



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 component will appear on the public Certification Register.

Name of Organization

POLYWELL COMPUTERS INC.

URL for your organization's website:

<https://www.polywell.com/>

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

The scope of this certification will be for Polywell Computers INC. as an original equipment manufacturer. Produce various products such as servers, mini pcs, and AIOs.

Indicate which of the following best describes the nature of your Organization as it applies to your Scope of Certification:

Original Equipment Manufacturer (OEM)

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_STR: Supply Chain Security Training
 - SC_ISS: Information Systems Security
 - SC_TTC: Trusted Technology Components
 - SC_STH: Secure Transmission and Handling
 - SC_OSH: Open Source Handling
 - SC_CTM: Counterfeit Mitigation
 - SC_MAL: Malware Detection
-

Tier of Certification

Tier of Certification

Self-Assessed