NCC Group
Risk Management & Governance

PRP PRIVACY
certified by nccgroup™

Thoropass, Inc.

APEC PRP Report

APEC PRP Certification Review

Asia Pacific Economic Cooperation (APEC) Privacy Recognition for Processors (PRP) System

Version 1.1 – May 10, 2024

www.nccgroup.com

Document Control

Document Version Control	
Document Classification:	Confidential
Client Name	Thoropass, Inc. (“Thoropass”)
NCCGP Document:	Version 1.0 for Thoropass review Version 1.1 Final Report
Document Title	APEC PRP Report
Author Names:	Randy Rodriguez & Erin Gergory
Technical Approval:	Kurt Osburn

Table of Contents

1. Background and Scope

i. Name of the Organization that is seeking certification:
Thoropass, Inc. (“Thoropass”)

ii. List of subsidiaries and/or affiliates governed by your privacy policy to be covered by this certification, their location, and the relationship of each to you:
* Location(s) in Scope: All work will be performed remotely. Client scope is all cloud hosted.
* Applications/Systems in Scope: Thoropass Application system, including the Jarvis and Polaris applications.

iii. Organization's Contact Point for Privacy Recognition for Processors ("PRP")
Name: Jay Trinckes
Title: Data Protection Officer/CISO
Email: jay.trinckes@thoropass.com
Phone: 352-339-3887

iv. For what type(s) of personal information are you applying for certification?
Customer/ Prospective Customer: Both customers and prospective customers
Employee/Prospective Employee: Both employees and prospective employees

v. In which economies do you, your affiliates and/or subsidiaries collect or anticipate collecting personal information to be certified under this system?

Please check all that apply.

Economies	Check
Australia	☑
Brunei Darussalam	☑
Canada	☑
Chile	☑
People's Republic of China	☑
Hong Kong, China	☑
Indonesia	☑
Japan	☑
Republic of Korea	☑
Malaysia	☑
Mexico	☑
New Zealand	☑
Papua New Guinea	☑
Peru	☑

Economies	Check
Philippines	☑
Russia	☐
Singapore	☑
Chinese Taipei	☑
Thailand	☑
United States	☑
Vietnam	☑

vi. To which economies do you, your affiliates and/or subsidiaries transfer or anticipate transferring personal information to be certified under this system?

Please check all that apply.

Economies	Check
Australia	☐
Brunei Darussalam	☐
Canada	☐
Chile	☐
People's Republic of China	☐
Hong Kong, China	☐
Indonesia	☐
Japan	☐
Republic of Korea	☐
Malaysia	☐
Mexico	☐
New Zealand	☐
Papua New Guinea	☐
Peru	☐
Philippines	☐
Russia	☐
Singapore	☐
Chinese Taipei	☐
Thailand	☐
United States	☑
Vietnam	☐

Thoropass is a leading content services provider that enables thousands of organizations to focus on what they do best and deliver better experiences to the people they serve.
Thoropass engaged the NCC Group to perform a certification review on the organization's current levels of compliance with the Asia Pacific Economic Cooperation (APEC) Privacy Recognition for Processors (PRP) System. NCC Group is a recognized Accountability Agent under the APEC PRP Program.

The program reviews twenty-four (24) controls across the following Privacy Principles:

1. Security Safeguards
2. Accountability Measures

The purpose of this report is to provide the compliance status of Thoropass's compliance review related to the baseline program requirements of the APEC Privacy Recognition for Processors (PRP) System to ensure this process is conducted consistently throughout participating APEC Economies. NCC Group, a recognized Accountability Agent, is responsible for receiving an Applicant's intake documentation, verifying an Applicant's compliance with the requirements of the PRP System and, where appropriate, assisting the Applicant in modifying its policies and practices to meet the requirements of the PRP System. NCC Group will certify those Applicants deemed to have met the minimum criteria for participation provided herein and will be responsible for monitoring the Participants' compliance with the PRP System, based on these criteria.

