the audit log. The action groups highlighted in yellow in the table below are the ones SCG has selected to log.

**Table 1. Audit Action Groups Logged in the Audit Log**

Action Group Name	Description
APPLICATION_ROLE_CHANGE_PASSWORD_GROUP	This event is raised whenever a password is changed for an application role. It is equivalent to the <a href="#">Audit App Role Change Password Event Class</a> .
AUDIT_CHANGE_GROUP	This event is raised whenever any audit or audit specification is created, modified, or deleted. Any change to an audit is audited in that audit. It is

Action Group Name	Description
	equivalent to the <a href="#">Audit Change Audit Event Class</a> .
BACKUP_RESTORE_GROUP	This event is raised whenever a backup or restore command is issued. It is equivalent to the <a href="#">Audit Backup/Restore Event Class</a> .
BROKER_LOGIN_GROUP	This event is raised to report audit messages related to Service Broker transport security. It is equivalent to the <a href="#">Audit Broker Login Event Class</a> .
DATABASE_CHANGE_GROUP	This event is raised whenever any database is created, altered, or dropped. It is equivalent to the <a href="#">Audit Database Management Event Class</a> .
DATABASE_LOGOUT_GROUP	This event is raised when a contained database user logs out of a database. It is equivalent to the <a href="#">Audit Database Logout Event Class</a> .
DATABASE_MIRRORING_LOGIN_GROUP	This event is raised to report audit messages related to database mirroring transport security. It is equivalent to the <a href="#">Audit Database Mirroring Login Event Class</a> .
DATABASE_OBJECT_ACCESS_GROUP	<p>This event is raised whenever database objects such as message type, assembly, contract are accessed. This event also is raised for any access to any database. It is equivalent to the <a href="#">Audit Database Object Access Event Class</a>.</p> <p><b>Note: This could potentially lead to large audit records.</b></p>
DATABASE_OBJECT_CHANGE_GROUP	<p>This event is raised when a CREATE, ALTER, or DROP statement is executed on database objects, such as schemas. This event is raised whenever any database object is created, altered or dropped. It is equivalent to the <a href="#">Audit Database Object Management Event Class</a>.</p> <p><b>Note: This could potentially lead to very large quantities of audit records.</b></p>

Action Group Name	Description
DATABASE_OBJECT_OWNERSHIP_CHANGE_GROUP	This event is raised when there is a change of owner for objects within the database scope. This event is raised for any object ownership change in any database on the server. It is equivalent to the <a href="#">Audit Database Object Take Ownership Event Class</a> .
DATABASE_OBJECT_PERMISSION_CHANGE_GROUP	This event is raised when a GRANT, DENY, or REVOKE (GDR) has been issued for database objects, such as assemblies and schemas. This event is raised for any object permission change for any database on the server. It is equivalent to the <a href="#">Audit Database Object GDR Event Class</a> .
DATABASE_OPERATION_GROUP	This event is raised when operations in a database, such as checkpoint or subscribe query notification, occur. This event is raised on any database operation on any database. It is equivalent to the <a href="#">Audit Database Operation Event Class</a> .
DATABASE_OWNERSHIP_CHANGE_GROUP	This event is raised when you use the ALTER AUTHORIZATION statement to change the owner of a database, and the permissions that are required to do that are checked. This event is raised for any database ownership change on any database on the server. It is equivalent to the <a href="#">Audit Change Database Owner Event Class</a> .
DATABASE_PERMISSION_CHANGE_GROUP	This event is raised whenever a GRANT, DENY, or REVOKE is issued for a statement permission by any principal in SQL Server (this applies to database-only events, such as granting permissions on a database). This event is raised for any database permission change (GDR) for any database in the server. It is equivalent to the <a href="#">Audit Database Scope GDR Event Class</a> .
DATABASE_PRINCIPAL_CHANGE_GROUP	This event is raised when principals, such as users, are created, altered, or dropped from a database. It is equivalent to the <a href="#">Audit Database Principal Management Event Class</a> . (Also



