Sonatype
Information Security Management System Policy

Purpose

To establish an Information Security Management System (ISMS) which is a defined, documented management system that consists of a set of policies, processes, systems and a leadership body Information Security Management Committee (ISMC) which are used by the organization to govern itself and to manage risks to organizational assets.

Scope

Involved Persons: Every Sonatype employee, contractor, partner, agent, service provider, advisor and representative (collectively the "Sonatype Personnel") is governed by, and must comply with, this ISMS Policy and other related information security documents.

Involved Systems and Information: This ISMS Policy applies to all data, computer and network systems owned, operated and/or administered by or on behalf of Sonatype including all personal computer systems (including all operating systems and application systems) and devices that are used to access Sonatype resources and networks.

Involved Locations: The physical scope will be limited to the operations performed at Sonatype's Fulton (MD), Tysons Corner (VA), and London (UK) offices.

Exclusions: All services and locations provided and managed by third party service providers with ISO 27001 or SOC 2 certifications will be excluded from the ISMS audit scope.

Effective Date

This policy is effective upon ratification by the Information Security Management Committee, and supersedes previously existing iterations.

Policy

Sonatype is committed to protecting the confidentiality, integrity, and availability of the data and systems which comprise the Sonatype products, services, and supporting infrastructure. The objectives of the ISMS are to; (a) establish a governing body known as the Information Security Management Committee (ISMC); (b) implement a comprehensive, effective and continuously improving information security program in order to protect and manage information based on a systematic business risk approach; (c) prohibit unauthorized access, disclosure, modification, destruction, loss, misuse, or theft of information and assets owned, controlled or in the custody of Sonatype; (d) protect

information belonging to third-parties that has been entrusted to Sonatype by maintaining the integrity, security, and confidentiality of that information as well as in accordance with applicable regulatory requirements, binding agreements, and contracts; (e) demonstrate support for and commitment to achieving compliance with applicable privacy protection legislation and the contractual terms agreed between Sonatype and Sonatype's clients.

ISMS Roles and Responsibilities

Information Security Management Committee (ISMC) is a cross-functional group of leaders responsible for providing executive management direction, authority, funding, and guidance for all aspects of the ISMS. The ISMC will meet no less than once per calendar quarter. The agenda for these meetings will include review of security metrics, improvements, risks, policy updates, and security incidents. Members are responsible for the disposition of all risks identified to the ISMS. All ISMS policies will be reviewed annually and ratified by the ISMC to ensure security requirements within Sonatype are documented and approved for implementation. Departmental Stakeholders are accountable for ensuring that ISMS policies covering their area of the business are operationalized. See **table 1** below for current members.

Sonatype is committed to continuous improvement, as such, the ISMC will regularly review information from internal and external sources, including:

- Internal/External audit results
- Incidents and other nonconformities
- Status of Corrective and Preventive actions
- Trends identified through monitoring and measurement processes

Through this review process the ISMC identifies actions to improve the suitability, adequacy and effectiveness of the Sonatype's ISMS, and will take action to eliminate the cause of nonconformities associated with the implementation and operation of the ISMS in order to prevent recurrence by:

- Identifying non-conformities
- Determining the causes of nonconformities
- Evaluating the need for actions to ensure that nonconformities do not recur
- Determining and implementing the corrective action needed
- Recording results of action taken
- Reviewing corrective action taken

The Information Security team works under the guidance of the ISMC and, acting as chair of the ISMC, is responsible for reporting to the ISMC on the overall status of the ISMS Program at Sonatype. Key responsibilities include: (a) centralizing all guidance, direction, and authority related to information security activities at Sonatype; (b) establishing, maintaining, and communicating organization-wide information security policies, standards, guidelines, and procedures; (c) compliance checking to ensure that organizational units are operating in a manner consistent with the requirements stated in this ISMS Policy; and (d) along with Sonatype's IT and Ops teams, investigating system intrusions and other information security incidents. Local managers working in conjunction with Sonatype's Human Resources

department are responsible for handling disciplinary matters resulting from violations of information security requirements.

Sonatype Personnel are responsible for familiarizing themselves with and complying with all ISMS Policies and all other procedures, and standards that govern information security.

Exceptions

The Information Security team acknowledges that, under rare circumstances, certain Sonatype Personnel will need to employ systems that are not compliant with these Policies. All such instances must have documented written approval in advance by an Information Security Management Committee member.

Violations

Any violation of this ISMS Policy may result in disciplinary action, up to and including termination of employment. Sonatype reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Sonatype will consider conduct in violation of this ISMS Policy to be outside the course and scope of Sonatype Personnel's employment, and/or not a direct consequence of the discharge of Sonatype Personnel's duties. Accordingly, to the extent permitted by law, Sonatype reserves the right not to defend or pay any damages awarded against Sonatype Personnel that result from violation of this ISMS Policy.

Sonatype Personnel who are requested to undertake an activity that is believed to be in violation of this ISMS Policy must provide a written or verbal complaint to his or her manager, any Sonatype executive or the Human Resources Department as soon as possible.

ISMS Policies

All security documentation including policies will be developed in accordance with the Security Documentation Standard.

