

VERSION 1.9 · 28 OCTOBER 2026

Colitu Security Whitepaper

Security architecture, threat model and privacy design

What you have to trust when you use Colitu, who can see what, which attacks Colitu protects against, which it does not, and how you can check our claims. Every statement describes what ships today. Where something is missing or weaker than it should be, we say so.

VERSION

1.9

LAST UPDATED

28 October 2026

SECURITY CONTACT

security@colitu.com

APPLIES TO

Android 2.9.9 · Windows 3.0.5 · Linux 1.6.2 (beta) · iOS 5.9.7 (TestFlight) · control plane as of 16 October 2026, node agent as of 7 October 2026

SOURCE

Android, Windows and Linux apps: github.com/colitu; iOS app: github.com/colitu/ios (all GPL-3.0). Server software: closed source.

o Colitu security at a glance

A summary of the sections below. Green: works as described on every platform named. Yellow: partly, or with documented limits. Red: not available yet.

Open-source apps	● Android, iOS, Windows and Linux are open source (GPL-3.0). The server software is closed.
Encrypted tunnel	● Hysteria2, VLESS Reality, VLESS XHTTP, Trojan and Shadowsocks 2022, using established implementations (Xray-core, sing-box, Hysteria).
Traffic content and browsing history	● Not recorded. The VPN servers keep no per-connection logs.
Per-user traffic volume	● Recorded per server in roughly 15-second windows and kept 90 days for quotas, then only period totals.
DNS through the tunnel	● Yes in the Android and iOS apps and in TUN mode. Not for apps outside the proxy in system proxy mode (the Linux default; new Windows installs start in TUN mode).
IPv6 leak protection	● Blocked on Android and iOS, and on Windows and Linux in TUN mode with the kill switch on. Not covered in system proxy mode.
Kill switch	● Windows: its own service with persistent firewall rules; Linux (TUN mode): nftables rules; both keep blocking if the app crashes. Android relies on the system's Always-on VPN setting; iOS has an optional "Block internet without VPN" switch (off by default).
Regional sites routed outside the VPN	● Off by default for new installations (privacy mode is on) since Windows and Android 2.7.0, iOS 5.6.0 and Linux 1.3.0; installations from before keep their previous setting. When privacy mode is turned off, sites on a built-in list go outside the VPN in all four apps, except when you are connected to a server in that region. Disclosed in §9 .
Two-step verification for users	● Optional for every account (set up on the website); all four apps ask for the code at sign-in. Mandatory for admin accounts.

Passkeys and session control	<ul style="list-style-type: none"> Passkeys for the website (up to 10 per account); the security page lists and ends browser sessions; changing the password ends all other sessions. The apps sign in with the password as before.
Pinned API connection in the apps	<ul style="list-style-type: none"> Since the app releases of 10 October 2026 all four apps pin the Let's Encrypt (ISRG) and Google Trust Services root certificate authorities for the API. Limits: §12.
Split tunnelling	<ul style="list-style-type: none"> Apps, sites and IP addresses on Windows, Android and Linux (apps in TUN mode only on Windows and Linux); sites and IP addresses on iOS, which allows per-app VPN only for managed profiles.
Colitu Shield (DNS protection)	<ul style="list-style-type: none"> Optional. Blocks ad, tracker, malware, phishing, scam and cryptomining domains (about 380 thousand rules). No query log and no statistics on its resolvers.
Third-party analytics	<ul style="list-style-type: none"> None in any app (Android, iOS, Windows, Linux). Removed from the iOS app in version 5.4.1.
Signed updates	<ul style="list-style-type: none"> Signed update manifest (ECDSA P-256) plus SHA-256 on Android, Windows and Linux; App Store signing on iOS.
Windows code signing (Authenticode)	<ul style="list-style-type: none"> Not yet.
Reproducible builds	<ul style="list-style-type: none"> Android from 2.9.3 and Windows from 2.9.8: the tagged source builds a byte-identical file. iOS and Linux not yet.
SBOM	<ul style="list-style-type: none"> SPDX for every Android and Windows GitHub release; Linux not yet.
Independent security audit	<ul style="list-style-type: none"> Not yet completed.
Vulnerability disclosure	<ul style="list-style-type: none"> security@colitu.com, policy in §18 and security.txt.
Self-hosting	<ul style="list-style-type: none"> Not offered. Colitu runs every server itself.

1 Executive summary

Colitu is a VPN service with apps for Android, Windows, Linux and iOS. It is built for untrusted or unreliable networks: each server offers several transports, and the apps pick one that works on the user's network.

The design goal is to keep the amount of sensitive data in any single place small. Accounts and payments live on a control plane that never carries VPN traffic. VPN servers carry traffic but hold no e-mail addresses or payment data. The apps store their credentials with each platform's secure storage.

This document describes the architecture, the threat model, the protocols, how keys and accounts are handled, what is logged, how updates are protected, the known limitations and the work still to do. It is written for readers who want to check our claims rather than take them on trust.

Principles

- Collect as little as possible, and say exactly what we do collect.
- Encrypt traffic between the app and the VPN server with established protocols. Colitu has no cryptography of its own.
- Keep accounts and payments apart from the servers that carry traffic.
- Prefer documented limitations to broad promises.
- Make the apps' behaviour checkable: publish the source of the Android, Windows, Linux and iOS apps.

A VPN does not make you anonymous. It moves trust from your local network and internet provider to the VPN operator. This document explains what that trust covers.