2. Executive Summary

NCC Group performed this APEC PRP Certification by reviewing documentation provided as evidence to compliance, interviewing key stakeholders, observing processes in action, and performing sampling/testing where applicable. This report represents the results of this compliance review. The following ratings were used in determining the level of compliance to the APEC PRP:

Status	Description
Not Compliant	The Applicant's controls are undocumented or there are serious discrepancies between the documented controls and the APEC PRP requirements. The controls in place do not comply with or are inadequate to meet the requirements of the APEC PRP.
Partially Compliant	The Applicant maintains some documentation for existing security controls, but they may be incomplete. There are some minor discrepancies between the documented controls and the APEC PRP requirements. There may be some gaps between the control documentation and the requirements.
Compliant	The Applicant's controls adequately and sufficiently demonstrate accountability with the compliance to the APEC PRP requirements.
Not Applicable	The APEC PRP requirements are not applicable to this Applicant.

2.1 APEC PRP Compliance Status

Based on the assessment performed, Thoropass was determined to be in **compliance** with the PRP.

Section 2.2 of this report provides a summary of compliance. Section 3 of this report provides specific details of compliance efforts currently in place by the organization.

The following is a summary of the key points:

Good practices operating within Thoropass include:

General

- Thoropass shows a strong commitment and willingness to demonstrate compliance with the PRP.
- Thoropass, Inc. has provided an information security program management document which covers personal information being processed on behalf of a controller.

- Thoropass has appointed Jay Trinckes as the organization's point of contact for Privacy Recognition for Processors ("PRP").
- Thoropass, Inc. places significant emphasis on employee awareness and training for safeguarding personal information.

Security Safeguards

- Thoropass holds certifications such as SOC 2 Type II, ISO 27001:2022, and pending HITRUST CSF i1, among others. Thoropass also conducts continuous risk assessments and self-assessments for GDPR and CCPA compliance.
- Thoropass has a formal incident response policy and procedures in place, supported by technical controls like native AWS security tools and Orca Security.
- Thoropass has implemented robust measures to detect, prevent, and respond to security threats concerning personal information.

Accountability

- Thoropass restricts its processing of personal information to the purposes outlined by the controller, as stipulated in agreements such as the master service agreement (MSA), data protection addendum (DPA), and privacy notice.
- Thoropass maintains an approved list of subprocessors as specified by the controller. This list is regularly updated in Thoropass's Trust Center, and controllers are promptly notified of any additions, deletions, or modifications to this list.

2.2 Summary of Compliance

The following section provides a summary of compliance against the PRP requirements:

Number	Category	Status
1	Security Safeguards	Compliant
2	Accountability Measures	Compliant

3. Specific Details of compliance

The following provides relevant requirements of the APEC PRP, Thoropass's compliance state against the PRP framework, observations to include any deficiencies in compliance, and recommendations for improvement.

All remediation efforts must be carefully planned, funded, and resourced through a program of work to demonstrate accountability with the APEC PRP. This will enable Thoropass to achieve APEC PRP Certification.

3.1 Security Safeguards

Assessment Purpose - The questions in this section are directed towards ensuring that when individuals entrust their information to an applicant, that applicant will implement reasonable security safeguards to protect individuals' information from loss, unauthorized access or disclosure, or other misuses.

1. Has your organization implemented an information security policy that covers personal information processed on behalf of a controller?
Status: Compliant

Observations:
NCC Group observed that Thoropass, Inc. has provided an information security program management document which covers personal information being processed on behalf of a controller.

Recommendations:
No further recommendations at this time.

2. Describe the physical, technical, and administrative safeguards that implement your organization's information security policy.
Status: Compliant

Observations:
NCC Group observed that Thoropass, Inc. implements a comprehensive set of physical, technical, and administrative safeguards to protect personal information. Thoropass maintains a robust security posture with physical controls such as key fobs, cameras, security measures, and limited access to the office WiFi network, which is used solely for internet connectivity. Notably, Thoropass leverages AWS's physical security controls for its platform. Thoropass employs authentication mechanisms, stringent access controls, password protection, encryption protocols, and boundary protection via firewalls and security groups. Monitoring and audit

logging are conducted using tools like Orca Security and DataDog, as well as vulnerability assessments and penetration testing. Thoropass has a set of policies and procedures aligned with industry standards such as NIST 800-53r5, SOC 2 trust service criteria, ISO 27001:2022, ISO 27701:2019, and HITRUST CSF.

Recommendations:
No further recommendations at this time.