Action Group Name	Description
	equivalent to the <a href="#">Audit Add DB Principal Event Class</a> , which occurs on the deprecated sp_grantdbaccess, sp_revokedbaccess, sp_addPrincipal, and sp_dropPrincipal stored procedures.) This event is raised whenever a database role is added to or removed by using the sp_addrole, sp_droprole stored procedures. This event is raised whenever any database principals are created, altered, or dropped from any database. It is equivalent to the <a href="#">Audit Add Role Event Class</a> .
DATABASE_PRINCIPAL_IMPERSONATION_GROUP	This event is raised when there is an impersonation operation in the database scope such as EXECUTE AS <principal> or SETPRINCIPAL. This event is raised for impersonations done in any database. It is equivalent to the <a href="#">Audit Database Principal Impersonation Event Class</a> .
DATABASE_ROLE_MEMBER_CHANGE_GROUP	This event is raised whenever a login is added to or removed from a database role. This event class is raised for the sp_addrolemember, sp_changegroup, and sp_droprolemember stored procedures. This event is raised on any database role member change in any database. It is equivalent to the <a href="#">Audit Add Member to DB Role Event Class</a> .
DBCC_GROUP	This event is raised whenever a principal issues any DBCC command. It is equivalent to the <a href="#">Audit DBCC Event Class</a> .
FAILED_DATABASE_AUTHENTICATION_GROUP	This class of events is raised by new connections or by connections that are reused from a connection pool. Indicates that a principal tried to log on to a contained database and failed. It is equivalent to the <a href="#">Audit Login Failed Event Class</a> .
FAILED_LOGIN_GROUP	This class of events is raised by new connections or by connections that are reused

Action Group Name	Description
	from a connection pool. Indicates that a principal tried to log on to SQL Server and failed. It is equivalent to the <a href="#">Audit Login Failed Event Class</a> .
FULLTEXT_GROUP	This event indicates that a fulltext event occurred. It is equivalent to the <a href="#">Audit Fulltext Event Class</a> .
LOGIN_CHANGE_PASSWORD_GROUP	This event is raised whenever a login password is changed by way of ALTER LOGIN statement or sp_password stored procedure. It is equivalent to the <a href="#">Audit Login Change Password Event Class</a> .
LOGOUT_GROUP	This class of events is raised by new connections or by connections that are reused from a connection pool. Indicates that a principal has logged out of SQL Server. It is equivalent to the <a href="#">Audit Logout Event Class</a> .
SCHEMA_OBJECT_ACCESS_GROUP	This event is raised whenever an object permission has been used in the schema. It is equivalent to the <a href="#">Audit Schema Object Access Event Class</a> .
SCHEMA_OBJECT_CHANGE_GROUP	This event is raised when a CREATE, ALTER, or DROP operation is performed on a schema. Equivalent to the <a href="#">Audit Schema Object Management Event Class</a> . This event is raised on schema objects. It is equivalent to the <a href="#">Audit Object Derived Permission Event Class</a> . This event is raised whenever any schema of any database changes. It is equivalent to the <a href="#">Audit Statement Permission Event Class</a> .
SCHEMA_OBJECT_OWNERSHIP_CHANGE_GROUP	This event is raised when the permissions to change the owner of schema object (such as a table, procedure, or function) is checked. This occurs when the ALTER AUTHORIZATION statement is used to assign an owner to an object. This event is raised for any schema ownership change for any database on the

Action Group Name	Description
	server. It is equivalent to the <a href="#">Audit Schema Object Take Ownership Event Class</a> .
SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP	This event is raised whenever a GRANT, DENY, or REVOKE is performed against a schema object. It is equivalent to the <a href="#">Audit Schema Object GDR Event Class</a> .
SERVER_OBJECT_CHANGE_GROUP	This event is raised for CREATE, ALTER, or DROP operations on server objects. It is equivalent to the <a href="#">Audit Server Object Management Event Class</a> .
SERVER_OBJECT_OWNERSHIP_CHANGE_GROUP	This event is raised when the owner is changed for objects in server scope. It is equivalent to the <a href="#">Audit Server Object Take Ownership Event Class</a> .
SERVER_OBJECT_PERMISSION_CHANGE_GROUP	This event is raised whenever a GRANT, DENY, or REVOKE is issued for a server object permission by any principal in SQL Server. It is equivalent to the <a href="#">Audit Server Object GDR Event Class</a> .
SERVER_OPERATION_GROUP	This event is raised when Security Audit operations such as altering settings, resources, external access, or authorization are used. It is equivalent to the <a href="#">Audit Server Operation Event Class</a> .
SERVER_PERMISSION_CHANGE_GROUP	This event is raised when a GRANT, DENY, or REVOKE is issued for permissions in the server scope, such as creating a login. It is equivalent to the <a href="#">Audit Server Scope GDR Event Class</a> .
SERVER_PRINCIPAL_CHANGE_GROUP	This event is raised when server principals are created, altered, or dropped. It is equivalent to the <a href="#">Audit Server Principal Management Event Class</a> . This event is raised when a principal issues the sp_defaultdb or sp_defaultlanguage stored procedures or ALTER LOGIN statements. It is equivalent to the <a href="#">Audit Addlogin Event Class</a> .