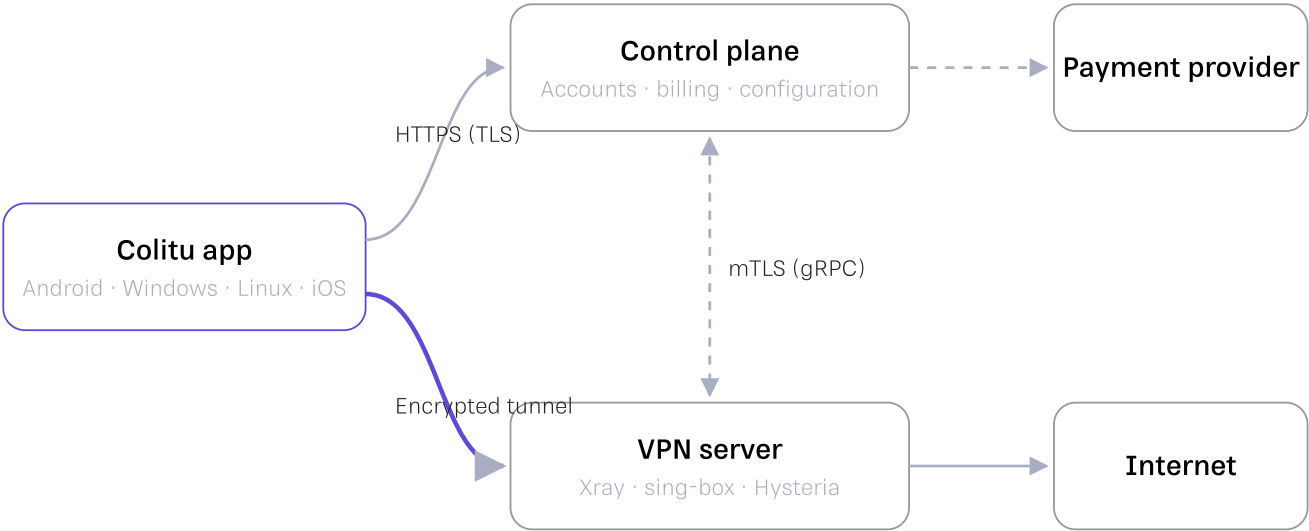
2 Scope

Covered: the Colitu apps for Android, Windows, Linux and iOS; the control plane (account API, billing, configuration, admin panel); the VPN servers and the node agent that configures them; the Colitu Shield DNS servers; update delivery; colitu.com and its subdomains.

Not covered: the security of the user's operating system and device, browser extensions and other software on the device, the internal security of the payment provider and other third parties named in [§11](#), and websites the user visits.

3 Architecture

Colitu separates a control plane, which knows who the users are, from a data plane, which carries their traffic.



Control plane and data plane. The control plane never carries VPN traffic; VPN servers hold no e-mail or payment data.

Components

Component	Responsibilities	Holds
App	Sign-in, server choice, protocol selection and fallback, tunnel set-up, routing and DNS settings, kill switch where available, update checks.	Session tokens and the current connection settings (§12).
Control plane	Accounts, sign-in, subscriptions and payments, device registration, generating each server's configuration, admin panel, support.	Account and billing data (§10). Runs on one server; the database is not reachable from the internet.
Node agent	Runs on every VPN server. Fetches its configuration over mutually authenticated TLS, starts the VPN cores, reports per-user traffic counters and health.	That server's protocol keys and the connection credentials of users who use it, identified by an internal user ID. No e-mail addresses.

Component	Responsibilities	Holds
VPN server (data plane)	Terminates the encrypted tunnel and forwards traffic to the internet.	Nothing beyond the agent's data. No traffic or connection logs (§10).
Colitu Shield DNS	Optional DNS-over-HTTPS resolver (AdGuard Home) on three VPN servers, reachable from inside the tunnel, that blocks ad, tracker, malware, phishing, scam and cryptomining domains: about 380 thousand rules, lists refreshed every 24 hours. Upstream resolvers are Cloudflare and Quad9 over DoH, ECS off.	No query log, no statistics.

How a connection is made

1. The app signs in over HTTPS and receives short-lived tokens.
2. It asks the control plane for the list of servers and the connection settings for the chosen one.
3. It tries the transports in order and keeps the first one that passes a connectivity check.
4. Traffic then flows app → VPN server → internet. The control plane is not on that path.

4 Trust model

When you use Colitu you must trust:

- the Colitu app you installed, and the device and operating system it runs on;
- the VPN server you connect to, and the hosting provider that runs it (VPN servers are rented virtual machines without disk encryption, so the provider has technical access to them);
- Colitu's control plane and the people who operate it;
- the protocol implementations Colitu uses (Xray-core, sing-box, Hysteria) and the cryptographic libraries beneath them.

You do not need to trust your local network or internet provider with the contents or destinations of tunnelled traffic. They can still see:

- that you connect to a Colitu server, its IP address and port;
- when you are connected, and roughly how much data you send and receive;
- possibly that the traffic is VPN traffic, depending on the protocol and the network's inspection tools;
- traffic that the app deliberately sends outside the tunnel: some regional sites (§9), local network traffic, update checks and latency measurements.

You	Local network / ISP	VPN server	Website
	Sees your IP, the server's IP, timing and volume	Sees your IP, destinations and timing; not HTTPS content	Sees the VPN server's IP

Who sees what for traffic that goes through the tunnel.

5 Threat model

Colitu is designed to protect traffic from hostile or untrusted local networks, from internet providers reading or recording what you do, and from many kinds of network filtering. It is not designed to give anonymity against an adversary who can watch traffic entering and leaving the VPN at the same time.

Threat	Protected?	Explanation
Eavesdropping on public Wi-Fi	● Yes	Tunnelled traffic is encrypted between the app and the VPN server.
Internet provider reading traffic content or destinations	● Yes, for tunnelled traffic	Except traffic deliberately routed outside the tunnel (§9).
Internet provider noticing that a VPN is used	● Sometimes	Reality, XHTTP and Hysteria2 are designed to look like ordinary TLS or QUIC, but no transport is undetectable.
DNS leaks	● Mostly	Android, iOS and Windows TUN mode resolve through the tunnel. Windows proxy mode does not cover the system resolver.
IPv6 leaks	● Partly	See §9.
Leak when the tunnel drops	● Partly	Windows and Linux have a kill switch that keeps blocking if the app crashes (documented gaps below); Android needs the system setting; iOS has an optional "Block internet without VPN" switch that is off by default.

Threat	Protected?	Explanation
Man-in-the-middle on the account API	● Yes	TLS with system certificate validation; since the app releases of 10 October 2026 all four apps also pin the Let's Encrypt (ISRG) and Google Trust Services root certificate authorities, so a root certificate that someone installed on the device cannot be used to read API traffic.
Malicious or compromised VPN server	● No	A server sees your IP address and the destinations of your traffic, though not the content of HTTPS connections.
Compromised control plane	● Partly	An attacker would get account and billing data and could push configurations to servers. Traffic content is never there.
Stolen account password	● Partly	Rate limits slow guessing and you can sign out devices. Optional two-step verification (authenticator app) means a stolen password alone no longer signs in, but it is off until you turn it on. Passkeys are an alternative sign-in on the website; a password change ends all other sessions, and a password reset locks account deletion and turning off two-step verification for 24 hours.
Malware on your device	● No	Outside the scope of any VPN.
Browser fingerprinting, cookies, signed-in accounts	● No	A VPN changes your IP address, not your identity on websites.
Traffic correlation by a global observer	● No	Timing and volume can be matched between the tunnel and the internet.