3. Describe how your organization makes employees aware of the importance of maintaining the security of personal information.
Status: Compliant

Observations:
NCC Group observed that Thoropass, Inc. places significant emphasis on employee awareness and training for safeguarding personal information. They conduct structured security and privacy training within 60 days of hiring, with annual refresher courses. This training is supported by regular staff meetings and communication through Slack/email, reinforcing security updates. Employees acknowledge their responsibilities through signed policies.

Recommendations:
No further recommendations at this time.

4. Has your organization implemented measures to detect, prevent, and respond to attacks, intrusions, or other security failures related to personal information?
Status: Compliant

Observations:
NCC Group observed that Thoropass has implemented robust measures to detect, prevent, and respond to security threats concerning personal information. They have a formal incident response policy and procedures in place, supported by technical controls like native AWS security tools and Orca Security.

Recommendations:
No further recommendations at this time.

5. Does your organization have processes in place to test the effectiveness of the safeguards referred to in the question above? Please describe.
Status: Compliant

Observations:
NCC Group observed that Thoropass actively tests the effectiveness of its safeguards in detecting, preventing, and responding to security threats. Daily reviews of tools allow prompt action against suspicious activities. Minor incidents are handled according to Thoropass's incident response process. Additionally, Thoropass conducts annual business continuity and

incident response tabletop exercises to validate policy/procedure adherence during incidents, followed by after-action reviews to enhance security and privacy safeguards.

Recommendations:
No further recommendations at this time.

6. Do you have a process in place to notify the controller of occurrences of a breach of the privacy or security of their organization's personal information?
Status: Compliant

Observations:
NCC Group observed that Thoropass maintains a record of processing and is obligated to notify controllers within seventy-two (72) hours of any breach affecting the privacy or security of personal information. This swift notification process ensures timely responses and mitigates potential risks associated with breaches.

Recommendations:
No further recommendations at this time.

7. Has your organization implemented procedures for the secure disposal or return of personal information when instructed by the controller or upon termination of the relationship with the controller?
Status: Compliant

Observations:
NCC Group observed that Thoropass has established procedures for securely disposing of or returning personal information as directed by the controller or upon termination of their relationship with the controller. This ensures that data is handled responsibly and in accordance with privacy guidelines.

Recommendations:
No further recommendations at this time.

8. Does your organization use third-party certifications or other risk assessments? Please describe.
Status: Compliant

Observations:
NCC Group observed that Thoropass employs third-party attestations, certifications, ongoing risk assessments, and self-assessments to validate the effectiveness of its security safeguards. They hold certifications such as SOC 2 Type II, ISO 27001:2022, and pending HITRUST CSF i1, among others. Thoropass also conducts continuous risk assessments and self-assessments for GDPR and CCPA compliance.

Recommendations:
No further recommendations at this time.

3.2 Accountability Measures

Assessment Purpose - The questions in this section are directed towards ensuring that the Applicant is accountable for complying with measures that give effect to the other Principles stated above. Additionally, when transferring information, the Applicant should be accountable for ensuring that the recipient will protect the information consistently with these Principles when not obtaining consent. Thus, you should take reasonable steps to ensure the information is protected, in accordance with these Principles, after it is transferred. However, there are certain situations where such due diligence may be impractical or impossible, for example, when there is no on-going relationship between you and the third party to whom the information is disclosed. In these types of circumstances, you may choose to use other means, such as obtaining consent, to assure that the information is being protected consistently with these Principles. However, in cases where disclosures are required by domestic law, you would be relieved of any due diligence or consent obligations.

9. Does your organization limit its processing of personal information to the purposes specified by the controller?
Status: Compliant

Observations:
NCC Group observed that Thoropass restricts its processing of personal information to the purposes outlined by the controller, as stipulated in agreements such as the master service agreement (MSA), data protection addendum (DPA), and privacy notice. This ensures that data processing remains aligned with contractual obligations and enhances transparency regarding the purposes for which personal information is used.

Recommendations:
No further recommendations at this time.

