VERACODE

System and Organizational Controls 3 Report

Veracode Online Security Platform

Report on Veracode, Inc.'s Online Security Platform Relevant to Security, Availability, and Confidentiality for the Period April 1, 2022 through March 31, 2023

Prepared in accordance with:
AT-C 205 pursuant to *TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria)

VERACODE, INC.

REPORT ON VERACODE, INC.'S ONLINE SECURITY PLATFORM RELEVANT TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY

For the Period April 1, 2022 through March 31, 2023

TABLE OF CONTENTS

SECTION I

INDEPENDENT SERVICE AUDITORS' REPORT

BAKER NEWMAN NOYES

Baker Newman & Noyes LLC
MAINE | MASSACHUSETTS | NEW HAMPSHIRE
800.244.7444 | www.bnncpa.com

INDEPENDENT SERVICE AUDITORS' REPORT

To the Management of Veracode, Inc.
Burlington, Massachusetts

Scope

We have examined Veracode, Inc.'s (Veracode) accompanying assertion in Section II, titled "Assertion of Veracode's Management" (the assertion), that the controls within Veracode's Online Security Platform (the system) were effective throughout the period April 1, 2022 to March 31, 2023 to provide reasonable assurance that Veracode's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria).

Veracode uses the following subservice organizations:

- Deepwatch, Inc. to provide managed security services;
- Amazon Web Services, Inc. to provide cloud and infrastructure hosting services; and
- From April 1, 2022 to January 18, 2023, CoreSite Realty Corporation to provide data center hosting services.

The description of the boundaries of the System (description) indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Veracode, to achieve the service organization's service commitments and system requirements based on the applicable trust services criteria. The description presents the boundaries of Veracode's system. The description does not include any of the controls expected to be implemented at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Veracode, to achieve the service organization's service commitments and system requirements based on the applicable trust services criteria. Our examination did not include such complementary user entity controls, and we have not evaluated the suitability of the design of such controls.

Service Organization's Responsibilities

Veracode is responsible for its service commitments and system requirements and for designing, implementing and operating effective controls within the system to provide reasonable assurance that Veracode's service commitments and system requirements were achieved. In Section II, Veracode has provided the accompanying assertion about the effectiveness of the controls within the system. When preparing its assertion, Veracode is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

To the Management of Veracode, Inc.
Burlington, Massachusetts

Service Auditors' Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Our examination included the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements;
- Assessing the risks that the controls are not effective to achieve Veracode's service commitments and system requirements based on the applicable trust services criteria; and
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Veracode's service commitments and system requirements based on the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risks that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Veracode's Online Security Platform were effective throughout the period April 1, 2022 to March 31, 2023 to provide reasonable assurance that Veracode's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Baker Newman & Noyes LLC

Boston, Massachusetts
April 27, 2023

SECTION II

ASSERTION OF VERACODE, INC.'S MANAGEMENT

VERACODE

ASSERTION OF VERACODE, INC.'S MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within Veracode's Online Security Platform (the system) throughout the period April 1, 2022 to March 31, 2023 to provide reasonable assurance that Veracode's service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented in Attachment A and identifies the aspects of the system covered by our assertion.

Veracode uses the following subservice organizations:

- Deepwatch, Inc. to provide managed security services;
- Amazon Web Services, Inc. to provide cloud and infrastructure hosting services; and
- From April 1, 2022 to January 18, 2023, CoreSite Realty Corporation to provide data center hosting services.

The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Veracode, to achieve Veracode's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system does not disclose the actual controls at the subservice organizations.

The description of the boundaries of the system indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Veracode, to achieve its service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system does not extend to controls of the user entities.

We have performed an evaluation of the effectiveness of controls within the system throughout the period April 1, 2022 to March 31, 2023 to provide reasonable assurance that Veracode's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria). Veracode's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period April 1, 2022 to March 31, 2023 to provide reasonable assurance that Veracode's service commitments and system requirements were achieved based on the applicable trust services criteria.

Veracode, Inc.

DocuSigned by:
Sohail Iqbal
F6571610268A48D...