The policies which support the ISMS Program for Sonatype are listed below, along with a summary. All policies must be reviewed by an ISMC member annually with that review reported to the ISMC. Any material changes require ISMC approval prior to implementation. All document changes and required reviews will be documented via an approved work tracking solution for audit and historical purposes. Document reviews must include documentation of the date the changes occurred, what changes were made, and the date on which the changes were approved by the ISMC.

ISMS policies are supported by operational plans and procedures which provide guidance on operation, reporting, and implementation status to support the ISMS policies.

Acceptable Use Policy establishes rules for the acceptable use of information and of assets associated with information and information processing facilities.

Business Continuity and Disaster Recovery Policy lays out processes and procedures that

enable Sonatype to respond to any significant business disruption. It allows Sonatype to make a financial and operational assessment, it ensures quick recovery and resumption of operations, and it allows Sonatype customers to transact business.

Change Management Policy establishes the requirements and responsibilities associated with Change Management at Sonatype. This policy also defines the approval process for system changes, and the reporting requirements for all changes.

Compliance Program Policy establishes a framework to help Sonatype maintain compliance with the laws applicable to our business, to meet Sonatype's privacy-related contractual commitments, and ensure that we adhere to our internal company commitments. The program also is aimed at building and retaining the trust of Sonatype's customers, website users, employees, and partners based on respect for their privacy concerns and our protection of information with reasonable security safeguards.

Cryptographic Management Policy establishes the roles, responsibilities, and reporting requirements for cryptography and public-key infrastructure at Sonatype.

Information Classification Policy establishes a framework for classifying data based on its sensitivity, value and criticality to the organization, so highly sensitive, valuable and/or critical corporate and customer data can be secured appropriately.

Global Information Security Policy protects Sonatype and allow for the efficient execution of generally accepted security principles designed to secure the confidential, proprietary and/or sensitive information and information systems and assets of Sonatype, its customers and any other third party that has entrusted Sonatype with the same (collectively, the "Sonatype Information"). Includes acceptable use of computer equipment at Sonatype and establishes controls for end user devices, remote access, mobile computing, and storage devices processing, storing or accessing Sonatype information.

Risk Management Policy describes how we identify and manage risks to the organization and establishes the use of an industry standard framework, tracking, and reporting methodologies.

Secure Software and Systems Development Policy establishes the roles, responsibilities, and reporting requirements for software and system development at Sonatype. Includes, secure coding, system hardening, anti-malware, testing, and backup/restore.

Security Incident Management Policy provides the framework to identify, report, and act upon security events, incidents, and breaches.

Third Party Risk Assessment Policy designed to help Sonatype identify and assess security risks associated with vendors (outsourcing firms, technology and service partners, and contractors) who will connect or have access to Sonatype systems or information assets or information that is installed on or operated by Sonatype Personnel.

Vulnerability Management and Monitoring Policy establishes the roles, responsibilities, and requirements related to auditing, logging, and monitoring of security audit/event logs,

vulnerability or penetration assessments and remediation associated with the creation and operation of Sonatype systems, and its supporting infrastructure.

Table 1

Sonatype Information Security Management Committee	
Members	**Chairperson**
<Redacted>, SVP Engineering	<Redacted>, Information Security
<Redacted>, SVP and CTO	
<Redacted>, CFO	
<Redacted>, General Counsel	
<Redacted>, VP HR	

Table 2

Sonatype Summary of Interested Parties				
Interested Party	**Ref**	**Requirement**	**Source/supporting documents**	**Internal/External**
Shareholders	R1	System Integrity must be maintained	System Monitoring, Auditing, and Reporting	Internal/External
	R2	Organizational reputation must be protected	System Monitoring, Auditing, and Reporting	Internal/External
Suppliers	R3	Compliance Requirements must be met		External
	R4	Data Confidentiality must be maintained	Supplier agreements	External
Customers	R5	System Availability must be maintained	System Monitoring, Auditing, and Reporting	External
	R6	Data Confidentiality must be maintained	System Monitoring, Auditing, and Reporting	External
	R7	Data Integrity must be maintained	System Monitoring, Auditing, and Reporting	External

	R8	Compliance Requirements must be met	ISO 27001:2013	Internal/External
Contractors providing services to the organization	R9	Sonatype Sensitive and Confidential information must be protected	Non-Disclosure agreements must be signed prior to access	External
Employees of the organization	R10	Must agree to all company security policies	Signed and retained copies of the Acceptable Use Agreement section of the Employee Handbook	Internal
	R11	Must comply with ISO ISMS requirements	ISMS Program and Supporting artifacts.	Internal
Sonatype Internal Departments	R12	Department determines the role played to interdependently make Sonatype successful.	ISO Policies followed and Department procedures followed for Departments in scope.	Internal

Document Control

Version #	Date	Author	Description of Change
00.00.01	06 March 2020	<Redacted>	Initial Draft
01.00.00	31 March 2020	<Redacted>	Ratified
01.01.00	26 October 2020	<Redacted>	Added ISMC Responsibilities for improvement and corrective actions, Included Table 2 for Interested parties, Removed policies that were integrated into GIS policy.
01.01.00	19 November	<Redacted>	Ratified