O-TTPS Conformance Statement

The Conformance Statement contains a series of questions that need to be answered. Complete all of the fields in the questionnaire. The completed document is a Conformance Statement for your Organization that identifies the version of the Open Trusted Technology Provider™ Standard (O-TTPS) with which you comply and indicates how you comply with the O-TTPS. Your completed form must be submitted to the Certification Authority as part of your application for certification. Please note that all information in this Conformance Statement will appear on the public Certification Register.

Certification ID
BAS10275

Name of Organization
Base64.ai

URL for your organization's website:
https://base64.ai

Tier of Certification

Tier of Certification
Self-Assessed

Scope of Certification

The certification will be against the current version of the Standard.

Enter the specific release of the O-TTPS against which the Organization's Scope of Certification is to be certified.
O-TTPS Version 1.1.1 (ISO/IEC 20243:2018)

Enter a full unambiguous description of the Scope of Certification
Base64.ai Inc

Optionally enter any explicit exclusions to the Scope of Certification:

Indicate which of the following best describes the nature of your Organization as it applies to your Scope of Certification:
Original Equipment Manufacturer (OEM)
Integrator/Value-Add Reseller
Pass-Through Reseller or Distributor

Scope of Certification

If you indicated that you are an Integrator/Value-Add Reseller, then please indicate which of the following areas represent your value add. Check all that apply:

Product Development/Engineering Method
PD_DES: Software/Firmware/Hardware Design Process
PD_CFM: Configuration Management
PD_MPP: Well-defined Development/Engineering Method Process and Practices
PD_QAT: Quality and Test Management
PD_PSM: Product Sustainment Management

Secure Development/Engineering Method
SE_TAM: Threat Analysis and Mitigation
SE_RTP: Run-time Protection Techniques
SE_VAR: Vulnerability Analysis and Response
SE_PPR: Product Patching and Remediation
SE_SEP: Secure Engineering Practices
SE_MTL: Monitor and Assess the Impact of Changes in the Threat Landscape

---

Supply Chain Security
SC_RSM: Risk Management
SC_PHS: Physical Security
SC_ACC: Access Controls
SC_ESS: Employee and Supplier Security and Integrity
SC_BPS: Business Partner Security
SC_ISS: Information Systems Security
SC_TTC: Trusted Technology Components
SC_STH: Secure Transmission and Handling
SC_MAL: Malware Detection

Self-Assessed Assessment Summary

When entering a response to each appropriate Attribute, please refer to Chapter 4 of the O-TTPS Standard document. The document can be found here: http://ottps-cert.opengroup.org/ottps-standard.

The Assessment Procedures document provides additional guidance to those that choose the Self-Assessed tier. The document can be found here: http://ottps-cert.opengroup.org/ottps-assessment-procedures.

It is important to note that the Certification Authority will not publicly release the Self-Assessed Assessment Summary. This information is intended solely for the Certification Authority and will not be disclosed to the public.

PD_DES: Software/Firmware/ Hardware Design Process
A formal process exists that defines and documents how the requirements are translated into a product design. Product Owner (PO) defines the scope and expectations of the feature. PO typically uses various tools such as Google Docs, Google Slides, Figma, Photoshop to adequately explain the design and collect feedback from various groups within the company (engineering, sales, customer success, etc.) as well as from the customers when needed. PO updates the materials with the feedback and reiterates the process until a satisfactory solution is achieved. Once ready, the project is placed in the weekly sprint planning for engineering to work on it. Depending of the size of the feature, the engineer may need to create a separate engineering design document and seek feedback from their peers. When the engineer is done with the development, they seek code review and visual check (if UI or API) feedback from other team members and authorized engineers. When the teams are ready to launch, the engineer submits their code in GitHub. The go-live process (testing, build, deployment) are automated. Once the feature is in production a final sanity check is ran manually to ensure the feature works as intended and the quality is satisfactory.

PD_CFM: Configuration Management
A formal process and supporting systems exist, which assure the proper management, control, and tracking of change to product development and manufacturing assets and artifacts. The changes are designed using the "PD_DES: Software/Firmware/ Hardware Design Process" methodology. The changes are first tested in testing/staging environment to avoid any possible outages. Configuration changes can only be applied by a limited set of lead engineers that are trained for this change. The changes can be tracked in the platform for root cause analysis and audit purposes.

PD_MPP: Well-defined Development/Engineering Method Process and Practices
Development/engineering processes and practices are documented, managed, and followed across the life cycle. The engineers must followed the practices including engineering onboarding, secure coding training, design review, code review, production monitoring. Engineers cannot bypass the automated checks to deploy code to production. Their performance is assessed regularly by their team leads and managers. Employees who don't show satisfactory performance can be terminated.

PD_QAT: Quality and Test Management
Each change in the codebase goes through rigorous automated and manual tests. Automated tests include static code analysis, unit/feature/scenario tests. The codebase is scanned against malicious codes and new third party libraries. The company undergoes periodic penetration and vulnerability testing.