Sohail Iqbal, Chief Information Security Officer
Date: April 27, 2023

ATTACHMENT A

VERACODE, INC.'S ONLINE SECURITY PLATFORM OVERVIEW

VERACODE, INC.

ATTACHMENT A: VERACODE, INC.'S ONLINE SECURITY PLATFORM OVERVIEW

For the Period April 1, 2022 through March 31, 2023

OVERVIEW OF VERACODE, INC.

Veracode, Inc. (Veracode) is an Application Security (AppSec) partner for creating secure software, reducing the risk of security breach, and increasing security and development teams' productivity. As a result, companies using Veracode can move their business forward. With its combination of automation, integrations, process, and speed, Veracode helps companies get accurate and reliable results to focus their efforts on fixing, not just finding, potential vulnerabilities.

Veracode serves more than 2,600 customers worldwide across a wide range of industries. The Veracode Online Security Platform (VOSP or the System) has assessed more than 120 trillion lines of code and helped companies fix more than 82 million security flaws.

VERACODE ONLINE SECURITY PLATFORM OVERVIEW (BOUNDARIES OF THE SYSTEM AND SOFTWARE)

The VOSP is designed to assist organizations in verifying an application's security state and determining acceptable levels of risk before the software is deployed for business use. It resides on Veracode's private cloud and provides a centralized way for customers to secure web, mobile and third-party applications across their global infrastructure throughout the system lifecycle.

The traditional, on-premises approach to application security may not adequately address pervasive application-layer risk across global enterprises. Unnecessary complexity for rapidly moving development teams and a decentralized model present challenges to consistently apply policies, reporting and metrics.

The Veracode cloud-based approach is fundamentally different. It is simpler and more scalable to help systematically reduce application-layer risk across Veracode's customers' entire global software infrastructure.

The VOSP is comprised of the following characteristics:

Central Policy Manager

The Central Policy Manager enables enterprises to define and enforce uniform security policies across their applications, including third-party software (such as outsourced applications and third-party libraries), business units, and development teams in their organizations.

Security Analytics and Peer Benchmarking

The VOSP provides a suite of analytical dashboards to provide customers with a fast and comprehensive way to track their application security program and to compare their security posture to industry peers.

The dashboards present an analysis of results from the numerous applications and lines of code scanned by the VOSP to help better understand the threat space and quantitatively compare the security of applications against industry peers.

Compliance Workflow Automation

The VOSP assesses applications for compliance with common compliance frameworks and industry standards and allows customers to customize policies to support specific audit requirements. It contains compliance workflows to automate tasks such as notifications about policy changes and approval workflows for compensating controls.

Role-Based Access Control

The VOSP utilizes role-based access control to help enable user organizations to securely upload and scan binaries, scan web applications, and view results and metrics. Veracode and customer users are assigned to specific roles with pre-defined permissions.

APIs & Plugins

To help maximize developer productivity and adoption, the VOSP helps integrate security analysis into existing workflows with application program interfaces (APIs) and plugins.

PRODUCTS

Veracode Static Analysis

Veracode Static Analysis provides fast, automated security feedback to developers with an Integrated Development Environment (IDE) Scan, a Pipeline Scan, and a full Policy Scan before deployment to ensure compliance with industry standards and regulations. It gives clear guidance on what issues to focus on and how to fix them. Results have high accuracy without manual tuning based on the amount of code scanned through the System's SaaS-based engines. Veracode's development security operations programs help organizations automate security feedback, align with development to reduce the security debt, and help scale to more applications through best practices and on-demand expertise.

Veracode Dynamic Analysis

Veracode Dynamic Analysis helps companies scan their web applications for exploitable vulnerabilities at scale. Dynamic Analysis scans detect potential attack points by crawling web applications and API specifications and checking for vulnerabilities that put applications at risk of attack. With an ability to test applications simultaneously, coupled with comprehensive remediation guidance, customers are able to reduce their risk of a breach across their web applications.