Adversaries considered

Class	Example	Colitu's protection
A1 Local network attacker	Someone on the same café Wi-Fi	Strong for tunnelled traffic.
A2 Internet provider	The user's ISP or mobile operator	Strong for content and destinations; timing and volume remain visible.
A3 Censor	Network-wide filtering with DPI and active probing	Several transports and automatic fallback; no guarantee (\$14).
A4 Malicious VPN server or host	A compromised server or a hostile hosting provider	Limited: sees the same metadata as the server. Credentials are separate per server, so one server cannot be used to reach the others.
A5 Compromised control plane	An attacker with access to the panel	Limited: account data exposed; no traffic content or browsing history to take.
A6 Endpoint attacker	Malware on the user's device	None.
A7 Global passive adversary	An observer of both ends of the tunnel	None.

6 Protocols

Every server offers the same set of transports. Colitu does not invent cryptography: encryption, authentication and key exchange are provided by Xray-core, sing-box and Hysteria and the libraries they use.

Transport	How it works	Server authentication	Notes and limits
Hysteria2	QUIC (UDP) with TLS 1.3	Certificate issued to the server by Let's Encrypt (ACME)	Fast on lossy networks. Fails where UDP is blocked or throttled.

Transport	How it works	Server authentication	Notes and limits
VLESS Reality	TCP; Reality performs a TLS 1.3 handshake that imitates a real website, using X25519 keys	The server's Reality public key, delivered with the configuration	Built against DPI and active probing. Not a guarantee against blocking by IP.
VLESS XHTTP	Reality plus an HTTP-like stream	As Reality, with its own keys	For networks that cut long-lived TCP connections.
Trojan	TCP with TLS (version 1.2 or 1.3; the server does not yet enforce 1.3)	Same certificate as Hysteria2	TLS fallback where UDP is blocked.
Shadowsocks 2022	2022-blake3-aes-256-gcm (AEAD), transport depends on the platform. Android and iOS use Xray-core for every transport, including Hysteria2. Windows and Linux use Xray-core for VLESS, Trojan and Shadowsocks and sing-box for Hysteria2. On the servers, Xray runs VLESS, sing-box runs Trojan and Shadowsocks, and the official Hysteria server runs Hysteria2.	Pre-shared key	Light and fast. No forward secrecy: a keylogger could

Switching transports is automatic but not seamless: when the app moves to another transport the tunnel is torn down and rebuilt, which takes about a second or more.

7 Cryptography and key management

Purpose	Mechanism
App and website to the API	TLS 1.2/1.3 with system certificate validation. Since the app releases of 10 October 2026 the Windows, Android, Linux and iOS apps also pin the Let's Encrypt (ISRG) and Google Trust Services root keys for the API. The pins stop being enforced on 31 December 2027, so old app versions are never locked out.

Purpose	Mechanism
Password storage	Argon2id: 64 MiB memory, 3 passes, 2 lanes, 16-byte random salt, 32-byte hash. Passwords are never stored in plaintext.
Access tokens	JWT signed with HMAC-SHA256 from a rotating key ring, valid 15 minutes.
Refresh tokens	32 random bytes, stored only as a SHA-256 hash, valid 30 days, replaced on every use. Reusing an old token revokes the whole token family.
Control plane ↔ VPN servers	Mutual TLS 1.3 (gRPC). ECDSA P-256 certificate authority; server certificates last 30 days and renew automatically; revocation by fingerprint allow-list.
Reality keys	X25519 key pair per transport per server, generated on the control plane.
Server TLS certificates	Let's Encrypt, issued on each server; the private key stays on that server.
Secrets in the database	Payment, e-mail and AI provider credentials are encrypted with AES-256-GCM.
Update manifests	ECDSA P-256 signatures verified by the apps against an embedded public key.
Backups	Encrypted with age to a public key; making a backup needs only that key. The decryption key is kept offline, not on any server.
Abuse-check and migration fingerprints	HMAC-SHA256 under a key derived from the settings encryption key, which is not stored in the database.

Where keys live and what happens if one leaks

- The certificate authority's private key is a file on the control plane. Anyone who obtained it could issue server identities, so it is the most sensitive key we hold.
- Each VPN server holds its own Reality private keys, its TLS certificate key and the connection credentials of users who have used it. These credentials are random and different on every server, so a compromised server does not expose credentials valid on the others.

- Reality private keys and users' connection credentials are stored unencrypted in the control plane database. Database-level encryption of these values is on the roadmap.
- There is no scheduled rotation of Reality keys yet. If a server is suspected to be compromised it is removed from the apps and its keys and credentials are replaced.
- The control plane makes an encrypted backup every day and keeps it for 3 days. A copy goes to Backblaze B2 (EU Central, Amsterdam) with Object Lock: for 30 days nobody, Colitu included, can delete or change it, and it is deleted automatically after at most 36 days. The decryption key is kept offline since 16 October 2026, so neither the server nor Backblaze can read the backups. A restore from the off-site copy was tested on 16 October 2026. Database snapshots taken before a deployment are not encrypted and stay on the control plane server for at most 7 days.

8 Accounts and sessions

- Sign-in is with e-mail and password. A TV can sign in by showing a QR code that a signed-in phone approves (8-character code, valid 10 minutes). There is no sign-in through Google, Telegram or other third parties.
- Passwords must be at least 10 characters. A new account gets VPN access only after confirming a 6-digit code sent by e-mail.
- Password reset uses a 6-digit code valid 15 minutes, usable once, limited to 5 attempts. The answer is the same whether or not the address has an account. Resetting the password signs out every device and web session. After a reset by e-mail code, deleting the account and turning off two-step verification are locked for 24 hours (error RECOVERY_LOCKED).
- Sign-in, registration, password reset and promo codes are rate-limited per IP address. On the website, sign-in and reset are also limited per e-mail address; in the apps, sign-in is limited per IP only. There is no lockout for user accounts.
- Signing out revokes that device's refresh token. Its access token stays valid until it expires (at most 15 minutes).
- You can remove devices from your account page. The security page lists browser sessions with a device label (browser and operating system), country, sign-in method and IP address; you can close one session, close all others (the current one stays) or sign out everywhere.
- Changing the password on the website keeps the browser session you are in and ends all other web sessions and all app refresh tokens. App access tokens issued before the change stop working immediately (error AUTH_SESSION_REVOKED).
- Actions that ask for the password again (changing the password, deleting the account, two-step verification changes, passkeys) are limited to 10 attempts per 15 minutes per account.
- Two-step verification (TOTP) is optional for every account. You turn it on at colitu.com/account/security with an authenticator app and receive 10 one-time recovery codes; after that the apps ask for the code after the password (supported from Windows 2.6.0,

