Supply Chain Risk Management Plan

Vertosoft LLC
1602 Village Market Blvd. #320
Leesburg, VA 20175

7/1/2021

Table of Contents

1 Introduction

Vertosoft's Supply Chain Risk Management (SCRM) Plan is based on the National Institute of Standards and Technology (NIST) 800-161 – Supply Chain Risk Management practices for Federal Information Systems and Organizations. In addition, Vertosoft has begun the implementation of the Cybersecurity Maturity Model Certification (CMMC) Level 3 controls across the organization and will schedule a third-party audit once that process is worked out by the CMMC-AB. In addition, Vertosoft has followed the guidance from NIST 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations which also references NIST 800-53.

Vertosoft has developed a System Security Plan (SSP) following the NIST 800-53 "process for selecting controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile cyber-attacks, natural disasters, structural failures, and human errors (both intentional and unintentional)."

Following this process, Vertosoft has implemented controls from the following control families, Access Control; Audit and Accountability; Awareness and Training; Assessment, Authorization and Monitoring; Configuration Management; Contingency Planning; Identification and Authentication; Incident Response; Maintenance; Media Protection; Personnel Security; Physical and Environmental Protection; Planning; Risk Assessment; System and Communications Protection; System and Information Integrity; System and Services Acquisition.

Vertosoft also asks each of our Vendors to complete an SCRM checklist to identify potential downstream risks that may require remediation and guidance to ensure supply chain fidelity.

2 Controls

2.1 AT-1 Security Awareness and Training Policy and Procedures

Maintain a security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

Follow procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.

Review and updates the current security awareness and training policy and training procedures on a set frequency.

2.2 CM-1 Configuration Management Policy and Procedures

Develops, documents, and disseminates to a configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.

Reviews and updates the current configuration management policy and configuration management procedures on a set frequency.

2.3 CM-3 Configuration Change Control

Determines the types of changes to the information system that are configuration-controlled;

Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;

Documents configuration change decisions associated with the information system;

Implements approved configuration-controlled changes to the information system;

Retains records of configuration-controlled changes to the information system;

Audits and reviews activities associated with configuration-controlled changes to the information system; and

Coordinates and provides oversight for configuration change control activities through a set group/committee that convenes on a regular basis.

2.4 CM-5 Access Restrictions for Change

The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.

2.5 CM-8 Information System Component Inventory

The organization develops and documents an inventory of information system components that:

1. Accurately reflects the current information system;
2. Includes all components within the authorization boundary of the information system;
3. Is at the level of granularity deemed necessary for tracking and reporting; and
4. Includes company relevant information and

Reviews and updates the information system component inventory

2.6 IR-4 (10) Incident Handling – Supply Chain Coordination

The organization coordinates incident handling activities involving supply chain events with other organizations involved in the supply chain.

2.7 IR-6 (3) Incident Reporting – Coordination with Supply Chain

The organization provides security incident information to other organizations involved in the supply chain for information systems or information system components related to the incident.

2.8 PE-3 Physical Access Control

The organization enforces physical access authorizations at defined company facilities by:

a. Verifying individual access authorizations before granting access to the facility and controlling ingress/egress to the facility;
b. Maintains physical access audit logs;
c. Provides safeguards to control access to areas within the facility officially designated as publicly accessible;
d. Escorts visitors and monitors visitor activity;
e. Secures keys, combinations, and other physical access devices;
f. Inventories physical access devices; and
g. Changes combinations and keys and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

2.9 PE-20 Asset Monitoring and Tracking

The organization employs technologies to track and monitor the location and movement of assets within organization-defined controlled areas; and

Ensures that asset location technologies are employed in accordance with applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.

2.10 PV-2 Tracking Provenance and Developing a Baseline

The organization:

a. Provides unique identification for the provenance document for tracking as it traverses the ICT supply chain
b. Develops methods to document, monitor, and maintain valid provenance baselines for systems and components of the information system or component and the ICT supply chain infrastructure
c. Tracks, documents, and disseminates to relevant supply ICT chain participants changes to the provenance
d. Tracks individuals and processes that have access and make changes to the provenance of components, tools, data, and processes in the information system or the ICT supply chain infrastructure; and
e. Ensures non-repudiation of provenance information and the provenance change records including when, what, and to whom.

2.11 RA-3 Risk Assessment

The organization

a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
b. Documents risk assessment results;
c. Reviews risk assessment results;
d. Disseminates risk assessment results; and
e. Updates the risk assessment on a set frequency or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

2.12 SA-4 Acquisition Process

The organization includes security requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs.

2.13 SA-8 Security Engineering Principles

The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

2.14 SA-11 Developer Security Testing and Evaluation

The organization requires the developer of the information system, system component, or information system service to create and implement a security assessment plan; perform testing/evaluation; produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation; implement a verifiable flaw remediation process; and correct flaws identified during security testing/evaluation.