Veracode Software Composition Analysis

Veracode Software Composition Analysis (SCA) identifies risks from open-source libraries early so customers can reduce unplanned work, covering both security and license risk. The SCA tool helps engineering departments keep roadmaps on track, security teams achieve regulatory compliance, and business teams make smart decisions.

Veracode SCA also protects customers' applications from open-source risk by identifying known vulnerabilities in open-source libraries used by their applications. In addition to providing a list of vulnerabilities when a customer's application is scanned, Veracode SCA can also alert them when new vulnerabilities are discovered after their application has been scanned or when existing known vulnerabilities have had their severity level elevated. Integrated with continuous integration (CI) systems, a customer can fail their build based on vulnerabilities discovered as well as any components that their security team has blacklisted. As part of the VOSP, Veracode SCA provides a unified experience to display all of its security testing results in one place. Additionally, the VOSP provides unified management of users, policies, mitigations, and integrations.

Veracode Developer Training

Veracode developer training was created to help foster a higher level of security awareness and proficiency among developers with comprehensive training delivered via Veracode's platform and help address compliance requirements and embed security best practices into the Software Development Lifecycle (SDLC) to rapidly address compliance requirements.

SERVICES

Strong security means more than having powerful technology. Veracode services help developers rapidly identify, understand and remediate critical vulnerabilities, and help transform decentralized, ad hoc application security processes into ongoing, policy-based governance.

Veracode Application Security Consulting

Veracode's services help developers efficiently incorporate secure coding skills and practices into their existing development processes. Veracode has assisted development teams overcome their resistance to changes required to develop secure code.

Veracode's specialized services help developers understand assessment results, prioritize remediation efforts, and integrate with existing SDLC tools and processes.

Veracode Security Program Management

Veracode's Security Program Managers (SPMs) enable the end-to-end success of a customer's global application security program. Veracode's Program Managers help customers implement enterprise-wide governance models and day-to-day tactics to systematically reduce risk from application-layer attacks based on industry-wide best practices, and address risk associated with third parties.

Veracode Manual Penetration Testing

Veracode Manual Penetration Testing (MPT) adds the benefit of specialized human expertise to automated binary static and dynamic analysis, and it uses the same methodology cyber-criminals use to exploit application weaknesses such as business logic vulnerabilities.

Reducing false negative (FN) rates in the most critical applications requires a combination of multiple techniques, including static application security testing (SAST), dynamic application security testing (DAST), and MPT.

The VOSP provides a single central location for consolidating results from these multiple techniques, as well as for sharing results across multiple teams and evaluating risk using a consistent set of enterprise-wide policies.

Veracode Verified

Veracode Verified provides customers attestation that their development team has a framework in place to assess the security of an identified application. Implementing this program helps customers make security part of their competitive advantage, defend their AppSec budget, and better integrate security with development. Through the use of Veracode Verified, customers can integrate their secure development process around an application and their developers can integrate AppSec into their development process.

VERACODE, INC.

ATTACHMENT A: VERACODE, INC.'S ONLINE SECURITY PLATFORM OVERVIEW

For the Period April 1, 2022 through March 31, 2023

COMPONENTS OF THE SYSTEM

Collectively, the VOSP consists of the following components:

Software

The VOSP, developed in-house and managed by Veracode, is responsible for supporting certain aspects of Veracode's services provided to customers, including application submission, job scheduling, establishing user accounts, generating notifications, customer reporting, and collaborative remediation of application security flaws. The VOSP system's architecture is supported by the following software components:

Veracode Online Security Platform (VOSP) Production Cloud Systems	Production Cloud Systems
Application Servers	JBoss
Web Servers	Tomcat Apache
Production Databases	Amazon Relational Database Service (Amazon RDS) • Oracle • Aurora PostgreSQL Non-RDS Databases • Amazon Redshift • Amazon Web Services, Inc. (AWS) ElastiCache for REDIS
Operating Systems	Amazon Linux v2
Network Components	AWS Elastic Load Balancers AWS Virtual Private Cloud (VPC) private networking AWS VPC Peering AWS Transit Gateway AWS Direct Connect for management access to corporate networks CloudFlare Proxies and DDOS protection for edge security
Cloud Compute	AWS EC2 autoscaling groups

Infrastructure

The technology infrastructure supporting the VOSP resides primarily within data center facilities hosted by third-party service provider AWS, within US-East availability zone, with additional supporting infrastructure, from April 1, 2022 to January 18, 2023, within a co-location data center facility owned by CoreSite Realty Corporation (CoreSite) in Somerville, Massachusetts. As part of Veracode's internal controls, Veracode management has designed and implemented policies and procedures that monitor activities performed by AWS and CoreSite, including physical security, logical security and change management.