Android 2.6.0, Linux 1.2.0 and iOS 5.5.0; an older app asks you to update). It is set up on the

- **Passkeys only.** On colitu.com you can add up to 10 passkeys under Account → Security (password required), name each one and delete it with your password, and then use 'Sign in with a passkey' on the login page. A passkey with user verification counts as two factors, so it skips the two-step verification code; a sign-in from a country not seen in the last 90 days still asks for an e-mail code. Passkeys do not work on mirror domains. The apps sign in as before, or by approving a device-link QR code in a browser that is signed in with a passkey.
- Colitu sends a security e-mail for: a new app device (not for the first one), a sign-in from a new country (not seen in 90 days), two-step verification turned on or off, recovery codes regenerated, a passkey added or removed, and a password change.
- Subscription links: besides the main link you can create up to 5 extra named links, each with an optional expiry of 7, 30 or 90 days, and revoke them one by one. A warning appears when a link is used from many different networks in a short time. Colitu stores no IP addresses for this, only an anonymous per-day count of distinct networks, kept for 48 hours.

Connection credentials are issued per device (and per subscription link) and per server. Removing a device, or rotating a subscription link, deletes its credentials from every server: new connections from it are refused within about 15 seconds, and connections already open end when they close. A device paused because your plan allows fewer devices is left out the same way until you make it active again. If a device is lost, change your password as well.

Administrator access

Colitu is run by a very small team. The admin panel is on a separate address with role-based permissions, admin endpoints are closed on the public API, admin accounts lock for 15 minutes after 5 failed attempts, and admin actions are written to an audit log. Two-step verification (TOTP) is mandatory for admin accounts: an admin without it can only set it up after signing in, and every later sign-in needs the code or a one-time recovery code (attempts are rate limited). An admin can also register a hardware security key (WebAuthn); once one is registered, sign-in needs the password and the key instead of TOTP, and a one-time recovery code remains as a logged emergency fallback. A lost key is replaced with a recovery code or, after an out-of-band identity check, by a logged reset command on the server. Access is revoked by disabling the account, which takes effect on the next request. Admin sessions are bound to the browser and network they were opened from.

9 Traffic, DNS, IPv6 and kill switch

What the VPN server can see

A VPN server must know where to send your traffic, so it technically sees your IP address, the IP addresses and often the host names (TLS SNI) of the sites you connect to, and the timing and volume of your traffic. It cannot read the content of HTTPS connections, which stay encrypted between your device and the website. Colitu does not decrypt or inspect HTTPS traffic.

Routing defaults

	Android	Windows	iOS	Linux (beta)
How traffic is captured	System VPN (all apps)	TUN mode (all traffic) for new installs; installs that used system proxy mode keep it	System VPN (all apps)	System proxy by default; TUN mode optional
Not covered by default	Local network	In system proxy mode: apps that ignore the system proxy, the Windows DNS resolver, browser UDP (QUIC/WebRTC), IPv6. TUN mode covers them.	Local network	As Windows in system proxy mode
Regional sites and IPs (built-in list)	Outside the VPN only if privacy mode is off, unless the server is in that region	Outside the VPN only if privacy mode is off, unless the server is in that region	Outside the VPN only if privacy mode is off, unless the server is in that region	Outside the VPN only if privacy mode is off, unless the server is in that region
DNS	Through the tunnel to 1.1.1.1	TUN: through the tunnel to Cloudflare DNS-over-HTTPS. Proxy mode: only for traffic that reaches the proxy.	Through the tunnel (8.8.8.8 → Xray → 1.1.1.1)	As Windows

	Android	Windows	iOS	Linux (beta)
IPv6	● Blocked	● Blocked in TUN mode with the kill switch; not covered in system proxy mode	● Does not leak: routed into the tunnel and dropped there	● As Windows
Kill switch	● Uses Android's Always-on VPN and "Block connections without VPN" settings, which the user must turn on	● Own Windows service with persistent Windows Filtering Platform rules, on by default (see below)	● "Block internet without VPN" (iOS includeAllNetworks), off by default; Wi-Fi sign-in pages cannot open while it is on. "Always-on" only reconnects	● nftables rules that stay if the app crashes; TUN mode only
Split tunnelling	● Apps, sites and IP addresses	● Apps (TUN mode only), sites and IP addresses	● Sites and IP addresses only (iOS allows per-app VPN only for managed profiles)	● Apps (TUN mode only), sites and IP addresses
Multihop and rotating IP	● VLESS only	● VLESS only	● VLESS only	● VLESS only

Regional sites outside the VPN

Some regional sites (domains and IP ranges on a built-in list) open directly, outside the tunnel, so that services which refuse foreign IP addresses keep working. This does not apply when you are connected to a server in that region. For this traffic the site and your internet provider see your real IP address. The rule applies only when privacy mode is off. Privacy mode is on by default for new installations (Windows and Android 2.7.0, iOS 5.6.0, Linux 1.3.0 and later), so by default all traffic goes through the VPN; installations from before keep their previous setting. When the rule is active, the first time you connect the app shows a one-time notice that explains this. You can also choose a server in that region.

Windows kill switch in detail

- It blocks all IPv4 and IPv6 traffic except loopback, the local network (a setting, on by default), DHCP, the VPN cores, the TUN adapter and the Colitu app itself.
- It is active for the whole session, in TUN mode and in system proxy mode. In proxy mode, apps that do not use the proxy have no internet while you are connected.
- The rules are held by a separate Windows service (ColituKillSwitch, LocalSystem, automatic start) as persistent Windows Filtering Platform rules. If the app or the VPN core crashes, or the service restarts, the rules stay in place and the internet stays blocked until Colitu reconnects (fail-closed).
- A normal Windows restart or shutdown ends the block. This is deliberate: nobody would be there to explain why the internet is blocked. The exception is when Auto-connect and start with Windows are both on; then the block stays until Colitu has reconnected. Pressing Disconnect ends the block, and uninstalling removes all rules.
- If the service is missing (for example after a damaged installation), the app warns you and falls back to the older in-app kill switch. Its filters belong to the app's process: if the app crashes or is killed, Windows removes them and traffic flows (fail-open).
- Traffic that the app routes directly, such as regional sites on the built-in list, is not blocked by design.

