nistBlue

FedRAMP System Security Plan



Veris Group

Sky Solutions SaaS

Version 1.4

January 1, 2016

**Company Sensitive and Proprietary**

**For Authorized Use Only**

Document Revision History

| Date | Description | Version | Author |
| --- | --- | --- | --- |
| 01/01/2012 | Initial Publication | 1.0 | Veris Goup |
| 01/01/2013 | Annual Review | 1.1 | Veris Group |
| 01/01/2014 | Annual Review | 1.2 | Veris Group |
| 01/01/2015 | Annual Review | 1.3 | Veris Group |
| 01/01/2016 | Annual Review | 1.4 | Veris Group |

1. Information System Name/Title

This System Security Plan provides an overview of the security requirements for the Veris Group Sky Solutions SaaS system and describes the controls in place or planned for implementation to provide a level of security appropriate for the information to be transmitted, processed or stored by the system. Information security is an asset vital to our critical infrastructure and its effective performance and protection is a key component of our national security program. Proper management of information technology systems is essential to ensure the confidentiality, integrity and availability of the data transmitted, processed or stored by the Sky Solutions SaaS information system.

The security safeguards implemented for the Sky Solutions SaaS system meet the policy and control requirements set forth in this System Security Plan. All systems are subject to monitoring consistent with applicable laws, regulations, agency policies, procedures and practices.

|  |  |  |
| --- | --- | --- |
| Unique Identifier | Information System Name | Information System Abbreviation |
| SkySol | Sky Solutions SaaS | Sky Solutions |

1. Information System Categorization

The overall information system sensitivity categorization is noted in the table that follows.

Table 2-1. Security Categorization

|  |  |
| --- | --- |
| Low |  |
| Moderate |  |
| High |  |

2.1 Information Types

This section describes how the information types used by the information system are categorized for confidentiality, integrity, and availability sensitivity levels.

The following tables identify the information types that are input, stored, processed, and/or output from Sky Solutions. The selection of the information types is based on guidance provided by OMB Federal Enterprise Architecture Program Management Office Business Reference Model 2.0, and FIPS Pub 199, *Standards for Security Categorization of Federal Information and Information Systems* which is based on NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*.

The tables also identify the security impact levels for confidentiality, integrity, and availability for each of the information types expressed as low, moderate, or high. The security impact levels are based on the potential impact definitions for each of the security objectives (i.e., confidentiality, integrity, and availability) discussed in NIST SP 800-60 and FIPS Pub 199.

The potential impact is *low* if—

- The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

- A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

The potential impact is *moderate* if—

- The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

- A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

The potential impact is *high* if—

- The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

- A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

Table 2-2. Sensitivity Categorization of Information Types

The following information types have been derived utilizing guidance from NIST SP 800-60.

| Information Type  (Use only information types from NIST SP 800-60, Volumes I and II as amended) | NIST 800-60 identifier for Associated Information Type | Confidentiality | Integrity | Availability |
| --- | --- | --- | --- | --- |
| Information Security | C.3.5.5 | Moderate | Moderate | Low |
| Continuity of Operations | C.2.4.2 | Moderate | Moderate | Moderate |
| Security Management | C.3.1.3 | Moderate | Moderate | Moderate |
| IT Infrastructure Maintenance | C.3.5.4 | Low | Moderate | Low |
| System and Network Monitoring | C.3.5.8 | Moderate | Moderate | Low |

Given the information types and impact levels, the following final impact levels for the system are recommended as follows:

|  |  |  |  |
| --- | --- | --- | --- |
| **Final Impact Level for Confidentiality** | **Final Impact Level for Integrity** | **Final Impact Level for Availability** | **Overall Impact Level** |
| M | M | M | M |

2.2 Security Objectives Categorization (FIPS 199)

Based on the information provided in Table 2-2, Information Types, for Sky Solutions SaaS the default to the high-water mark for the noted Information Types as identified in the table below.

Table 2-3. Security Impact Level

| Security Objective | Low, Moderate or High |
| --- | --- |
| Confidentiality | Moderate |
| Integrity | Moderate |
| Availability | Moderate |

Through review and analysis, it has been determined that the baseline security categorization for the Sky Solutions SaaS system is listed in the table that follows.

Table 2-4. Baseline Security Categorization

|  |  |
| --- | --- |
| Sky Solutions Security Categorization | Moderate |

Using this categorization, in conjunction with the risk assessment and any unique security requirements, we have established the security controls for this system, as detailed in this SSP.

1. System Interconnections

Sky Solutions Interconnected Systems

The Sky Solutions SaaS does not have interconnections to other systems. Qualifying interconnections are described as either a direct physical connection (e.g., via T1, T3) between systems or a Point to Point Virtual Private Network (VPN) (e.g., via IPSec, L2TP) over the internet between systems. Interconnections require an Interconnection Security Agreement (ISA). If Personally Identifiable Information (PII) data is shared, a Memorandum of Understanding (MOU), or Memorandum of Agreement (MOA) is also required.

