



PRIVACY NO LOG AUDIT REPORT

For

GZ Systems Limited

June 28, 2019



Table of Contents

I. Executive Summary	1
A. Introduction	1
B. Certified Auditors	1
C. Audit Methodology	1
D. Disclaimer	1
II. VPN Privacy Overview	3
A. Virtual Private Network	3
B. User Personal Information	3
C. User Activity Monitoring	3
D. User Privacy	4
III. Audit Process	5
A. PureVPN Privacy Policy	5
B. Technical Evaluation Process	6
IV. Audit Findings and Opinions	7
A. Purpose	7
B. Findings and Opinions	7
Exhibits	8
Exhibit A – Auditor’s Qualifications and Certifications	9
Exhibit B – PureVPN Privacy Policy	11

I. Executive Summary

A. INTRODUCTION

With the emergence of various privacy laws, organizations are required to ensure that their personnel and service providers comply with the organization's stated privacy practices.

Transparency is one of the Fair Information Practice Principles that underlie privacy laws and regulations globally. Beyond good security and privacy policies, transparency requires proof of proactive compliance. Independently verifying or "auditing" is a practical solution to determine the quality and integrity of privacy practices and to enhance transparency.

Altius IT's audits help ensure your organization operates with transparency, providing openness and clarity to all activities concerning the capture, collection, dissemination, and use of information.

B. CERTIFIED AUDITORS

Altius IT is board certified by the Information Systems Audit and Control Association (ISACA) as:

- Certified Information Systems Auditors
- Certified in Risk and Information Systems Controls
- Certified in the Governance of Enterprise IT

In performing the privacy no log audit, Altius IT complied with the independence and ethical requirements of the Information Systems Audit and Control Association.

Please see Exhibit A – Auditor's Qualifications and Certifications for more information.

C. AUDIT METHODOLOGY

Altius IT's services and scope included a review and evaluation of selected PureVPN documents and systems during the period June 10, 2019 – June 28, 2019.

Altius IT methodology included developing an audit work program to review and evaluate PureVPN's VPN server configurations and PureVPN's system/service log files. The purpose of the audit work program was to obtain reasonable assurance as to whether PureVPN's VPN server configurations and/or PureVPN's system/service log files independently, or collectively, could lead to identifying a specific person and/or the person's activity over the PureVPN service.

D. DISCLAIMER

This report is based on information available to Altius IT solely on the dates of our review. Any changes to the information available to Altius IT after the review date are not included in the report. Altius IT's findings and opinions rendered in this report are

based only on information and system configurations as existed and available during our review period. Based upon your organization's request for services, our scope did not include, and/or evaluate:

- Security safeguards for sufficiency and effectiveness
- Privacy and security controls at third party service provider organizations

II. VPN Privacy Overview

A. VIRTUAL PRIVATE NETWORK

A virtual private network (VPN) allows a user to send and receive data across shared or public networks (e.g. the Internet) as if he/she were directly connected to a network or private device.

A VPN can use encryption and other security mechanisms to ensure that unauthorized persons do not have access to the data during transmission. A VPN with encryption provides a secure tunnel to transmit data between the user and the network.

The VPN encrypted connection helps ensure that sensitive data is securely transmitted. Encryption prevents unauthorized persons from viewing traffic and activities and allows the user to conduct work remotely.

B. USER PERSONAL INFORMATION

Organizations may capture data necessary to provide services to their customers and users. The types of personal information that can be captured and maintained include:

- Account information – user name, e-mail address, password
- Payment information – name, address, credit card/bank account
- Communications – e-mails, text messages, chats, faxes, etc.

C. USER ACTIVITY MONITORING

User activity monitoring is the process of monitoring and recording user actions. User activity may include:

Connection logs

- Incoming and outgoing Internet Protocol (IP) addresses
- Connection success/failure, dates, times, and duration of connections
- Types and amounts of data transmitted/received
- Servers/devices accessed

Usage logs

- Browsing history, web sites visited
- Files downloaded and uploaded
- Software/applications used
- Application crashes including device information, username, and e-mail address if user chose e-mail address as a VPN username

Technical data

- Application/device – Windows, iOS, Android, etc.
- Username/e-mail if the service allows multiple VPN connections at the same time
- Timestamp of the last session
- Service performance data, used to identify most suitable servers for connectivity

D. USER PRIVACY

Many organizations require its personnel to comply with policies and procedures authorizing the specific type and extent of user activity that may be monitored and logged by the organization.

Compliance with these policies and procedures help ensure the organization's products and services are delivered in a timely and consistent manner while also ensuring the need for user privacy.

