IPRoyal

IPRoyal Know-Your-Customer Practices

Learn about our step-by-step approach to KYC (Know Your Customer) practices, and see how it helps us maintain a secure, trustworthy, and reliable infrastructure to help your business.

Executive Summary

At IPRoyal, our Know Your Customer (KYC) practices are in place to keep our infrastructure safe and ensure responsible usage. Our process extends beyond initial purchase and onboarding, continuing throughout the entire customer lifecycle to stay ahead of potential threats.

We have automated systems in place to validate payments and restrict our services until customers fully confirm their identities. We also continuously monitor how our infrastructure is used to prevent any malicious activities or targeting of sensitive websites.

If we spot anything suspicious, we may request additional details from customers to ensure compliance with our Acceptable Use Policy. If this occurs, we continue monitoring these customers to ensure all activity aligns with our policies and their reported usage.

Our strict practices and automated systems are implemented with a single goal in mind: to protect our customers, provide the highest quality of service, and maintain ethical use of our infrastructure.

We also continue to adapt our services and policies to meet evolving challenges, ensuring that our services remain secure and efficient for all customers.

"IPRoyal KYC is constantly in motion. Unlike others who set and stick to static principles, we adapt and improve our policies continuously to keep up with new challenges and threats in an ever-changing environment. Guaranteeing the best possible services without any risk of abuse or malicious usage is one of the cornerstones of our business."

Karolis Toleikis

Chief Executive Officer at IPRoyal

1

Early Stages of KYC

Our KYC journey starts from the moment someone registers an account with IPRoyal.

At Registration

We immediately verify emails and IP addresses, and match them against potentially fraudulent activity to detect any potential risks. If an email domain or IP is flagged as suspicious, registration is blocked until further verification and authorization is complete.

Customers coming through our direct sales team may be verified during that process. All sales team members are trained in KYC best practices to verify legitimacy and intended business activities of a potential customer throughout sales conversations.

After registration

Once verified, customers can purchase any plan, but have limited access to certain features. To ensure purchases are safe and not intended for illegal transactions, other custom-built solutions are in place including:

- Third-party identity verification
- Automated detection systems
- Monitoring of usage patterns

Identity verification is required to access more advanced features and use our infrastructure for larger-scale activities.

Customers who haven't verified their identity through our third-party provider face restrictions in potential targets and pool size, and some product features remain completely unavailable.

Identity verification unlocks access to the following features:

- The full Residential Proxies IP address pool
- The Residential Proxies API
- Custom rotation options for Mobile Proxies
- The Sub-Users management feature
- All websites, without restrictions

2

Identity Verification Requirements

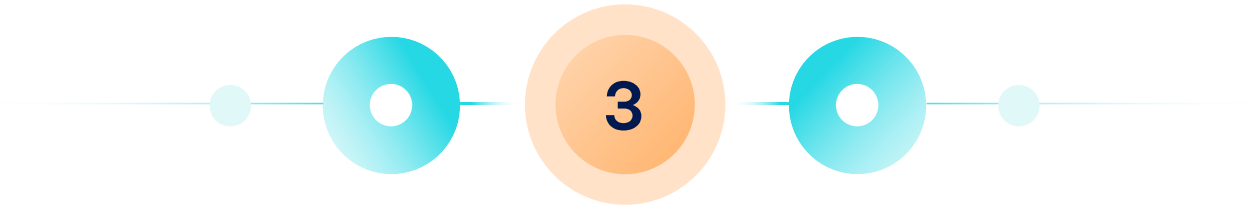
To handle identity verification, we partner with iDenfy, a trusted third-party provider serving numerous respected financial institutions and other businesses. They use live photos and government-issued IDs to curb any attempts to bypass procedures or provide fake documents, including:

- Live photo and ID submission
- Photo manipulation checks
- Manual reviews if needed

In addition to checks run by iDenfy, we may also request business registration information to ensure that a potential customer is truly associated with the company they intend to purchase services for.