Sky Solutions Information Sharing Systems

The Sky Solutions SaaS does not share information with other systems, applications or groups outside of the Sky Solutions authorization boundary for the purpose of sharing information resources. Systems, applications or groups may share data without having a direct interconnection (e.g., via tape, paper, electronic file or E-mail) to allow business processes to be executed

* 1. AC-11 Session Lock

The information system:

1. Prevents further access to the system by initiating a session lock after [FedRAMP Assignment: fifteen (15) minutes] of inactivity or upon receiving a request from a user; and
2. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

| AC-11 | Control Summary Information |
| --- | --- |
| Responsible Role: System Administrator | |
| Parameter AC-11(a): fifteen (15) minutes | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for SkySol , Date of Authorization | |

| AC-11 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | A session lock is initiated via Group Policy Object (GPO) settings after 15 minutes of inactivity on all Veris Group issued Windows workstations utilized by Sky Solutions Administrators. In addition, the Sky Solutions application is configured to initiate a session lock after 15 minutes of inactivity via Internet Information Services (IIS) configuration settings. |
| Part b | All session locks employed in the Sky Solutions environment are retained until the user re-authenticates to the Sky Solutions information system utilizing their associated username and password. |

* 1. CA-9 Internal System Connections

The organization:

1. Authorizes internal connections of [Assignment: organization-defined information system components or classes of components] to the information system; and
2. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

| CA-9 | Control Summary Information |
| --- | --- |
| Responsible Role: System Administrator | |
| Parameter CA-9(a): None | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for SkySol , Date of Authorization | |

| CA-9 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The Sky Solutions SaaS does not have any internal systems connected. CA-9 does not apply. |
| Part b | The Sky Solutions SaaS does not have any internal systems connected. CA-9 does not apply. |

* 1. IA-2 User Identification and Authentication

#### **IA-2 (1) Control Enhancement**

The information system implements multifactor authentication for network access to privileged accounts.

| IA-2 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: System Administrator | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for SkySol , Date of Authorization | |

| IA-2 (1) What is the solution and how is it implemented? |
| --- |
| All network access is considered privileged. In order to gain access to the network, personnel are required to logon to OpenVPN via username, password and MFA pin. Duo Security is the MFA application used to authenticate to the network. Once a user successfully logons onto OpenVPN via username and password, they are prompted to enter their Duo Security MFA pin. Duo Security provides a six digit one time pin which users must enter before being allowed access to the network. |

* 1. IR-2 Incident Response Training

The organization provides incident response training to information system users consistent with assigned roles and responsibilities in accordance with NIST SP 800-53 Rev 4:

1. Within [Assignment: organization-defined time period] of assuming an incident response role or responsibility;
2. When required by information system changes; and

| IR-2 | Control Summary Information |
| --- | --- |
| Responsible Role: Learning and Development Director | |
| Parameter IR-2(a): 90 days | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for SkySol , Date of Authorization | |

| IR-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | All personnel are considered to have roles and responsibilities within the incident reporting process. As a result, incident response training is provided as a part of new hire onboarding. New hires are required to complete the incident response training within 90 days of employment at Sky Solutions. |
| Part b | When changes to the system occur, the incident response training is updated to reflect any changes that affect incident response. Personnel are required to complete the updated training within 90 days of its release. Currently, no changes to the system have occurred, necessitating the update of the incident response training. |

* 1. PL-4 Rules of Behavior

The organization:

1. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage;
2. Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system;
3. Reviews and updates the rules of behavior [FedRAMP Assignment: at least every three (3) years]; and
4. Requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated.

| PL-4 | Control Summary Information |
| --- | --- |
| Responsible Role: Human Resources Director | |
| Parameter PL-4(c): annually or whenever FedRAMP releases a newer version | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for SkySol , Date of Authorization | |

| PL-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Veris Group makes use of the FedRAMP approved Rules of Behavior template. The Rules of Behavior are provided to new hires during the onboarding process. |
| Part b | As a part of the onboarding process, new hires are required to sign off on the Rules of Behavior, the day that they are hired. The signed RoB serves as the acknowledgement that personnel have read and understood the RoB. Once the RoB is signed off on, personnel are required to send it to their manager and the Human Resources director via e-mail. A copy of the signed RoB is kept within their employee file for record keeping purposes. |
| Part c | The Rules of Behavior are reviewed and updated (if necessary) on January 1st every year. In the event that FedRAMP releases a newer version of the document outside of the annual review cycle, that version of the RoB is adopted and baselined as the current version until the next review takes place on January 1st of the following year. |
| Part d | Personnel are required to sign the RoB annually on the anniversary of their hiring date. In the event that FedRAMP releases a newer version of the document, that version of the RoB is adopted and all personnel are required to read and sign the updated document. |

* 1. RA-2 Security Categorization

The organization:

1. Categorizes information and the information system in accordance with applicable Federal Laws, Executive Orders, directives, policies, regulations, standards, and guidance;
2. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and

| RA-2 | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for SkySol , Date of Authorization | |

| RA-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Veris Group completed a FIPS 199 system security categorization of the Sky Solutions SaaS information system in accordance with applicable Federal Laws, Executive Orders, directives, policies, regulations, standards and guidance. The security categorization for the Sky Solutions SaaS system was determined following FIPS 199, Standards for Security Categorization of Federal Information and Information Systems and NIST SP 800-60 Guide for Mapping Types of Information and Information Systems to Security Categories, Revision 1. The result was a categorization of Moderate. As such, all assets and information hosting web services shall be handled and protected in such a manner as to reflect this high sensitivity classification. |
| Part b | The Sky Solutions FIPS 199 categorization is summarized in section 2.2 of the SSP and detailed in the FIPS 199 document included as part of the Sky Solutions SaaS Authorization Package. |

* 1. SI-16 Memory Protection

The information system implements [Assignment: organization-defined fail-safe procedures] to protect its memory from unauthorized code execution.

| SI-16 | Control Summary Information |
| --- | --- |
| Responsible Role: System Administrator | |
| Parameter SI-16: Windows DEP Feature | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for SkySol , Date of Authorization | |

| SI-16 What is the solution and how is it implemented? |
| --- |
| Veris Group employs the use of the Windows Data Execution Prevention (DEP) feature on all Windows hosts in the Sky Solutions environment to assist in protecting its memory from unauthorized code execution. The DEP feature helps prevent code execution from data pages, such as the default heap pages, various stack pages, and memory pool pages. |