10. Does your organization have procedures in place to delete, update, and correct information upon request from the controller?
Status: Compliant

Observations:
NCC Group observed that Thoropass has established procedures for promptly deleting, updating, and correcting information upon request from the controller. Controllers are primarily responsible for managing the information they provide within the platform under their own account. However, if a controller requires assistance with any deletion, updates, or corrections, Thoropass assigns a customer service manager to facilitate and support such requests.

Recommendations:
No further recommendations at this time.

11. What measures does your organization take to ensure compliance with the controller's instructions related to the activities of personal information processing? Please describe.
Status: Compliant

Observations:
NCC Group observed that Thoropass takes proactive measures to comply with the controller's instructions regarding the processing of personal information. They keep controllers informed about all processing activities and empower controllers to direct Thoropass in the handling of personal information. Additionally, Thoropass maintains contracts with controllers that clearly specify the processing activities to be carried out with any personal information provided by the controller to Thoropass.

Recommendations:
No further recommendations at this time.

12. Have you appointed an individual(s) to be responsible for your overall compliance with the requirements of the PRP?
Status: Compliant

Observations:
NCC Group observed that Thoropass has designated the Director of Compliance as the Data Protection Officer (DPO) responsible for ensuring overall compliance with the requirements of PRP. This role encompasses overseeing data protection measures, ensuring adherence to privacy regulations, and facilitating communication between Thoropass and regulatory authorities regarding data protection matters.

Recommendations:
No further recommendations at this time.

13. Does your organization have procedures in place to forward privacy-related individual requests or complaints to the controller or to handle them when instructed by the controller?
Status: Compliant

Observations:
NCC Group observed that Thoropass has established procedures to either forward privacy-related individual requests or complaints to the controller or handle them as per the controller's instructions. Notably, Thoropass has not received any individual requests or complaints that needed forwarding to a controller in the past year.

Recommendations:
No further recommendations at this time.

14. Does your organization notify controllers, except were prohibited by law, of judicial or other government subpoenas, warrants or orders that require the disclosure of personal information?
Status: Compliant

Observations:
NCC Group observed that Thoropass has processes in place to inform controllers, unless legally prohibited, about judicial or government subpoenas, warrants, or orders mandating the disclosure of personal information. This obligation is addressed in agreements such as the Data Protection Addendum (DPA), Master Service Agreement (MSA), and Mutual Non-Disclosure Agreement (MNDA). Notably, Thoropass has not received any subpoenas, warrants, or orders for notification to a controller in the past year.

Recommendations:
No further recommendations at this time.

15. Does your organization have a procedure in place to notify the controller of your engagement of sub processors?
Status: Compliant

Observations:
NCC Group observed that Thoropass maintains an approved list of subprocessors as specified by the controller. This list is regularly updated in Thoropass's Trust Center, and controllers are promptly notified of any additions, deletions, or modifications to this list.

Recommendations:
No further recommendations at this time.

16. Does your organization have mechanisms in place with sub processors to ensure that personal information is processed in accordance with your obligations under the PRP? Please describe.
Status: Compliant

Observations:
NCC Group observed that Thoropass maintains mechanisms with subprocessors to ensure that personal information is processed in compliance with the obligations outlined in PRP. This includes conducting comprehensive vendor due diligence and third-party provider reviews, which involve vendor classification, assessment of attestations/certifications, review of contracts to ensure confidentiality/security/privacy requirements, evaluation of Trade/Sanction Compliance, and conducting data protection impact assessments (DPIAs) where relevant. These measures are integral to ensuring that subprocessors adhere to the same high standards of data protection and security as Thoropass.

Recommendations:
No further recommendations at this time.

17. Do the mechanisms referred to above generally require that sub processors:
a) Follow-instructions provided by your organization relating to the manner in which personal information must be handled?
b) Impose restrictions on further sub processing
c) Have their PRP recognized by an APEC Accountability Agent in their jurisdiction?
d) Provide your organization with self-assessments or other evidence of compliance with your instructions and/or agreements/contracts? If YES, describe.
e) Allow your organization to carry out regular spot checking or other monitoring activities? If YES, describe.
f) Other (describe)
Status: Compliant

Observations:
NCC Group observed that Thoropass ensures that subprocessors handle personal information in accordance with the terms outlined in their contracts, master service agreements, and/or privacy notices. Contracts impose limitations on processing to only what is necessary for the services provided. Thoropass conducts thorough vendor due diligence, which includes reviewing SOC 2 Type II attestations, ISO certifications, security questionnaires, and agreements/contracts. Additionally, Thoropass reserves the right to audit and conducts annual reviews of high-priority or critical vendors to maintain compliance and data security standards.