III. Audit Process

A. PUREVPN PRIVACY POLICY

Altius IT reviewed privacy-related logging statements in PureVPN's Privacy Policy <https://www.purevpn.com/privacy-policy.php> (included in this report as Exhibit B – PureVPN Privacy Policy). Section numbers listed below refer to sections within the Privacy Policy.

No Records or Logs

PureVPN's Privacy Policy stated there was no log or record of:

- Browsing activities (Section I)
- Connection logs (Section I)
- VPN IPs, original IPs (Section I)
- Connection time (Section I)
- History of browsing (Section I)
- Sites visited (Section I)
- Outgoing traffic (Section I)
- Content or data accessed (Section I)
- DNS queries (Section I)
- Origin IP address (Section IV)
- Assigned VPN server IP address (Section IV)
- VPN session timestamp (Section IV)
- Browsing activities (Section IV)
- DNS requests (Section IV, Section V)
- Specific time when connect to VPN server (Section IV)
- Activities after connecting to the server (Section IV)
- Traffic details (Section V)
- IP addresses (Section V)

General Statements

PureVPN's Privacy Policy stated in pertinent part:

- We collect minimal data (Section I)
- Systems, processes, and servers are designed not to keep any sensitive/personally identifiable data (Section I)
- No data to share (Section I)
- Data associated with payments is processed in real time without keeping any record of it (Section III)
- We don't know what you access, browse, upload, or download (Section IV)
- We have nothing personally identifiable to share (Section IV)
- We are unable to identify at what time you connect to the VPN, with which IP address, and which VPN IP was assigned (Section IV)

Information Captured

PureVPN's Privacy Policy stated that the following information was captured:

- Date the user connects to the PureVPN service (Section IV)
- User's Internet Service Provider (ISP) (Section IV)
- Total bandwidth consumed (Section IV)
- Minimal connection statistics that do not include uniquely identifiable user data or behavior (Section V)
- How often the application is used, events that occur within the application (Section V)
- Aggregated usage and performance data (Section V)
- Failed connection attempts (Section V)

PureVPN's Privacy Policy stated that tools were used to gather software analytics, stats, and diagnostics. Examples of tools listed include Google Analytics, iTunes, Crashlytics, Apptentive, Firebase, New Relic, MixPanel, and Facebook Pixel (Section V).

PureVPN's Privacy Policy listed emails, live chats, and Feedback forms as information collected and retained. Information retained include names and e-mail addresses (Section VI).

B. TECHNICAL EVALUATION PROCESS

Prior to our technical evaluation, Altius IT reviewed written documents/documentation made available to Altius IT by GZ Systems Limited. Documents evaluated by Altius IT included:

- Network diagram
- Default VPN server provisioning configuration(s) and processes documented in Orchestration server playbooks
- Process to approve and deploy updates and changes to the network

Altius IT's technical evaluation process included a comparison of PureVPN Privacy Policy's no log statements against technical configurations and logs. Altius IT:

- Identified a target sample of central servers that support the PureVPN service
- Inspected a target sample of central server relevant configurations
- Identified a target sample of VPN servers to be evaluated
- Installed PureVPN application on mobile device
- Used PureVPN mobile application in various modes (e.g. Privacy/Security, Streaming, Internet Freedom, and File Sharing) to connect to selected servers, perform browsing of various sites, and other activities
- Inspected a target sample of VPN server relevant configurations
- Inspected a target sample of VPN server log files

IV. Audit Findings and Opinions

A. PURPOSE

Altius IT 's audit process examined selected written documents, system configurations, and user processes to obtain reasonable assurance as to whether PureVPN's VPN server configurations and/or system/service log files independently, or collectively, could lead to identifying a specific person and/or the person's activity over the PureVPN service.

B. FINDINGS AND OPINIONS

On the dates of our review, Altius IT did not find any evidence of system configurations and/or system/service log files that independently, or collectively, could lead to identifying a specific person and/or the person's activity when using the PureVPN service.

Exhibits

EXHIBIT A **Auditor's Qualifications and Certifications**

EXHIBIT A – AUDITOR’S QUALIFICATIONS AND CERTIFICATIONS

A. Altius IT

Altius IT offers a full range of asset protection, security audit, privacy audit, and risk management services. Founded in 1993, Altius Information Technologies, Inc. (Altius IT) is a California Corporation providing IT security audits, security consulting, risk management, and privacy audit services. Over 1,000 organizations have relied on our expertise to help them develop and implement strategies to reduce risks.