Traffic the apps send outside the tunnel

- Update checks and update downloads (colitu.com).
- Latency measurements to the servers.
- On Windows, resolving the servers' host names through Cloudflare or Google DNS-over-HTTPS.

Connectivity checks (for example Google's generate_204 address) are sent through the tunnel.

10 Logging and data inventory

This is the complete list of what Colitu stores. The privacy policy contains the same list in legal form.

VPN service

Data	Stored?	Retention and purpose
Content of your traffic	<div><div></div></div> Never	—

Data	Stored?	Retention and purpose
Sites and IP addresses you visit	● Not stored	Not recorded.
Your DNS queries	● Not stored	Colitu Shield's resolvers have query logging and statistics turned off. By default the apps use public resolvers (Cloudflare, Google), which receive queries from the VPN server's IP address, not yours.
Your IP address on the VPN servers	● Not stored	Used in memory for the connection only.
Traffic volume per user	● Stored	Bytes per user per server in windows of about 15 seconds, kept 90 days for quotas and fair use; afterwards only totals per billing period. This shows when an account was active and how much it used, but not where it went.

Account and website

Passkeys, web sessions and subscription links are included in the table below. For subscription links no IP addresses are stored: only an anonymous per-day count of distinct networks per link is kept, for 48 hours.

Data	Retention	Purpose
E-mail address, password hash (Argon2id), language, account dates	Until the account is deleted; deletion replaces the address with a placeholder and makes the password unusable	Account and sign-in
E-mail verification and password reset codes (address, hashed code, IP address)	7 days	Verifying the e-mail address, password reset
Sign-in events (IP address, country, browser or app)	180 days	Account security, abuse prevention

Data	Retention	Purpose
IP address and country at registration and at the last sign-in	Registration: 180 days. Last sign-in: erased after 180 days without a sign-in	Account security, regional rules
Sign-ups and sign-ins refused under regional rules (IP address, country)	90 days	Enforcing regional rules
Web sessions (IP address, country, browser, sign-in method)	Deleted 30 days after the session ends (sign-out, expiry or revocation)	Signing in, sessions list on the account page
App sign-in tokens (stored only as hashes, tied to a device)	Deleted 30 days after they expire or are revoked	Keeping the apps signed in
Two-step verification (encrypted authenticator secret, hashes of single-use recovery codes, 5-minute sign-in steps)	Secret and recovery codes until you turn it off or the account is deleted; sign-in steps are deleted 1 day after they expire	Account security
Passkeys (public key, credential ID, the name you give it, signature counter, creation and last-use dates; the private key and any biometric data never leave your device; 5-minute single-use verification challenges)	Until you remove the passkey or the account is deleted; verification challenges expire and are deleted after 5 minutes	Password-free sign-in and account security
VPN connection credentials (random secrets per server, tied to a device or a subscription link)	While the device or link is in use; deleted 30 days after it is removed or replaced	VPN access

Data	Retention	Purpose
Subscription links (the name you give, creation, last-use and expiry dates, a "may be shared" flag; the link itself is stored only as a hash). The IP addresses that use a link are not stored; only a daily, anonymous, approximate count of how many different networks used each link is kept for 48 hours	Until you revoke the link or delete the account (an expired link is revoked automatically); the network count deletes itself after 48 hours	One link per device and the shared-link warning
TV sign-in requests (device name, IP address, country)	Deleted 1 day after the 10-minute code expires	QR sign-in
Devices (name, platform, app and OS version, last IP address and country, keyed hash of a hardware identifier)	Kept while the device is on the account. A removed device's name, IP address, country and hardware hash are erased after 30 days; the IP address and country of a device not seen for 180 days are erased	Device limits, account security
Refused device and trial attempts (IP address, device details)	180 days	Device limits, abuse prevention
Free plan and trial abuse checks (HMAC-SHA256 keyed hashes of the e-mail address, hardware ID and network; the key is not stored in the database)	Network: 30 days. E-mail and hardware ID: while the account exists and for 180 days after it is deleted. Unkeyed SHA-256 hashes written before this change are deleted at the latest 180 days after they were written	Preventing repeated free accounts

Data	Retention	Purpose
Automatic bot and abuse screening: for held or blocked accounts the score, the signals that triggered it, IP address, country, network (ASN) and user agent; for sign-ups refused before an account existed also the e-mail address	Held or blocked accounts: while the account exists, deleted with it. Refused sign-ups: 30 days	Preventing bots, scripted sign-ups and the harvesting of server addresses
Trial promo code abuse checks (HMAC-SHA256 keyed hashes of the normalised e-mail address, the device hardware ID and the network – IPv4 /32 and /24 or IPv6 /64 and /48; the key is not stored in the database)	Network: 35 days. E-mail and hardware ID: 365 days, also after the account is deleted	One trial code per person
Migration requests from the previous service (Telegram ID and name, notes, IP address)	Deleted 30 days after the last change. Of an approved request only a keyed hash of the Telegram ID remains, for 2 years	Moving old subscriptions; preventing the same subscription from being moved twice
A signup source label (e.g. "github", "app:android") from the utm/ref tag of the site's entry link, the name of the site that sent you (e.g. github.com) or the app; no cookie, tracking pixel or URL is stored. The time of the first VPN connection.	Deleted with the account	Measuring, in aggregate, which channels bring real users and how long the first connection takes
Your invite code; the link between an account opened with an invite link and the inviting account, the invite's status (pending, earned, not valid and why) and the Premium days granted. The inviter is never shown the invitee's name or e-mail.	Deleted when either account is deleted	Granting invite rewards; preventing abuse (same IP address or device, throwaway e-mail); measuring invite signups in aggregate