Action Group Name	Description
	This event is raised on the sp_addlogin and sp_droplogin stored procedures. It is equivalent to the <a href="#">Audit Login Change Property Event Class</a> . This event is raised for the sp_grantlogin, sp_revokelogin, or sp_denylogin stored procedures. It is equivalent to the <a href="#">Audit Login GDR Event Class</a> .
SERVER_PRINCIPAL_IMPERSONATION_GROUP	This event is raised when there is an impersonation within server scope, such as EXECUTE AS <login>. It is equivalent to the <a href="#">Audit Server Principal Impersonation Event Class</a> .
SERVER_ROLE_MEMBER_CHANGE_GROUP	This event is raised whenever a login is added or removed from a fixed server role. This event is raised for the sp_addsrvrolemember and sp_dropsrvrolemember stored procedures. It is equivalent to the <a href="#">Audit Add Login to Server Role Event Class</a> .
SERVER_STATE_CHANGE_GROUP	This event is raised when the SQL Server service state is modified. It is equivalent to the <a href="#">Audit Server Starts and Stops Event Class</a> .
SUCCESSFUL_DATABASE_AUTHENTICATION_GROUP	This event indicates that a principal successfully logged in to a contained database. It is equivalent to the <a href="#">Audit Successful Database Authentication Event Class</a> .
SUCCESSFUL_LOGIN_GROUP	This class of events is raised by new connections or by connections that are reused from a connection pool. This event indicates that a principal has successfully logged in to SQL Server. It is equivalent to the <a href="#">Audit Login Event Class</a> .
TRACE_CHANGE_GROUP	This event is raised for all statements that check for the ALTER TRACE permission. It is equivalent to the <a href="#">Audit Server Alter Trace Event Class</a> .

Action Group Name	Description
USER_CHANGE_PASSWORD_GROUP	This event is raised whenever the password of a contained database user is changed by using the ALTER USER statement.
USER_DEFINED_AUDIT_GROUP	This group monitors events raised by using <code>sp_audit_write</code> (Transact-SQL). Typically triggers or stored procedures include calls to <code>sp_audit_write</code> to enable auditing of important events.

The Web Server log (Microsoft IIS 7.5) includes the following data points. SCG selected the first 14 data points to include in the log report:

1. Date
2. Time
3. Client IP Address
4. User Name
5. Server IP Address
6. Server Port
7. Method
8. URI Stem
9. URI Query
10. Protocol Status
11. Protocol Substatus
12. Win32 Status
13. Time Taken
14. User Agent
15. Protocol Version
16. Host
17. Bytes Sent
18. Bytes Received
19. Cookie
20. Referer
21. Service Name
22. Server Name

There are various logs that come with SharePoint, one of which is a built-in feature called Auditing that can be enabled through the SharePoint site. Once enabled, auditing allows for the tracking of:

- List Access

- Editing Items
- Copying\Moving\Deleting items
- Editing permissions
- Library Access
- Opening of Documents
- Check In\Check Out
- Searching

In addition to these features, SharePoint has Forms-based Authentication (FBA) that can be enabled on a per site basis. This allows administrators to navigate to Site Settings and view a specific site's "User Membership." The Membership interface will list all the FBA users that are registered with the site, with columns for "Active", "Locked", and "Last Login." These columns all correspond to user accounts within the FBA database.

The SharePoint Audit log includes the following events for audit log reports:

- Opened and downloaded documents, viewed items in lists, or viewed item properties
- Edited items
- Checked out and checked in items
- Items that have been moved and copied to other location in the site collection
- Deleted and restored items
- Changes to content types and columns
- Search queries
- Changes to user accounts and permissions
- Changed audit settings and deleted audit log events
- Workflow events
- Custom events

The following events must be identified within the firewall audit logs:

- Device startup and shutdown
- Administrator logon and logoff
- Configuration changes
- Account creation, modification, or deletion
- Modifications of privileges and access controls
- All incoming and outgoing traffic
- System alerts and error messages

SCG has selected these auditable events because this is the information that is deemed to be adequate to support after-the-fact investigations of security incidents. SCG would have to take steps to adjust the depth and breadth of audit logging capabilities for

SCGSC to allow for an increase of these capabilities should there be a heightened threat or risk to system security.