2.15 SA-12 Supply Chain Protection

The organization protects against supply chain threats to the information system, system component, or information system service by employing appropriate safeguards as part of a comprehensive, defense-in-breadth information security strategy. This includes:

- acquisition strategies, contract tools, and procurement methods for the purchase of the information system, system component, or information system service from suppliers
- supplier review prior to entering into a contractual agreement to acquire the information system, system component, or information system service
- security safeguards] to limit harm from potential adversaries identifying and targeting the organizational supply chain
- conducts an assessment of the information system, system component, or information system service prior to selection, acceptance, or update
- uses all-source intelligence analysis of suppliers and potential suppliers of the information system, system component, or information system service
- employs Operations Security (OPSEC) safeguards in accordance with classification guides to protect supply chain-related information for the information system, system component, or information system service
- security safeguards] to validate that the information system or system component received is genuine and has not been altered
- organizational analysis, independent third-party analysis, organizational penetration testing, independent third-party penetration testing supply chain elements, processes, and actors associated with the information system, system component, or information system service
- inter-organizational agreements and procedures with entities involved in the supply chain for the information system, system component, or information system service
- security safeguards to ensure an adequate supply of critical information system components
- establishes and retains unique identification of supply chain elements, processes, and actors for the information system, system component, or information system service
- a process to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements

2.16 SA-15 Development Process, Standards, and Tools

The organization requires the developer of the information system, system component, or information system service to follow a documented development process that explicitly

addresses security requirements; identifies the standards and tools used in the development process; documents the specific tool options and tool configurations used in the development process; and documents, manages, and ensures the integrity of changes to the process and/or tools used in development.

Reviews the development process, standards, tools, and tool options/configurations to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy security requirements.

2.17 SA-18 Tamper Resistance and Detection

The organization implements a tamper protection program for the information system, system component, or information system service.

2.18 SA-19 Component Authenticity

The organization develops and implements anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the information system; and reports counterfeit information system components to supply chain participants.

2.19 SI-2 Flaw Remediation

The organization identifies, reports, and corrects information system flaws; tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; installs security-relevant software and firmware updates within an organization-defined time period of the release of the updates; and incorporates flaw remediation into the organizational configuration management process.

2.20 SI-4 Information System Monitoring

The organization:

- monitors the information system to detect attacks and indicators of potential attacks in; and unauthorized local, network, and remote connections;
- Identifies unauthorized use of the information system;
- Deploys monitoring devices strategically within the information system to collect organization-determined essential information; and at ad hoc locations within the system to track specific types of transactions of interest to the organization;
- Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
- Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;

- Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations;

2.21 SI-7 Software, Firmware, and Information Integrity

The organization employs integrity verification tools to detect unauthorized changes to software, firmware, and information.

3 Vertosoft Supplier SCRM Checklist

COMPANY NAME	Yes/No	Comments
AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES Maintain a security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Follow procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls. Review and updates the current security awareness and training policy and training procedures on a set frequency.		
CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES Develops, documents, and disseminates to a configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and procedures to facilitate the implementation of the configuration management policy and associated configuration management controls. Reviews and updates the current configuration management policy and configuration management procedures on a set frequency.		
CM-3 CONFIGURATION CHANGE CONTROL Determines the types of changes to the information system that are configuration-controlled; Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses; Documents configuration change decisions associated with the information system; Implements approved configuration-controlled changes to the information system; Retains records of configuration-controlled changes to the information system; Audits and reviews activities associated with configuration-controlled changes to the information system; and Coordinates and provides oversight for configuration change control activities through a set group/committee that convenes on a regular basis.		
CM-5 ACCESS RESTRICTIONS FOR CHANGE The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.		
CM-8 INFORMATION SYSTEM COMPONENT INVENTORY The organization develops and documents an inventory of information system components that: 5. Accurately reflects the current information system; 6. Includes all components within the authorization boundary of the information system; 7. Is at the level of granularity deemed necessary for tracking and reporting; and 8. Includes company relevant information and Reviews and updates the information system component inventory		
IR-4 (10) INCIDENT HANDLING - Supply Chain Coordination The organization coordinates incident handling activities involving supply chain events with other organizations involved in the supply chain.		
IR-6 (3) INCIDENT REPORTING - Coordination with supply chain The organization provides security incident information to other organizations involved in the supply chain for information systems or information system components related to the incident.		
PE-3 PHYSICAL ACCESS CONTROL The organization enforces physical access authorizations at defined company facilities by: h. Verifying individual access authorizations before granting access to the facility and controlling ingress/egress to the facility; i. Maintains physical access audit logs; j. Provides safeguards to control access to areas within the facility officially designated as publicly accessible; k. Escorts visitors and monitors visitor activity; l. Secures keys, combinations, and other physical access devices;		