Data	Retention	Purpose
<p>The apps' anonymous usage statistics: connection results and the kind of failure, connect and recovery times (as range counts), unexpected disconnects, Adaptive Connect's protocol switches, latencies measured to servers and automatic mode's server choice, features used and the kill-switch state; the network type and the country and internet-provider number (ASN) of the network in use (from a signed label received while the VPN is off). The server keeps only totals per day, with networks (country + ASN) and servers in separate tables; no account, device, IP address or visited site is stored. Can be turned off in the app settings.</p>	<p>Totals kept indefinitely (not linkable to a person)</p>	<p>Measuring and improving connection quality, Adaptive Connect and feature use</p>
<p>Colitu Passport is saved to your account and follows you to every device you sign in on. Per stamp country: unlock time and pieces; achievements, collections, weekly expedition progress, nickname, title, cover, time-zone offset and collector number; day totals (minutes of use, pieces, night and early-morning minutes, and the list of countries used that day); the current run (country, its length and the last counted minute); reward events for the apps' reveal animations. Our servers count the minutes from connection time: a minute counts when one of our servers reports traffic for your account in that minute (each minute at most once, whatever the number of devices), and the country is the server's country; apps cannot add minutes. Only totals per day and per country are stored; there is no per-minute or per-session log, and no sites or IP addresses. Progress already on a device from the old version is imported once per device (capped to what is plausible, the higher value wins).</p>	<p>Day totals 400 days, reward events 30 days, the rest until the account is deleted</p>	<p>Saving the passport to your account, showing it on every device and working out rewards and weekly expeditions</p>

Data	Retention	Purpose
Colitu Passport's optional anonymous counters, at most one report a day: number of stamps opened, highest open chapter, stamps per level, finished weekly expeditions, pieces earned that day and whether the passport was opened that day. Sent without authentication; the server only adds each report to per-day totals and stores no report row, account, device or IP address. Which countries the stamps came from, and when, is not sent. Only older app versions send it; new versions do not, because the passport is now kept on your account (see the "Colitu Passport" row). The setting starts off and can be turned off in the app.	Totals kept indefinitely (not linkable to a person)	Seeing in aggregate how much the passport is used and whether its rules are balanced (level and piece pace)
Your answers to in-app surveys: recommendation score (0–10), how you would feel without Colitu, why you did not renew Premium, an optional comment and the platform; surveys you closed (at most one survey in 30 days)	When the account is deleted the link to it and the comment are removed; only the anonymous score remains	Measuring satisfaction (NPS), product–market fit and reasons for leaving in aggregate
The 1–5 rating and optional comment you give a resolved support conversation; when it was first answered and resolved	Deleted with the support conversation	Measuring support quality (satisfaction, response and resolution time) in aggregate
Which transports worked for a device on which server, and how fast (no IP address)	Overwritten with each report; deleted 35 days after the last report	Trying working transports first
Plan, payments and orders (amount, payment method type, provider transaction ID, the provider's notification; for Rialit payments, a fixed payer number tied to the account)	As long as accounting and tax law requires, also after the account is deleted; automatic deletion at the end of that period is not implemented yet	Billing, refunds, legal obligations

Data	Retention	Purpose
Colitu Business company account: company name, billing e-mail, country, tax number, number of seats and their term; membership (role, invitation, joining and leaving dates, who added the member); company invoices and the company activity log. The company's owner and admins see each member's e-mail address and role and their devices' name, platform, app version and last-seen time; they cannot see traffic or visited sites	Until Colitu closes the company account; company invoices as long as accounting and tax law requires; password set-up links are valid for 7 days. When a member deletes their account, the membership is closed and the seat returns to the company	Managing company seats, company billing, renewal reminders
Businesses and content creators we send Colitu Business partnership offers to: company or channel name, the e-mail address they publish for business contact on their website or channel description, country and language; the mails we sent and when; the subject and first 300 characters of replies, and bounces	Sending and reply records in the panel are deleted after 12 months. The contact list is kept until the contact asks us to stop or the address is no longer needed; an address that replies "don't write to me" is never mailed again	Offering Colitu Business reseller and white-label partnerships (legitimate interest; every mail says how to object and links this policy)
Support conversations and attachments, including app logs the app attaches (addresses, site names and secrets masked)	Closed conversations: deleted 2 years after the last message	Support, handling complaints
Security reports: the text of the vulnerability you report (title, description, steps, impact) and the messages with the team; if you ask to be credited in the Hall of Fame, the name you choose (published publicly with the month and severity)	Until the account is deleted; deletion removes the reports, the messages and the Hall of Fame entry	Fixing vulnerabilities and paying rewards (optionally: crediting you in the Hall of Fame)
An automatic job applies these periods every hour, and deleting an account erases at once what the privacy policy lists. Remaining gaps: plan, payment and order records and the audit log have no automatic deletion yet, and encrypted backups made before a deletion keep the data for at most 36 days, and unencrypted snapshots taken before a deployment for at most 7 days. Abuse-check hashes are keyed with a server secret; unkeyed SHA-256 hashes written before this change remain matchable until they are deleted. at the latest		

180 days after they were written.

Connection report: when support looks into a connection problem, your app sends app and device details, connection events and app logs the next time it opens; site names and addresses are masked on the device and on the server, the sites you visit are not sent	Deleted after 90 days	Fixing connection problems (support)
Colitu Bot conversations (text, IP address, "was this helpful" feedback)	180 days	Answering questions
E-mail delivery records (recipient address, type of e-mail)	90 days	Solving delivery problems
Newsletter subscription (e-mail address, language, time of confirmation); only if you confirm through the link in the e-mail	Until you unsubscribe; unconfirmed sign-ups are deleted after 7 days	Announcement, release-note and offer e-mails (with your consent)
Website and API access logs (IP address, address requested, browser)	14 days	Operating and protecting the Service
DNS leak test on our website	10 minutes, in memory only	Showing the test result
Audit log (admin actions, and some account actions such as deleting the account, by account ID)	Indefinitely; the optional reason you give when deleting your account: 180 days	Accountability for actions

11 Telemetry and third parties

Telemetry in the apps

- No Colitu app (Android, iOS, Windows, Linux) contains analytics, advertising or crash-reporting libraries; the iOS app has had none since version 5.4.1.

- All apps report to Colitu which transports worked on which server and how fast, tied to the device, so that working transports can be chosen first.
- Support requests attach recent app logs, with addresses and secrets masked.