Although customers who arrive through our sales team have already shared most information needed to confirm their business is legitimate, additional verification may still be performed by our third-party vendor.

All data required for identity verification is kept secure and confidential, and never shared with other third-parties.



Continued KYC Post-Onboarding

Our KYC practices don't end once a customer is onboard. We continue to have numerous security checks and balances in place to ensure proper usage of our infrastructure.

Monitoring Usage

- **Outgoing requests:** We verify that the number of outgoing requests and URLs visited don't indicate malicious activity.
- **Blocking risky targets:** Inherently risky targets are blocked by default to maintain security.
- **Policy compliance:** We ensure no one is bypassing our Acceptable Use Policy or other restrictions.

While we do not and cannot monitor our customers' activities directly, the above checks help keep our infrastructure secure and efficient.

Handling Suspicious Activity

If we suspect suspicious customer activity, our compliance team may take the following actions:

- **Temporary suspension:** We may temporarily suspend or limit the usage of our proxies.
- **Customer questionnaire:** A questionnaire is sent to the customer to gather a detailed description of the activities being performed.
- **Risk evaluation:** If the explanation is legitimate, service may resume. If not, further steps are taken.

If the initial explanation is unclear or insufficiently convincing, additional questions may be asked. We may also provide recommendations that must be implemented to reduce the risk for both our infrastructure and the customer's business activity.

Revoking Access

IPRoyal reserves the right to remove access to our infrastructure for any harmful or illegal activities. If we determine that an activity falls under either category, we may revoke access even if the customer provides an explanation that appears legitimate.

4

Forbidden Use Cases

Certain activities are strictly forbidden for all users of our infrastructure, regardless of verification or trust. Some common use cases that are illegal in most countries or highly risky, and therefore strictly prohibited, include:

- Distributed Denial of Service attacks (DDoS attacks)
- Spamming
- Brute force attacks
- Impersonation or identity theft

A full list of forbidden activities can be found in our Acceptable Use Policy.
Engaging in any of these activities will result in immediate account suspension without recourse. No exceptions.

The list of forbidden activities are subject to change and may be added or removed at any time. Customers will be informed of any changes and given an appropriate time window to adapt.

Risky Use Cases

Some use cases may be inherently risky but not strictly forbidden. We review these manually and may request a detailed explanation of the business model. If precautions are taken and our recommendations are followed, customers may be permitted to continue using our infrastructure.

Legal Compliance

As part of our KYC practices, we fully cooperate with legal authorities to ensure our services are not used for illegal purposes. If contacted by law enforcement, IPRoyal complies with their requests.

Summary

Our KYC practices guide every step of the customer journey, from registration to ongoing monitoring. Every step is carefully monitored and managed by both manual and automated reviews. We do this to maintain high-quality service and prevent any misuse of our infrastructure. Here's a quick recap:

Registration

We start by verifying emails and IP addresses to identify potential risks. Suspicious entries are blocked until further verification is completed.

Identity Verification

Optional identity verification is conducted to confirm legitimacy, allowing customers to access more advanced features and services.

Post-Onboarding Monitoring

Once onboard, we continue monitoring usage to ensure compliance, including outgoing requests, blocking risky targets, and enforcing adherence to our policies.

Handling Suspicious Activity

If suspicious activity is detected, we temporarily restrict access and request more information. Depending on the outcome, service may resume or further actions may be taken.

Revoking Access

For harmful or illegal activities, we reserve the right to revoke access. In severe cases, accounts are suspended outright.

Forbidden and Risky Use Cases

Certain activities are strictly forbidden, while some risky activities may be allowed with precautions and explicit approval.

Legal Compliance

We cooperate with legal authorities when necessary to ensure the safety of our infrastructure.

Ultimately, our goal is to ensure the reliability and integrity of our network, while addressing any threats swiftly, to maintain trust and provide a secure environment for all our customers.

Interested in IPRoyal Proxies?

Contact Our Sales Team