m. Inventories physical access devices; and n. Changes combinations and keys and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.		
PE-20 ASSET MONITORING AND TRACKING The organization employs technologies to track and monitor the location and movement of assets within organization-defined controlled areas; and Ensures that asset location technologies are employed in accordance with applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.		
PV-2 TRACKING PROVENANCE AND DEVELOPING A BASELINE The organization: a. Provides unique identification for the provenance document for tracking as it traverses the ICT supply chain b. Develops methods to document, monitor, and maintain valid provenance baselines for systems and components of the information system or component and the ICT supply chain infrastructure c. Tracks, documents, and disseminates to relevant supply ICT chain participants changes to the provenance d. Tracks individuals and processes that have access and make changes to the provenance of components, tools, data, and processes in the information system or the ICT supply chain infrastructure; and e. Ensures non-repudiation of provenance information and the provenance change records including when, what, and to whom.		
RA-3 RISK ASSESSMENT The organization f. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; g. Documents risk assessment results; h. Reviews risk assessment results; i. Disseminates risk assessment results; and j. Updates the risk assessment on a set frequency or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.		
SA-4 ACQUISITION PROCESS The organization includes security requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs.		
SA-8 SECURITY ENGINEERING PRINCIPLES The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.		
SA-11 DEVELOPER SECURITY TESTING AND EVALUATION The organization requires the developer of the information system, system component, or information system service to create and implement a security assessment plan; perform testing/evaluation; produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation; implement a verifiable flaw remediation process; and correct flaws identified during security testing/evaluation.		
SA-12 SUPPLY CHAIN PROTECTION The organization protects against supply chain threats to the information system, system component, or information system service by employing appropriate safeguards as part of a comprehensive, defense-in-breadth information security strategy. This includes: • acquisition strategies, contract tools, and procurement methods for the purchase of the information system, system component, or information system service from suppliers		

• supplier review prior to entering into a contractual agreement to acquire the information system, system component, or information system service • security safeguards] to limit harm from potential adversaries identifying and targeting the organizational supply chain • conducts an assessment of the information system, system component, or information system service prior to selection, acceptance, or update • uses all-source intelligence analysis of suppliers and potential suppliers of the information system, system component, or information system service • employs Operations Security (OPSEC) safeguards in accordance with classification guides to protect supply chain-related information for the information system, system component, or information system service • security safeguards] to validate that the information system or system component received is genuine and has not been altered • organizational analysis, independent third-party analysis, organizational penetration testing, independent third-party penetration testing supply chain elements, processes, and actors associated with the information system, system component, or information system service • inter-organizational agreements and procedures with entities involved in the supply chain for the information system, system component, or information system service • security safeguards to ensure an adequate supply of critical information system components • establishes and retains unique identification of supply chain elements, processes, and actors for the information system, system component, or information system service • a process to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements		
SA-15 DEVELOPMENT PROCESS, STANDARDS, AND TOOLS The organization requires the developer of the information system, system component, or information system service to follow a documented development process that explicitly addresses security requirements; identifies the standards and tools used in the development process; documents the specific tool options and tool configurations used in the development process; and documents, manages, and ensures the integrity of changes to the process and/or tools used in development. Reviews the development process, standards, tools, and tool options/configurations to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy security requirements.		
SA-18 TAMPER RESISTANCE AND DETECTION The organization implements a tamper protection program for the information system, system component, or information system service.		
SA-19 COMPONENT AUTHENTICITY The organization develops and implements anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the information system; and reports counterfeit information system components to supply chain participants.		
SI-2 FLAW REMEDIATION The organization identifies, reports, and corrects information system flaws; tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; installs security-relevant software and firmware updates within an organization-defined time period of the release of the updates; and incorporates flaw remediation into the organizational configuration management process.		
SI-4 INFORMATION SYSTEM MONITORING The organization: • monitors the information system to detect attacks and indicators of potential attacks in; and unauthorized local, network, and remote connections; • Identifies unauthorized use of the information system;		

• Deploys monitoring devices strategically within the information system to collect organization-determined essential information; and at ad hoc locations within the system to track specific types of transactions of interest to the organization; • Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; • Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; • Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations;		
SI-7 SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY The organization employs integrity verification tools to detect unauthorized changes to software, firmware, and information.		

CERTIFICATION IS REQUIRED BY AN AUTHORIZED REPRESENTATIVE VERIFYING INFORMATION CONTAINED ON THIS FORM IS TRUE.

Signature: _____
Print Name: _____
Title: _____
Company Name: _____
Phone: _____
Email Address: _____
Date: _____