The production hardware supporting the VOSP, the part which was hosted from April 1, 2022 to January 18, 2023 in CoreSite, included equipment from the following vendors:

Physical Production Systems	CoreSite Production System Vendors
Production Servers	Dell Hewlett Packard (HP)
Firewalls & Switches	Palo Alto Networks Cisco

The VOSP's architecture follows a multi-structured design model comprised of web, application, middleware, and database layers and microservices. Each respective layer and the supporting infrastructure are implemented utilizing server farms and high-availability clustering to eliminate any single point of failure. This n-tiered design includes a segmented DMZ Network.

Veracode's end-user devices include Microsoft Windows and Apple MacOS computers deployed with full disk encryption. Mobile devices used by Veracode employees / contractors are required to have mobile device management software incorporated to secure data.

People

The following functional groups within Veracode are responsible for supporting the VOSP:

- **Engineering:** This group is responsible for the design, development, quality assurance (QA), and performance testing of the VOSP.
- **Production Operations**: This group is responsible for the overall production environment and infrastructure, oversight of production software deployment, and coordination of the production engineering activity.
- **Services (Customer Success and Support)**: These groups are responsible for customer relationship management, satisfaction, and support, along with technical account management and user account management.
- **Information Technology (IT)**: This group is responsible for the monitoring and maintenance of the corporate IT infrastructure, Development, QA, and Staging environments as well as the infrastructure supporting the System.
- **Information Security Oversight Committee (ISOC)**: The ISOC serves as Veracode's overall governing Information Security body, responsible for providing strategic direction and oversight of the information security program, reviewing and approving changes, and monitoring ongoing effectiveness of security policies, procedures, and processes applicable to the VOSP.
- **Information Security Assessment Team (ISAT**): The ISAT is a subset of the ISOC and is primarily responsible for coordinating and executing incident response protocols, ensuring compliance with current security procedures, and developing changes to existing security and confidentiality policies, procedures, and processes.
- **Product Security Incident Response Team (PSIRT):** The PSIRT is a tactical cross-functional product team who assesses immediate and emerging threats to the VOSP. The PSIRT develops direct tactical response plans (countermeasures) to secure the VOSP.
- **Production Engineering:** This group provides management, monitoring, and maintenance of all the production hardware, operating systems, network infrastructure, and database components of the VOSP.

Procedures

Veracode has documented policies and procedures that support the management, operations, monitoring, and controls over the VOSP. Specific examples of relevant policies and procedures include, but are not limited to, the following:

- Policy management and communication
- System security and administration
- Computer and network operations
- Service application management and administration
- Backup management and processing
- Monitoring and event correlation
- Vulnerability management
- Incident response
- Change management, including release to production processes

Policies are made available to employees through the Veracode intranet site, reviewed annually by the ISOC, and updated where required.

Data

The System manages customer data stored on encrypted storage, as well as within production databases and devices within the physically secured data centers. Customer data files located on the operating system are encrypted using unique keys assigned to each individual customer application that is analyzed. Select fields of customer information within the database environments are also stored in encrypted format for enhanced protection.

Customer information currently maintained by the VOSP includes:

Data Used and Supported by the Veracode Application Security Services System		
Data Description	**Data Retention**	**Classification**
Account and user information	Based on customer contract	Confidential
Application metadata	Unlimited	Confidential
Application binary files	45 days	Confidential
Application vulnerability result data	Based on customer contract	Confidential
System and application log data	Six months	Confidential

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS (CSOCs)

Veracode utilizes various subservice organizations to provide its products and services. Veracode's controls related to the VOSP cover only a portion of overall internal control for each client of Veracode. It is not feasible for the controls to be achieved solely by Veracode. It is expected that the subservice organizations have implemented the controls to support achievement of the principal service commitments and system requirements based on the applicable trust services criteria, as described below.