B. Nationally Recognized Leadership

Elected by our peers into leadership roles, we are experienced information security auditors and have served on the Boards of Directors of international and national associations:

- International Association of Professional Security Consultants
- NetTeCH nationwide association of IT companies
- Association of Professional Consultants
- Technology Professionals Association



C. Expert Authority

As a leading authority, our track record of helping organizations manage risks has been featured on national television and in over 40 publications. Please visit www.altiusit.com/news.htm to view televised clips and articles.



D. Project Team Certifications

Altius, meaning "higher", embodies our philosophy of delivering higher performance and results to our clients. We believe we are uniquely qualified to provide security audit services to your organization.

Our project team certifications include:

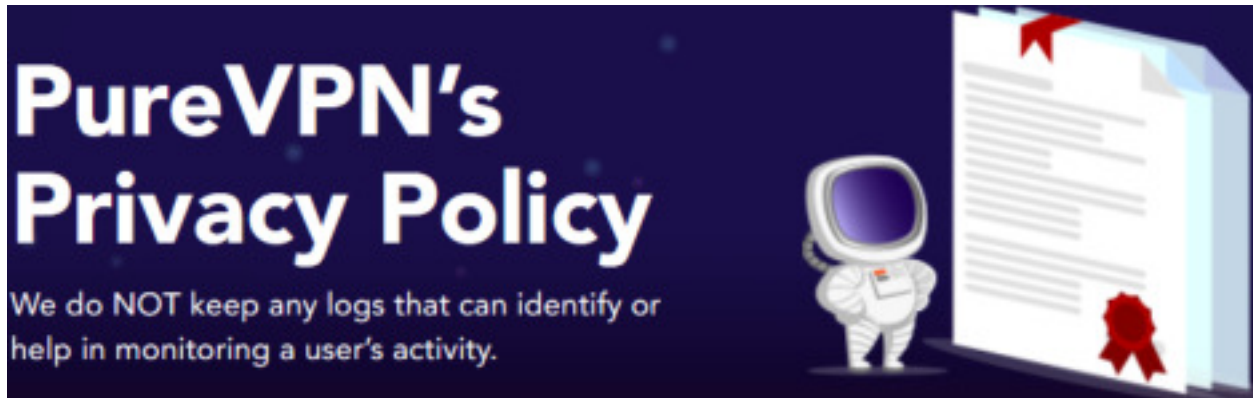
- *Certified Information Systems Auditor (CISA)*
- *Certified in Risk and Information Systems Controls (CRISC)*
- *Certified in the Governance of Enterprise IT (CGEIT)*



EXHIBIT B
PureVPN Privacy Policy

EXHIBIT B – PUREVPN PRIVACY POLICY

Information listed below was obtained from <https://www.purevpn.com/privacy-policy.php>.
Section numbers were added by Altius IT for reference purposes.



I. YOU ARE INVISIBLE – EVEN WE CANNOT SEE WHAT YOU DO ONLINE

We DO NOT keep any record of your browsing activities, connection logs, records of the VPN IPs assigned to you, your original IPs, your connection time, the history of your browsing, the sites you visited, your outgoing traffic, the content or data you accessed, or the DNS queries generated by you.

We want you to have the surety of knowing that we collect minimal data, the sole purpose of which is to operate our VPN and Proxy service and keep it running smoothly. Our systems, processes, and servers are designed to not keep any sensitive/personally identifiable data. This is done by design to ensure that we have NO data to share, even when required by law to do so.

II. TABLE OF CONTENTS

- [Information We Collect at Signup](#)
- [What We Don't Know, What We Know & What We Keep](#)
- [Information Included in VPN Connection Logs](#)
- [Details NOT Included In VPN Connection Logs](#)
- [Total Bandwidth Consumed](#)
- [Standalone DNS Service - Gravity](#)
- [URL Filter & App Blocker by PureVPN](#)
- [Software Analytics, Stats & Diagnostics](#)
- [Data from Emails, Live Chats, and Feedback Forms](#)
- [International Data Transfers](#)
- [Security Measures to Protect Your Information](#)

- [Data Retention Policy & Your Data Protection Rights](#)
- [Applicable Laws](#)
- [Cookies and PureVPN](#)
- [PureVPN and Third-Party Websites](#)
- [Consent and Age Restrictions](#)
- [Legal Basis](#)
- [Important Note](#)
- [Contact information](#)