Third parties that receive data

Party	What it receives
A payment provider (only for customers who bought a paid plan)	Order number, amount, currency, plan description and payment method; card or bank details are entered on the provider's page. Colitu does not send your e-mail or IP address.
Resend (e-mail)	Your e-mail address and the content of account e-mails (codes, receipts).
Brevo (e-mail relay)	Replies sent from our support mailbox.
DeepSeek (Colitu Bot)	The question and the last few messages of a bot conversation. No account details are sent, but anything you type is passed on.
Have I Been Pwned (Pwned Passwords)	When you sign up or set a new password: the first 5 characters of the password's SHA-1 hash, to check it against known breaches. Never the password, its full hash, your e-mail or IP address.
Cloudflare	Hosts DNS records and proxies docs.colitu.com and map.colitu.com. It also provides the default DNS resolvers in the apps and the egress for a few domains on two servers (\$17).
Backblaze B2 (EU Central, Amsterdam)	Encrypted copies of the daily backup. It cannot read them: the decryption key is kept offline.
Hosting providers	Run the servers and have technical access to them.

The website loads no third-party scripts, fonts or trackers.

12 App security

	Android	Windows	iOS	Linux (beta)
Session tokens	AES-256-GCM with an Android Keystore key (software key if the Keystore fails)	DPAPI (current user)	Keychain (available after first unlock)	AES-GCM with a key derived from the machine and user
Connection credentials	Encrypted (AES-GCM)	Plaintext in a database readable only by administrators and SYSTEM	Plaintext file in the app's private container	Protected files (0600)
Certificate pinning for the API	● Yes	● Yes (since 10 October 2026)	● Yes (since 10 October 2026)	● Yes (since 10 October 2026)
Privileges	Normal app with the VPN permission	Always runs as administrator; a separate background service (ColituKillSwitch, LocalSystem) holds the kill-switch rules	Network extension	Asks for sudo; password kept in memory
Local VPN logs	Warnings only; no access log	Warnings only; addresses masked; deleted after 7 days	Warnings only; no access log	Warnings only
Backups of app data	Disabled	—	Keychain items stay on the device	—

Pinning means that a root certificate installed on the device by someone else cannot be used to read the apps' API traffic. Security software that inspects HTTPS by inserting its own root certificate will therefore block the apps' API connection; exclude Colitu in such software.

13 Updates and supply chain

Platform	How an update is verified
Android (download version)	The manifest is signed with ECDSA P-256 and checked against a key built into the app. The APK must come over HTTPS from colitu.com, match the SHA-256 in the manifest, and be signed with the same certificate as the installed app. Older versions are refused.
Android (Google Play)	Updated through Google Play.
Windows	Same signed manifest, HTTPS download from colitu.com, SHA-256 check, checked again by the elevated installer step. The installer is not yet Authenticode-signed, so Windows SmartScreen may warn.
Linux	Signed manifest and SHA-256 of the package.
iOS	Distributed through Apple TestFlight; Apple signs and delivers updates.

Build and source

- Every release of the open-source apps is tagged on GitHub. The release page lists SHA-256 checksums and an SPDX software bill of materials (Android and Windows).
- CodeQL code scanning and Dependabot dependency updates run on the Android and Windows repositories; GitHub Actions are pinned to commit hashes.
- The Android release is built in CI; the Windows installer is built on the developer's machine; Linux packages are built in CI; iOS TestFlight builds are made on Codemagic.
- Android (from 2.9.3) and Windows (from 2.9.8) builds are reproducible, so anyone can rebuild the tagged source and compare the result with the published file. On iOS and Linux a checksum still only proves that you have the file we published, not that it was built from the tagged source. The Android Xray core library is the official upstream binary pinned by SHA-256, not rebuilt from source.

What is open and what is closed

Component	Source
Android app	● Open (GPL-3.0)
Windows app	● Open (GPL-3.0)
Linux app	● Open (GPL-3.0)
iOS app	● Open (GPL-3.0)
Control plane and node agent	● Closed
Website	● Closed

14 Censorship resistance

No transport can be guaranteed to keep working against every censorship system. Colitu's approach is to offer several transports with different properties and let the app fall back automatically.

Blocking technique	How Colitu responds
Blocking server IP addresses	Several servers in different networks, plus a relay (§17). A blocked IP stays blocked until the server changes.
Blocking ports or UDP	TCP transports (Reality, XHTTP, Trojan) when UDP is blocked; Hysteria2 when TCP is disrupted.
DNS poisoning	The apps receive server addresses from the API and resolve them over encrypted DNS where needed.
TLS fingerprinting and active probing	Reality answers probes as the real website it imitates.
Protocol fingerprinting (DPI)	Reality and XHTTP resemble ordinary HTTPS; Hysteria2 resembles QUIC.
Throttling and connection resets	Automatic fallback to another transport; XHTTP for networks that cut long connections.

15 Privacy limitations

A VPN hides your traffic from the network you are on. It cannot hide everything:

- Packet sizes, timing and total volume remain visible and can be matched by an observer who sees both ends.
- Websites can still identify you through cookies, browser fingerprinting and accounts you are signed in to.
- A VPN does not protect against malware, phishing or a compromised browser.
- Traffic routed outside the tunnel (§9) is not protected.

16 Incident response and incident log

If we suspect a VPN server is compromised, we hide it from the apps, replace its keys and connection credentials, and rebuild it. If a breach affects personal data, we e-mail affected users without undue delay and publish what happened in this section and on the Trust Centre. Service status is public at status.colitu.com.

17 Infrastructure

- All servers are rented virtual machines from several independent hosting providers. The VPN servers are spread over a number of countries; the live list is on the servers page. The control plane, which holds the account database, runs on a server in Turkey.
- Disks are not encrypted. Hosting providers have technical access to their machines.
- Administrative access is by SSH with keys only; password sign-in is disabled. Only the Colitu team holds the keys.
- Automatic security updates are enabled on most servers; enabling them everywhere is on the roadmap.
- The control plane and some VPN servers use a default-deny firewall. On the other VPN servers only the VPN services, SSH and the measurement endpoint listen; a default-deny firewall everywhere is on the roadmap.
- The control plane database is not reachable from the internet. VPN servers have no access to it.
- Two servers send a small, fixed set of domains (Google services on one, Google's AI services on the other) through Cloudflare WARP so that these services see a European location. For those domains Cloudflare is the exit and sees the same metadata as a VPN server would.
- One relay entry server forwards encrypted packets unchanged to an exit server in Latvia. The entry server cannot decrypt the traffic; it sees your IP address as any network would.

18 Vulnerability disclosure

Report security issues privately to security@colitu.com (also listed in </.well-known/security.txt>). Please include steps to reproduce and the affected version. The full policy is at colitu.com/responsible-disclosure.