The list of the auditable events should be reviewed and updated annually, when a major change to the SCGSC system occurs, or when there is an incident requiring an event to be audited. The list of events to be audited by the system includes the execution of privileged functions.

### **4.3 AU-3 – Content of Audit Records**

The SCGSC system must capture sufficient information in audit records.

**Note:** *Audit record content should include, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, file names involved, and access control rules invoked.*

At a minimum, the following elements must be identified in each audit record:

- Date and time when the event occurred
- The software or hardware component of the SCGSC system where the event occurred
- Source of the event (e.g., Windows security auditing, servicing, security Kerberos)
- Type of event that occurred
- Subject identity (e.g., user, device)
- The outcome (i.e., success or failure) of the event

The following additional elements are identified within the server audit record:

- Application—access and failure of an application
- Security—successful logons and failed logon attempts
- Setup—installation and removal of programs
- System—configuration changes in Windows

### **4.4 AU-4 – Audit Storage Capacity**

The SCGSC system must allocate audit record storage capacity to prevent such capacity being exceeded. The audit storage capacity for the SCGSC server is set at 100 times the default for the application (default = 2 Mb), security (default = 89 Mb), setup (default = 1 Mb), and system (default = 3 Mb) logs (a total of 9.5 Gb storage capacity for the server audit records). The audit storage capacity allocated for the Kiwi Syslog centralized audit records is a minimum of 30 Gb.

### **4.5 AU-5 – Response to Audit Processing Failures**

The SCGSC system automatically alerts the IT Director in the event of an audit failure or when audit capacity is 12% remaining. This alert is distributed by e-mail. The system

also signals this by an audible alarm. The IT Director then ensures the audit logs are backed up and clears the audit logs to free up capacity.

#### **4.6 AU-6 – Audit Review, Analysis, and Reporting**

Audit logs for SCGSC are reviewed and analyzed weekly for the following:

(1) indications of inappropriate or unusual activity, (2) assurance that logging is functioning properly, and (3) adherence to logging standards identified in this procedure.

The following review and analysis requirements must be adhered to:

- All logs will be correlated using Kiwi Syslog and examined weekly to determine if any incidents have occurred.
- The level of audit review, analysis, and reporting must be adjusted if there is an increase in risk to SCGSC.

All staff involved with log management responsibilities must be trained on how to review and analyze audit logs, and how to report incidents when applicable. Findings should be reported to the SCG President, Vice President of Administration, and Program Manager.

#### **4.7 AU-7 – Audit Reduction and Report Generation**

Kiwi Syslog is used by SCG for audit reduction and report generation capability. It is capable of providing an audit reduction and report generation capability to support near real-time audit review, analysis, and reporting requirements described in AU-6 and after-the-fact investigations of security incidents. Kiwi Syslog does not alter the original audit record and is capable of extracting useful and readable data for the review process. Kiwi Syslog has tools to filter audit logs and generate reports to help reduce the amount of information contained in audit records and distill useful information. It has query applications that have the ability to query an audit log by username, location, application name, date, and time, or other applicable parameters; and the ability to execute reports with the results of the query. It has the capability to automatically process audit records for events of interest based on selectable event criteria.

#### **4.8 AU-8 – Time Stamps**

The SCGSC system uses an internal system clock to generate time stamps for audit records. Time stamps generated by the system include both the date and time. The time is expressed in Coordinated Universal Time (UTC) to the nearest second.

The Windows Time service, also known as W32Time, synchronizes the date and time for all computers running in the SCGSC system. The Windows Time service uses the Network Time Protocol (NTP) to synchronize computer clocks on the network so that an accurate clock value, or time stamp, can be assigned to network validation and resource access requests. The service integrates NTP and time providers, making it a reliable and scalable time service for the system administrator.



#### **4.8.1 AU-8 (1) – Time Stamps**

The SCGSC SCSQL-PROD server compares the internal information system clock every 7 days and it synchronizes the SCGSC system time to the nearest second to time.windows.com, an external authoritative time source. The internal system clock synchronizes to the authoritative time source when the time difference is greater than 1 second.

### **4.9 AU-9 – Protection of Audit Information**

The SCGSC system protects audit information and audit tools from unauthorized access, modification, and deletion. The audit data for the SCGSC system are accessible only by privileged users, and the Windows Local Policy settings enforce this protection. Audit logs cannot be modified, which ensures audit information integrity. Only the Domain Administrator can clear logs, and accidental or deliberate deleting of logs can be investigated and confirmed through review of audit log tape backups.