III. INFORMATION WE COLLECT AT SIGNUP

- Your Name
- Email Address
- Payment Method

HOW WE USE THIS INFORMATION

- To provide, operate, and maintain our Services
- To improve, personalize, and expand our Services
- To communicate with you, either directly or through one of our partners, including for customer service, to provide you with updates and other information relating to the Service, and for marketing and promotional purposes
- To process your transactions
- To find and prevent fraud
- For compliance purposes, including enforcing our Terms of Service, or other legal rights

PureVPN and Data Associated With Payments

Similar to most ecommerce or online businesses, PureVPN too uses third-party payment processors. Except for a few payment processors who require us to process the payment, all the payment data rests with the respective payment processors. In instances where we are required to process the data, we process it in real time and pass it on to the processor and chargeback protection service without keeping any record of it with us. Please visit the privacy policy of the payment processor chosen by you to get a better understanding of what information it collects, stores, and uses.

Since we are huge believers in anonymity, we have included Coin Payments and Gift Cards – 100% anonymous payment methods – in the list of payment methods accepted by us.

PureVPN does not share, sell or rent your personal information with anyone apart from using your information to provide products or services you've requested for.

IV. WHAT WE DON'T KNOW, WHAT WE KNOW & WHAT WE KEEP

We have no logs or records of:

- Your origin IP address
- Assigned VPN server IP address
- VPN session timestamp
- Your browsing activities
- DNS requests

In a nutshell:

- We don't know what you access, browse, upload or download with our service.
- We are unable to identify at what time you connected to the VPN, with which IP address and which VPN IP was assigned to you.
- Even if we are compelled to share user information, we simply cannot because we have nothing personally identifiable to share.

Information Included in VPN Connection Logs

We know the day you connected to a specific VPN location and from which Internet Service Provider. This bare minimum set of data is required to help you with technical assistance, solving connecting problems, and overcoming region-specific problems.

Details NOT Included In VPN Connection Logs:

- Your origin IP
- Your VPN IP
- The specific time when you connected to our server
- Your activities after connecting to our server

Total Bandwidth Consumed

Every paid PureVPN user gets access to unlimited bandwidth, irrespective of how that bandwidth is used. We keep track of the total bandwidth consumed by you to make sure every PureVPN user gets the same highest level of speed and experience with PureVPN. If we suspect abuse of our service by any user where the user is found consuming an unnatural amount of bandwidth and disrupting the service for other users, then we reserve the right to contact that user and ask them to explain their conduct.

V. SOFTWARE ANALYTICS, STATS & DIAGNOSTICS

PureVPN collects minimal connection statistics and reports. The collection is done to ensure superior quality of service and customer support. However, the data collected as statistics and reports does not and will never include uniquely identifiable user data or behavior, such as traffic details, IP addresses, and DNS requests.

We conduct VPN diagnostics and monitor crash reports to better understand the functionality of our software, how often you use the application, the events that occur within the application, aggregated usage, performance data, failed connection attempts, and provision of uncapped speed to ensure smooth functioning of our apps, extensions, and other client software.

We employ a few tools in our client software for this purpose, the details of which are:

Google Analytics - Please visit Google's Terms [here](#).

iTunes - Please visit the Privacy Policy [here](#).

Crashlytics - Please visit the Privacy Policy [here](#).

Apptentive - Please visit the Privacy Policy [here](#).

Firebase - Please visit the Privacy Policy [here](#).

New Relic - Please visit the Privacy Policy [here](#).

MixPanel - Please visit the Privacy Policy [here](#).

Facebook Pixel - Please visit Facebook's Privacy Policy [here](#). You can stop the use of your data for the purpose of displaying Facebook ads by clicking [here](#).

To ensure compatibility with our terms and conditions, its the responsibility of the customers to keep their apps updated at all times. To facilitate that, we've simplified the upgrade process and do our best to notify the users about upgrades whenever possible.

VI. DATA FROM EMAILS, LIVE CHATS, AND FEEDBACK FORMS

It is necessary for us to keep the record of your correspondence with us to ensure smooth delivery of service and superior customer service. So, we keep a record of your correspondence with us, whether they are questions, complaints, or compliments submitted by you via our apps, website, or extensions.

We use various third-party platforms for support and correspondence: Zendesk for support tickets, LiveChat inc. to provide support via chat, Mailchimp, and SendGrid for emails, and MixPanel to maintain a relationship with our users. When you correspond with us using these platforms, your correspondence records, including your name and email address, are stored in their systems. All these platforms utilize modern security practices and HTTPS encryption.

Please visit the Privacy Policy of Zendesk [here](#) to know more about their data practices.

Please visit the Privacy Policy of LiveChat [here](#) to know more about their data practices.