The following is a table associated with the controls at the subservice organizations:

	Complementary Subservice Organization Controls	Trust Services Criteria
AWS and CoreSite		
1.	Subservice organizations are responsible for ensuring that physical access to the data center facilities is restricted to appropriate personnel who require such access to perform their job functions and monitored appropriately for breaches.	CC6.4
2.	Subservice organizations are responsible for notifying Veracode Management of potential security breaches.	CC6.4
3.	Subservice organizations are responsible for ensuring that environmental safeguards at the data center facilities are designed, implemented, operated, and maintained, including the following: • Fire detection and suppression systems • Climate, including temperature and humidity, control systems • Uninterruptible power supplies (UPS) and backup generators • Redundant power and telecommunications lines	A1.2
AWS and Deepwatch		
4.	Subservice organizations are responsible for ensuring that access to data, software, functions, and other IT resources is limited to authorized and appropriate personnel.	CC6.2, CC6.3
5.	Subservice organizations are responsible for ensuring that current and future processing capacity is monitored and evaluated.	A1.1
6.	Subservice organizations are responsible for ensuring that data backup processes and procedures, along with recovery infrastructure, are designed, developed, implemented, operated, monitored, and maintained to help ensure that the System is available and recoverable.	A1.2
AWS		
7.	Subservice organizations are responsible for ensuring that physical media is properly disposed of.	CC6.5, C1.2

COMPLEMENTARY USER ENTITY CONTROLS

Veracode's services were designed with the assumption that certain controls would be implemented by user entities. These controls should be in operation at user entities to complement Veracode's controls. The user entity controls subsequently presented should not be regarded as a comprehensive list of all controls that should be employed by user entities.

User entities of Veracode's system should maintain controls to provide reasonable assurance that the following requirements are met for the specified applicable trust services criteria:

CC2.0 Common Criteria Related to Communication and Information

	Complementary User Entity Controls	Trust Services Criteria
1.	User entities are responsible for communicating any identified security violations to Veracode on a timely basis.	CC2.2, CC2.3
2.	User entities are responsible for communicating security, availability, and confidentiality provisions to individuals accessing information within the VOSP.	CC2.2
3.	User entities of the VOSP are responsible for reviewing documentation provided by Veracode related to changes to the VOSP.	CC2.2

CC4.0 Common Criteria Related to Monitoring Activities

	Complementary User Entity Controls	Trust Services Criteria
1.	User entities are responsible for monitoring the VOSP for notification and status information.	CC4.1

CC6.0 Common Criteria Related to Logical and Physical Access

	Complementary User Entity Controls	Trust Services Criteria
1.	User entities who utilize the Veracode Static Analysis component are responsible for the management of their network and server infrastructure.	CC6.1
2.	User entities are responsible for ensuring that access to the VOSP is limited to authorized and appropriate individuals, including the process and controls around the administering of access and securing user IDs and passwords.	CC6.1, CC6.2
3.	User entities are responsible for reviewing their employees' (including any contractors) access to the VOSP and notifying Veracode of any discrepancies.	CC6.3

CC7.0 Common Criteria Related to System Operations

	Complementary User Entity Controls	Trust Services Criteria
1.	User entities are responsible for communicating any identified security violations to Veracode on a timely basis, as necessary.	CC7.3
2.	User entities of the VOSP are responsible for reporting any security or confidentiality breaches and availability incidents which impact the System.	CC7.3

C1.0 Additional Criteria for Confidentiality

	Complementary User Entity Controls	Trust Services Criteria
1.	User entities are responsible for approving and validating the appropriateness (and maintaining the confidentiality) of data provided to Veracode and any changes to that data.	C1.1
2.	User entities are responsible for communicating any changes to data retention and disposal requirements to Veracode on a timely basis.	C1.1, C1.2
3.	User entities are responsible for adequately securing data contained in any output reports provided by Veracode, including appropriateness of individuals accessing the output reports through the VOSP and storage/disposal of the output reports.	C1.2
4.	User entities are responsible for retaining and disposing of vulnerability reports in accordance with their data retention and disposal policies.	C1.1, C1.2

ATTACHMENT B

PRINICPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

VERACODE, INC.

