

# Security Standards & Policy



At TaxNodes, we place customer trust and data security at the forefront of our business. We are committed to maintaining the highest standards of security and have implemented a comprehensive range of measures to ensure the confidentiality and integrity of our customers' data. If you have any questions or concerns, please do not hesitate to contact us at [care@taxnodes.com](mailto:care@taxnodes.com).

## Product Security

### **Passwords:**

To provide our users with a secure login experience, we offer authentication through trusted third-party providers such as Google, Twitter, and LinkedIn. We do not store any passwords on our servers. In the case of email sign-ups, we employ a magic link system that expires after 15 minutes, and we do not store passwords in any form.

### **API Keys & Blockchain Keys:**

We store all API and blockchain keys securely before storing them in our database. TaxNodes does not require access to any private keys or funds on your exchanges. We recommend disabling withdrawal/trading privileges when connecting API keys and only require read-only keys.

### **Customer Data:**

At TaxNodes, we use AES 256-bit encryption standards to store customer data in an encrypted format within our database. Even in the unlikely event of a security breach, any intruder would be unable to obtain any sensitive information. We maintain strict confidentiality and never disclose any customer data to third parties for any reason.

### **Uptime:**

We have an uptime of 99.9% or higher. Any planned downtime is announced in advance on our social media platforms and on our Twitter handle @taxnodes\_.

### **Security Assertion Markup Language (SAML) Single Sign-On (SSO) :**

Our SSO feature allows users to authenticate without requiring additional login credentials.

## Application Security

### **Data Hosting and Storage:**

TaxNodes services and data are hosted on Amazon Web Services (AWS), a cloud application platform that applies security controls at every layer from physical to application. AWS isolates customer applications and data and rapidly deploys security updates without customer interaction or service interruption, effectively protecting customers from threats.

**Data Access:**

At TaxNodes, we limit access to customer data to authorized employees who require it for their job.

**Encryption:**

TaxNodes is served 100% over HTTPS. All data sent to or from TaxNodes is encrypted in transit using 256-bit encryption.

**VPN:**

We keep all critical parts of our application behind a secured VPN service. Only authorized employees who have been vetted can access the system.

**Vulnerability Assessment and Penetration Testing:**

TaxNodes uses third-party security tools to continuously scan for vulnerabilities. We also periodically audit our software and infrastructure through third-party security firms to ensure compliance with security standards. Our dedicated security team responds promptly to any issues raised.

## **Additional Security features**

**Training:**

At TaxNodes, all employees complete annual Security and Awareness training to ensure they remain up-to-date on the latest security protocols.

**Policies:**

We have developed a comprehensive set of security policies that cover a wide range of topics. We update these policies frequently and share them with all employees.

**Employee Vetting:**

TaxNodes performs background checks on all new employees in accordance with local laws.

**Confidentiality:**

Our employee contracts include a confidentiality agreement that emphasizes the importance of maintaining the confidentiality of customer data.

**PCI Obligations:**

All payments made to TaxNodes are processed through our trusted partners Payu, PhonePe, or Stripe. For more information about their security setup and PCI compliance, please refer to their respective Security pages.

## Privacy Features

Our application allows you to **delete all imported data** (and associated wallet/exchange information) at any time for any reason.

We will **never sell your data** to third parties. Please see our privacy policy for details.

We will never ask for your crypto wallet's **private keys**.

Our integrations only require **read access** to your data.

All API keys are securely stored and **encrypted in transit** and at rest.