PD_PSM: Product Sustainment Management
Product support, release maintenance, and defect management are product sustainment services offered to acquirers while the product is generally available. The company has a Customer Success team under

the management of a full-time Customer Success Director. They ensure that the customers can report issues from various channels, including email, Zendesk, Slack, phone, WhatsApp, and website chat. The tickets are tracked in Zendesk and can be audited. The CS team builds a bridge between the customers and engineers by facilitating communication and relaying expectations. The customers can also report issues from the website UI or API.

SE_TAM: Threat Analysis and Mitigation
Threat analysis and mitigation identify a set of potential attacks on a particular product or system and describe how those attacks might be perpetrated and the best methods of preventing or mitigating potential attacks. The company uses automated and manual thread analysis tools including dependency checking (e.g., npm audit), Grafana monitoring for resources (CPU, memory, disk, etc), and third party penetration and vulnerability testing. Issues are prioritized over features and resolved in accordance to the "PD_DES: Software/Firmware/ Hardware Design Process" and "PD_CFM: Configuration Management".

SE_RTP: Run-time Protection Techniques
The engineering team uses layered error catching and correction methods. The software has "honey pots" to detect bad actors. The exact location and content of honey pots are not publicly disclosed.

SE_VAR: Vulnerability Analysis and Response
As described in "PD_DES: Software/Firmware/ Hardware Design Process" and "SE_TAM: Threat Analysis and Mitigation", the software and service goes regular testing via static code analysis, dynamic testing (unit/feature/scenario), dependency testing, and third party analysis (vulnerability scan and pentest)

SE_PPR: Product Patching and Remediation
As described in "PD_DES: Software/Firmware/ Hardware Design Process" and "PD_CFM: Configuration Management", product is patched and improved regularly. The prioritization is security patches and critical bugs. Upon patching, the affected customers are notified as described in "PD_PSM: Product Sustainment Management". The cloud users are patched automatically while on-premises users are scheduled for a new deployment at their convenience.

SE_SEP: Secure Engineering Practices
All engineers must go through a third party secure coding training upon hire and at least once a year. The user inputs are sanitized on the backend services. The solution runs in containerized Google Cloud servers where the host security is owned by Google Cloud and engineers don't have access to servers. The data at rest (database and file stores) is encrypted. Only HTTPS connections are allowed to the cloud services.

SE_MTL: Monitor and Assess the Impact of Changes in the Threat Landscape
The engineering team reviews its plans and processes weekly in Engineering Team Meeting and monthly in the Incident Review Meeting. Customer Success and Engineering teams meet weekly in Customer Success Management Meeting to discuss open customer issues and create a mitigation plan for each issue.

SC_RSM: Risk Management
The vendor risk management is done upon onboarding. Critical vendors (such as Google Cloud) is assessed annually for risk management. The management team meets quarterly at the Quarterly Risk Committee to discuss the risks to the business. The employees undergo annual training and employee computers are monitored.

SC_PHS: Physical Security
The company does not own any physical assets. The employees work from their homes. The servers are managed by Google Cloud. Company physical mail is managed in a secure UPS mailbox.

SC_ACC: Access Controls
The company employs a user and role based access control. Users don't share their accounts. Each user has access to systems that are limited for their job function. The access is quarterly reviewed and unnecessary access rights are removed. Employees who left the company also lose their access at their last day or earlier when necessary.

SC_ESS: Employee and Supplier Security and Integrity
Background checks are conducted for employees and contractors whose activities are directly related to sensitive product supply chain activities. Checkr is used as a third party service for criminal background check, education & employment verification. The employees receive the Employee Code of Conduct and they must sign it. Employees receive a series of trainings from secure coding to anti-harassment. All employees must be eligible to work within their jurisdiction.

SC_BPS: Business Partner Security
As described in "SC_RSM: Risk Management", all vendors undergo verification to meet the company's SOC 2 Type 1 & 2, HIPAA, and GDPR standards. Critical vendors are periodically checked throughout the vendor lifecycle. Vendors who don't meet the certification standards won't have access to restricted data. Each vendor has an owner who is responsible for checking the vendor's eligibility.

SC_ISS: Information Systems Security
The Information Security Policy defines logical and physical security of the servers, laptops, and configuration.

SC_TTC: Trusted Technology Components
As defined in "SC_BPS: Business Partner Security", the vendor candidates must meet the certification and regulation bar to be accepted into the ecosystem.

SC_STH: Secure Transmission and Handling
The services only accept encrypted and secure HTTPS communication. Unencrypted transmissions are not accepted. The employees can only communicate via company Zoom, Slack, Google Drive, and email that is access controlled and audited. The employee laptops must have the disk encryption turned on.

SC_MAL: Malware Detection
The codebase is automatically checked against the latest malicious dependencies and vulnerabilities. The employee computers run antivirus and antimalware software. The email provider (Gmail) runs anti-malware, anti-phishing, and anti-spam.