INSTASHIFT SECURITY POLICY

At InstaShift, security is our top priority. We have taken a multitude of steps to help ensure your data is safe and secure. We recognize that in order to provide a secure platform in the digital currency space, security is an interminable effort. Our security team works perpetually to combat the latest in cyber threats in a proactive manner. While we cannot disclose all of our defence techniques, we're happy to provide the following policy and guidelines.

Account Protection

• All user data is encrypted with AES 256-bit encryption and sensitive user data (encrypted or not) is never returned to the client.

• Every request on InstaShift goes through a verified and secure (ORG) SSL.

• Every successful and failed login attempt is logged and timestamped by IP address and user agent.

• Failed login attempts will result in both an account lockout and IP ban for an extended period of time.

• Lockdown links are provided in every transactional e-mail that allows the user to completely disengage all of their API keys, requires a password reset and closes out any active sessions.

InstaShift OÜ, Narva mnt 9-8, Harjumaa
Tallinn, Estonia , 10117
support@instashift.io

• Heuristic algorithms are employed to monitor for unusual account activity and if flagged will immediately process an account lockdown and terminate any active sessions.

API Key Security

• API Accounts are stored with strong encryption and are never returned to the client under any circumstances.

• API Keys are never stored or displayed anywhere in an unencrypted format. Your browser does not ever make requests to the exchange API directly from your computer.

• In addition, every request to InstaShift.com is done across SSL. This ensures all data transmission to/from our servers is encrypted. This is true for your browser, as well as the mobile app. The first (and only) time your key/secret is submitted to our servers, it is encrypted by SSL.

• Most exchanges allow you to set restrictions on your exchange API keys which limit the capabilities they have to just the functionality you want to use on InstaShift.

• InstaShift strongly recommends that you only enable the API features that you intend to use and never enable withdrawals via API.

• It is the user's responsibility to keep both their InstaShift account and their exchange accounts secure.

System Security

• InstaShift uses a multi-tiered server architecture with complex credentials to ensure server integrity.

• InstaShift never handles your funds directly. All funds remain stored in the exchange's wallets.

• All user requests are filtered and checked on the front-end and back-end for XSS, CSRF, Clickjacking and Session Impersonation attacks.

• We use only parameterized queries to the database to further prevent injection attacks.

• InstaShift is hosted in Google's data centres and our team has a combined experience of more than 90 years in web security and best practices.

• All servers are protected with a strong firewall, and only key team members have access.

• Systems are audited regularly and always up-to-date with the latest in security fixes.

• DNS-level DDOS (Distributed Denial of Service) protection is employed.

• Internal auditing and security screening is employed across all networks and instances.

InstaShift OÜ, Narva mnt 9-8, Harjumaa
Tallinn, Estonia , 10117
support@instashift.io

Employee Security

• All employees are required to use hardware authentication devices where applicable.

• All employee accounts are restricted/compartmentalized to their specific area of knowledge.

• Sensitive information is never transmitted via insecure channels and further is always encrypted via PGP.

• A strong VPN is required for all employees to access any internals.

• All third-party accounts have 2FA (Two-Factor authentication) and in most cases require hardware authentication.

• Regular account auditing and password rotation are required.

Further Security Questions

Should you have any further questions with regards to security on InstaShift, please feel free to reach out via support@instashift.io.We're happy to hear from you.

InstaShift OÜ, Narva mnt 9-8, Harjumaa
Tallinn, Estonia , 10117
support@instashift.io