#### **4.9.1 AU-9 (4) Protection of Audit Information**

The Domain Administrators are the only privileged users who can access and modify audit configuration settings for the SCGSC system. This is enforced through Windows Local Policy settings, and access level in the firewall enforces this protection. Audit logs track changes in audit configuration settings to protect against accidental and deliberate tampering with audit configuration settings and audit data and records.

### **4.10 AU-11 – Audit Record Retention**

Audit logs must be retained to provide support for after-the-fact investigations of IT security incidents for SCGSC and to meet SCG and government information retention requirements. These logs include system, application, and database-level audit logs and logs for network devices. All audit logs for the SCGSC system are retained for a period of three (3) years in accordance with SCG retention requirements. The most recent 60 days of log files are stored online and the remaining time they are stored as tape backups. Audit logs are archived on monthly backup tapes and stored in a fire safe in the IT Director's office.

### **4.11 AU-12 – Audit Generation**

The system provides audit record generation capability for the list of auditable events defined in AU-2 on the servers and system components. The IT Director is responsible for configuring audit settings for the SCGSC system. SCG uses Kiwi Syslog to compile audit records in a centralized location. The time stamp on all audit records for components is consistent within the system as all components are synchronized simultaneously to the same external time source. All audit records are stored in Coordinated Universal Time (UTC) format.

## **5. Roles and Responsibilities**

### **5.1 SCG President**

The SCG President has the following responsibilities with respect to audit and accountability:

- Oversee the implementation and maintenance of audit trails for the SCGSC system and ensure auditable events are sufficient to protect the information system.
- Ensure that sufficient information is captured in audit records to establish the occurrence of events, the sources of events, and the outcome of events.
- Allocate sufficient audit record storage capacity to prevent such capacity from being exceeded.
- Verify that the information system automatically alerts appropriate officials when there is an audit failure or storage capacity is close to being reached.
- Review and analyze logs and records as needed.
- Investigate any suspicious activity or suspected violations and take the necessary actions to prevent/mitigate such actions.
- Ensure that staff involved with log management responsibilities are trained to review and analyze audit logs and to report incidents.
- Confirm that the system time is periodically updated from an authoritative resource.
- Ensure that audit information and audit tools are protected.
- Update the SCGSC Auditing and Accountability Policy and Procedures document in consultation with the IT Director.
- Verify that audit records are retained in accordance with SCG policies.
- Coordinate with appropriate SCG management and technical personnel to ensure that vulnerabilities are addressed if an investigation of an incident reveals an exploitable system or procedural vulnerability.
- Update the SCGSC Auditing and Accountability Policy and Procedures document in consultation with the IT Director.

### **5.2 Domain Administrators**

The Domain Administrators have the following responsibilities with respect to audit and accountability for the SCGSC system:

- Implement and maintain audit trails for the SCGSC system and ensure auditable events are sufficient to protect the information system.
- Configure audit logs to capture important events in the SCGSC system.
- Review audit trails for the SCGSC system to ensure compliance with SCG's policies, procedures, and standards.

- Review auditable events for necessary changes in conjunction with incident information and requirements to protect the SCGSC system.
- Report any operational or security problems to the appropriate authorities.
- Assess the list of auditable events annually and review it for necessary changes in conjunction with incident information and requirements to protect SCGSC.
- Modify the list of auditable events annually as needed and provide input for updating the SCGSC Auditing and Accountability Policy and Procedures document.

## Appendix A: Definitions

**Appropriate Technical and Management Personnel** – individuals responsible for the resources needed and required to track the access attempt through the system.

**Audit Reduction** – includes using tools and techniques that reduce audit data in order to save storage space and to abstract more useful, higher-level data for the review process.

**Incident** – an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

**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.

**Media** – physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, flash drives, hard drives, 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 portable and mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones).

**Records** – the recordings of evidence of activities performed or results achieved (e.g., forms, reports, test results) that serve as the basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).

**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.

## Appendix B: Acronyms

ACID	Atomicity, Consistency, Isolation, and Durability
FBA	Forms-Based Authentication
Gb	Gigabytes
GDR	Grant, Deny or Revoke
IP	Internet Protocol
IT	Information Technology
Mb	Megabytes
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
SCGSC	Scientific Consulting Group Secure Cloud
SP	Special Publication
SQL	Structured Query Language
URI	Universal Resource Indicator
UTC	Coordinated Universal Time