Recommendations:
No further recommendations at this time.

18. Do you have procedures in place for training employees pertaining to your privacy policies and procedures and related client instructions? Please describe.
Status: Compliant

Observations:
NCC Group observed that Thoropass incorporates privacy training into its overall security awareness program for employees. This training covers Thoropass's privacy policies, procedures, and any client-specific instructions. All employees are required to undergo privacy training within sixty (60) days of being hired and annually thereafter, ensuring that they remain informed and compliant with privacy regulations and client requirements.

Recommendations:
No further recommendations at this time.

Appendix A: Documentation Reviewed

Following is a list of documentation or evidence reviewed during this assessment.

Document
apn badge dark.png
AT - Awareness and Training Policy.pdf
AT - Awareness and Training Procedures.pdf
ato badge dark.png
AU - Audit and Accountability Policy.pdf
AU - Audit and Accountability Procedures.pdf
CA - Assessment Authorization and Monitoring Policy.pdf
CA - Assessment Authorization and Monitoring Procedures.pdf
CM - Configuration and Change Management Policy.pdf
CM - Configuration and Change Management Procedures.pdf
CP - Contingency Planning Policy.pdf
CP - Contingency Planning Procedures.pdf
Healthcare Competency dark.png
IA - Identification and Authentication Policy.pdf
IA - Identification and Authentication Procedures.pdf
IR - Incident Response Plans.pdf
IR - Incident Response Policy.pdf
IR - Incident Response Procedures.pdf
MA - Maintenance Policy.pdf
MA - Maintenance Procedures.pdf
MP - Media Protection Policy.pdf
MP - Media Protection Procedures.pdf
PE - Physical and Environment Protection Procedures.pdf
PE - Physical and Environmental Protection Policy.pdf
PL - Planning Policy.pdf
PL - Planning Procedures.pdf
PL-SSP -System Security Plan.pdf
PM - Information Security Program Management Policy.pdf
PM - Information Security Program Management Procedures.pdf
PS - Personnel Security Policy.pdf
PS - Personnel Security Procedures.pdf
PT - Privacy Policy.pdf
PT - Privacy Procedures.pdf
qualified badge dark.png

Document
RA - Risk Assessment Policy.pdf
RA - Risk Assessment Procedures.pdf
SA - System Development Life Cycle (SDLC) Policy.pdf
SA - System Development Life Cycle (SDLC) Procedures.pdf
SC - System Protection Policy.pdf
SC - System Protection Procedures.pdf
SI - System Integrity Policy.pdf
SI - System Integrity Procedures.pdf
SOC 2 Type 2 Bridge Letter 20231231.pdf
SR - Third Party Risk Management Policy.pdf
SR - Third Party Risk Management Procedures.pdf
Thoropass - Penetration Testing Report - WEB + AWS + Network - September 2023 - Customer Friendly.pdf
Thoropass CCPA Self-Assessment Report042023 (1).pdf
Thoropass CCPA Self-Assessment Report042023.pdf
Thoropass EU-US DPA Self-Assessment Report07182023 (1).pdf
Thoropass EU-US DPA Self-Assessment Report07182023.pdf
Thoropass GDPR Self-Assessment Report042023.pdf
Thoropass Infrastructure Diagram-10312023.pdf
Thoropass ISO 27701 Certificate.pdf
Thoropass Platform - DPIA20240404.pdf
Thoropass Platform - DPIA20240404.pdf
Thoropass Security and Privacy Whitepaper 09252023.pdf
Thoropass, Inc. SOC2 Type II Report - Final.pdf
ThoroPass-Final Certificate-3036.pdf
Thoropass-Global-Employee-Handbook-2023.pdf
Thoropass-ISO 27001-27701SoA09072023.pdf

Appendix B: Personnel Interviews

The following are individuals that were interviewed during this assessment.

Contact	Role	Email
Jay Trinckes	Data Protection Officer/CISO	jay.trinckes@thoropass.com