ATTACHMENT B: PRINICIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

For the Period April 1, 2022 through March 31, 2023

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Veracode designs its processes and procedures related to its system to meet its objective for providing its VOSP. Those objectives are based on the service commitments Veracode makes to user entities of the System. Service commitments made to customers are documented and communicated in customer contracts which stipulate the terms and conditions of the relationship between a customer and Veracode.

Base security, availability and confidentiality commitments include, but are not limited to, the following:

- **Security:** Veracode has made commitments to maintaining adequate security over customer information using reasonable safeguards over the hardware, software, personnel, and other relevant security controls, including role-based access controls, the principle of segregation of duties, the principle of least privilege, and related processes used to support the secure delivery of the VOSP;
- **Availability:** Veracode has made commitments to customers to make the software available at least 99% of the time in any calendar month during the customer's subscription term, excluding scheduled maintenance and any unavailability caused by circumstances beyond its reasonable control; and
- **Confidentiality:** Veracode has made commitments related to maintaining the confidentiality of customers' data through data classification policies, data encryption and data loss prevention tools.

Veracode has established operational and system requirements that support the achievement of security, availability, and confidentiality service commitments. Such requirements are communicated internally through system procedures described throughout the report.

ATTACHMENT C

AICPA TRUST SERVICES CRITERIA

VERACODE, INC.

ATTACHMENT C: AICPA TRUST SERVICES CRITERIA

For the Period April 1, 2022 through March 31, 2023

AICPA TRUST SERVICES CRITERIA

This attachment includes the AICPA trust services criteria, included in the scope of the engagement, relevant to security, availability, and confidentiality set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy,* American Institute of Certified Public Accountants (AICPA, Trust Services Criteria).

CRITERIA	COMMON CRITERIA RELEVANT TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY
CC1.0 Common Criteria: Control Environment	
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
CC2.0 Common Criteria: Communication and Information	
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.
CC3.0 Common Criteria: Risk Assessment	
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.
CC4.0 Common Criteria: Monitoring Activities	
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

VERACODE, INC.

ATTACHMENT C: AICPA TRUST SERVICES CRITERIA

For the Period April 1, 2022 through March 31, 2023

CRITERIA	COMMON CRITERIA RELEVANT TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY
CC5.0 Common Criteria: Control Activities	
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.
CC6.0 Common Criteria: Logical and Physical Access Controls	
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.
CC7.0 Common Criteria: System Operations	
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.

CRITERIA	COMMON CRITERIA RELEVANT TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.
CC8.0 Common Criteria: Change Management	
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.
CC9.0 Common Criteria: Risk Management	
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.

CRITERIA	ADDITIONAL CRITERIA RELATED TO AVAILABILITY
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.

CRITERIA	ADDITIONAL CRITERIA RELATED TO CONFIDENTIALITY
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.

You change the world, we'll secure it.

Veracode is the leading AppSec partner for creating secure software, reducing the risk of security breach, and increasing security and development teams' productivity. As a result, companies using Veracode can move their business, and the world, forward. With its combination of automation, integrations, process, and speed, Veracode helps companies get accurate and reliable results to focus their efforts on fixing, not just finding, potential vulnerabilities.

Learn more at www.veracode.com, on the Veracode blog, and on Twitter.

VERACODE

Veracode Headquarters
65 Network Drive
Burlington, MA 01803

Phone 339.674.2500
Fax 339.674.2502
Email contact@veracode.com

EMEA Headquarters
4th Floor, One Kingdom Street
Paddington Central
London, W2 6BD

Phone +44 (0) 203 427 6025
Email emeat@veracode.com