Please visit the Privacy Policy of Mailchimp [here](#) to know more about their data practices.

Please visit the Privacy Policy of SendGrid [here](#) to know more about their data practices.

Please visit the Privacy Policy of MixPanel [here](#) to know more about their data practices.

VII. INTERNATIONAL DATA TRANSFERS

Our service is spread globally, and as such, your data travels through our global servers, which might not or might be outside of your country of residence. We rely on some third-party service providers to enable us to provide you our services. Whenever we transfer your information, we take steps to protect it. We have strict data protection agreements in place with third parties to protect the data that we might share with them.

You acknowledge and understand that your information will be transferred, processed and stored as explained, as it is necessary to provide our services and live up to our [Terms of Service](#).

VIII. SECURITY MEASURES TO PROTECT YOUR INFORMATION

All PII, public and private keys and passwords are secured securely using strong cryptographic algorithms where necessary.

Appropriate security measures are taken for the protection of this information against unauthorized access, unauthorized alteration, destruction or disclosure of data. Access to personal information by PureVPN employees, contractors and agents is restricted. These officials require that information in order to operate, develop or improve our services but are bound by confidentiality obligations. They may be subjected to disciplinary action, which includes termination and criminal prosecution, upon failing to meet these obligations.

Please understand that we have taken even precautionary measure to ensure that your data remains protected, but there exists no system that can be declared 100% foolproof, protected and secure.

IX. DATA RETENTION POLICY & YOUR DATA PROTECTION RIGHTS

If you are a resident of the EEA, you have the following data protection rights:

- You can always access, correct and update the information you provided to us, within your member's area profile.
- You have the right to opt-out of marketing communications we send you at any time from within your member's area profile. You can also exercise this right by clicking on the "unsubscribe" or "opt-out" link in the marketing emails we send to you.
- You may also request deletion of your personal user profile, if you decide to leave our services completely. You can do so at any time by sending an email at support@purevpn.com. If you request the deletion of your profile, it may take up to a month (30 days) to complete. Your email address will be kept and used to avoid account duplication and creation of fake accounts in your name. Your email address will be deleted only after we receive an explicit request from you to do so.

X. APPLICABLE LAWS

PureVPN specifically chose Hong Kong (HK) for its headquarter because there are "No Mandatory Data Retention Laws" in Hong Kong. We are, therefore, not legally obliged to store user data and share it with anyone. Moreover, as stated above, we have no worthwhile data to share with any law enforcement agency from any particular country in the world. Even if and when we receive subpoenas that are legally upheld in the court of law in Hong Kong, we won't be of much help since we have almost nothing of value to share.

XI. COOKIES AND PUREVPN

PureVPN utilizes various types of cookies – small text files – to store information related to your visit on our website, to give you the best experience and to deliver advertising messages and offers that are relevant to you. Please refer to our [Cookie Policy](#) to get a better idea about the cookies we employ, what type of data is collected, how that data is used, and how you can opt-out of accepting these cookies.

XII. PUREVPN AND THIRD-PARTY WEBSITES

PureVPN's website might contain links to other third-party websites. Please know and understand that we do not control how they operate their privacy practices and we take no responsibility for them.

XIII. CONSENT AND AGE RESTRICTIONS

If you continue to use our website, apps, extensions or services, we will take it as your agreement to our Privacy Policy and our Terms of Usage.

The service provided by PureVPN is intended for people 18 years or older. If you think that your child has provided any information to use, then contact us immediately.

XIV. LEGAL BASIS

Our legal basis for collecting and using your personal information depends on:

- The personal information concerned
- The specific context in which we collect it.

The only time we collect personal information from you is (i) when we need the personal information to enter into a contract with you; (ii) where the processing is in our legitimate interests and does not violate your rights.

XV. IMPORTANT NOTE

PureVPN may change and amend its Privacy Policy at times. PureVPN holds the sole right to change and modify its Privacy Policy whenever it is felt necessary to do so. Whenever a revision is made, the updated revision date will be displayed at the top of this page. We encourage you to frequently check this page for any changes to stay informed. You acknowledge and agree that it is your responsibility to review this privacy policy periodically and be aware of the modifications. Since there is no other way for us to make sure about whether you are aware of the changes in the policy, we will take it as an agreement between you and PureVPN on the privacy policy if you continue to use PureVPN.

XVI. CONTACT INFORMATION

If anything mentioned in our Privacy Policy is unclear or you require more clarity on it, then send in your query at the following email address: legal@purevpn.com

* These features are neither offered via our iOS apps nor is this information collected via iOS apps

Last Updated on September 14, 2018