- We acknowledge reports within 3 working days and give an initial assessment within 10 working days.
- Please give us reasonable time to fix the issue before publishing details.
- We will not take legal action against research done in good faith that avoids other users' data, does not disrupt the service and is reported privately.
- We credit researchers who want to be credited. Through the bug bounty programme (colitu.com/bug-bounty), confirmed reports sent from your account are rewarded with 1 to 12 months of Plus depending on severity, and critical issues with a cash reward.
- In scope: the apps, colitu.com and its subdomains, the API and the VPN servers. Out of scope: denial of service, spam, social engineering and the third parties in §11.

19 Audit status

Colitu has not yet had an independent third-party security audit or penetration test. Current assurance consists of:

- public source code for the Android, Windows, Linux and iOS apps;
- automated code scanning (CodeQL) and dependency updates (Dependabot);
- internal security reviews of the apps (October 2026) and the verification behind this document;
- a public vulnerability disclosure process.

An independent audit is planned but not yet scheduled.

20 Known limitations

- No independent security audit yet.
- VPN servers and their hosting providers are part of what you must trust; server disks are not encrypted.
- Some regional sites on a built-in list go outside the VPN in the Windows, Android, iOS and Linux apps when privacy mode is turned off. Privacy mode is on by default for new installations since Windows and Android 2.7.0, iOS 5.6.0 and Linux 1.3.0, but installations from before keep their previous setting.
- New Windows installs start in TUN mode, but installs that used system proxy mode keep it, and proxy mode does not cover every app, the system DNS resolver or IPv6. A normal Windows restart ends the kill-switch block unless Colitu is set to reconnect at sign-in.

- Android has no kill switch of its own and needs two system settings that are off by default; the iOS "Block internet without VPN" switch is off by default and stops Wi-Fi sign-in pages from opening while it is on.
- Two-step verification is mandatory for admin accounts but only optional for users.
- Billing records and the audit log have no automatic deletion yet (§10).
- Security software that inspects HTTPS with its own root certificate blocks the apps' API connection because of certificate pinning; Colitu has to be excluded in it. Passkeys work on colitu.com only: not on mirror domains and not inside the apps.
- The Windows app is not Authenticode-signed, and iOS and Linux builds are not reproducible yet.
- Shadowsocks 2022 has no forward secrecy; Trojan accepts TLS 1.2.

21 Changes in 1.4 to 1.9

Version 1.3 described the apps as they were before the latest app releases. This version describes what ships today.

- Two-step verification (TOTP) is available to every user account, not only to administrators. The apps ask for the code at sign-in.
- Windows: the kill switch is now a separate Windows service with persistent firewall rules. It keeps blocking if the app or the VPN core crashes (it no longer fails open). A normal Windows restart still ends the block, unless Colitu is set to reconnect at sign-in. New installs start in TUN mode.
- Split tunnelling exists in all four apps: apps, sites and IP addresses on Windows, Android and Linux; sites and IP addresses on iOS.
- iOS: IPv6 no longer leaks, and an optional "Block internet without VPN" switch (off by default) blocks traffic outside the tunnel.
- Privacy mode (on by default for new installations) lets users of the Windows, Android, iOS and Linux apps decide whether the built-in rule that sends some regional sites outside the VPN is active.
- Multihop (double VPN) and rotating IP are available with VLESS servers.
- The ad blocker became Colitu Shield, optional DNS protection with five categories (ads and trackers, malware, phishing, scams, cryptomining) since 7 October 2026. Its resolvers keep no query log and no statistics, and no new data is collected. An optional adult-content filter, personal lists, an on-device counter and per-category switches are on the roadmap, not live.
- Versions, dates and checksums in this document, on the download pages and on the open-source page now come from one release manifest.
- Version 1.5 (9 October 2026): paid plans (Personal, Plus and Family) are on sale; payments are made on a payment provider's page and card details never reach Colitu. The statement that

paid plans were not offered has been removed. No other practice described in this document changed.

- Version 1.6 (10 October 2026): passkeys for the website, a session list with session controls, security e-mails, a 24-hour lock on account deletion and turning off two-step verification after a password reset, a limit on password re-verification attempts, extra named subscription links with expiry, optional hardware security keys for admin accounts, and pinning of the API connection to the Let's Encrypt (ISRG) and Google Trust Services root certificate authorities in all four apps. No other practice described in this document changed.
- Version 1.7 (16 October 2026): backups. The decryption key moved offline and is no longer stored on the server. A daily encrypted copy is kept off-site at Backblaze B2 (EU Central) with a 30-day deletion lock and is deleted after at most 36 days. Unencrypted snapshots taken before a deployment are deleted after 7 days. Backblaze was added to the list of third parties. No other practice described in this document changed.
- Version 1.8 (20 October 2026): reproducible builds for Android (from 2.9.3) and Windows (from 2.9.8). No other practice described in this document changed.
- Version 1.9 (28 October 2026): the bug bounty programme (1 to 12 months of Plus, a cash reward for critical issues) is described here, and the statement that no paid bounties were offered has been removed. The internal security assessment report is published at colitu.com/security-assessment. No other practice described in this document changed.

22 Security roadmap

Next (Q4 2026)

- Automatic deletion of billing records once the legal retention period ends.
- Shorter website access logs without full IP addresses.
- Default-deny firewall and automatic security updates on every server.
- Enforce TLS 1.3 for Trojan.

Later

- Authenticode signing for Windows.
- Reproducible builds for iOS and Linux, and an SBOM for every platform.
- An external penetration test and an independent audit.
- A PGP key for security reports and quarterly transparency reports.

23 Jurisdiction

Colitu is operated by COLITU LIMITED, a company registered in England and Wales (registered office: 128 City Road, London, United Kingdom, EC1V 2NX; company number 17520342), and is

subject to the law of England and Wales. The account database is on a server in Turkey; VPN servers are in the countries shown on the servers page and are subject to local law where they are. We can only hand over data we have; §10 lists all of it. Requests we receive are counted in the transparency reports on the Trust Centre.

24 References

- Hysteria 2 protocol: v2.hysteria.network
- Xray-core and REALITY: github.com/XTLS
- sing-box: sing-box.sagernet.org
- TLS 1.3: RFC 8446 · QUIC: RFC 9000 · security.txt: RFC 9116
- Argon2: RFC 9106
- OWASP ASVS and MASVS
- Android VpnService, Apple Network Extension and Windows Filtering Platform documentation

Colitu Security Whitepaper · Version 1.9 · 28 October 2026 · security@colitu.com · colitu.com/security