LegacySuite

Legacy Suite Security: A Trusted & Robust Approach

At Legacy Suite, we understand that securing your data is of paramount importance. Our unwavering commitment to this end is underpinned by our meticulously designed security protocols.

Legacy Suite Proudly Anchors Its Security With Five Distinct Layers:

01 Database Level

02 On-Chain Security

03 Server Level Security

04 Host Level Security

05 User-Specific Security

Database Level Security:

Our primary layer, where all encrypted data, including personal details, is stored. With certificate-based authentication access and SSL encryption for data in transit, we ensure utmost data protection. IP whitelisting, specific to our client-side, prevents unauthorized database access. Beyond storing data, our proactive approach involves regular security assessments, staying abreast of the latest security best practices, and using separate PostgreSQL clusters for different services, ensuring isolated impacts in case of breaches.

On-Chain Security:

We're elated to announce our smart contracts' successful audit by CertiK, a leading blockchain security firm. Their rigorous assessment and subsequent approval stand as a testament to our commitment to absolute security, confirming that our platform's foundation is unwaveringly secure.

Server Level Security:

Our server infrastructure, particularly on AWS, is fortified with a robust security strategy. We've implemented a myriad of measures, including VPC environment setup, IAM roles, HTTPS protection for our NestJS application, traffic control via firewalls, encryption for data at rest, and continuous threat monitoring. Our proactive approach helps us anticipate and combat potential vulnerabilities.

Host Level Security:

In our front-end application, security is paramount. We've implemented a comprehensive security framework that includes measures against Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF). Secure development practices, coupled with regular security audits, ensure that our users always have a secure experience. Additionally, our backend only accepts requests from whitelisted IP addresses, ensuring another layer of safety.

User-Specific Security:

Your personal safety is our priority. We've enforced strong authentication, multi-factor validation, and robust password policies. With data encryption both at rest and in transit, role-based access, audit logs, and an incident response plan, we've left no stone unturned in ensuring your data's safety and maintaining your trust. In our commitment to bolstering user-specific security measures, we have also implemented two-factor authentication (2FA) as an integral component. By adding this extra layer of security, users are required to provide two distinct forms of identification before accessing their accounts, further diminishing the likelihood of unauthorized access.

At Legacy Suite, our layered approach to security is not just about protocols; it's about our commitment to you. Your trust drives us to implement and consistently upgrade our security measures, making sure that you and your legacy remain safeguarded.

Crypto & NFT Will:

The Crypto Will is a patented feature in Legacy Suite which harnesses the power of smart contracts to allow you to plan for the future of your digital assets. With this tool, you can set up automatic transfers of your cryptocurrencies to a designated beneficiary or a backup wallet, ensuring they're safely passed on without any middlemen. These smart contracts operate independently on the blockchain, executing transfers directly between your wallet and your beneficiary's. Rest assured, our smart contracts have been rigorously audited by top-tier security experts to maintain the highest standards of safety. Legacy Suite acts only as a facilitator, providing this service within your subscription package, without any additional fees or intermediary handling of your assets or information.

LegacyPass:
Blockchain-Based Password Management and Sharing

LegacyPass is a pioneering patented password manager utilizing blockchain technology. It integrates with the user's in-app web3 wallet (Torus), automatically assigned upon registration, ensuring continuous access through the Legacy Suite account. This feature addresses the common issue of lost web3 wallet access. Passwords and passphrases are encrypted using the user's public key, turning them into secure strings within our backed-up databases. This method guarantees that only the private key holder, the rightful owner, can decrypt and access their passwords. Our system is designed to be fully secure, making it impossible for even Legacy Suite to view or access the stored passwords. When shared, passwords are encrypted with the beneficiary's public key, ensuring that only their corresponding private key can decrypt them, thereby maintaining strict confidentiality and access control.

Post-Death System Protocols: Ensuring Smooth Transition

Life is unpredictable, and ensuring that our digital assets are safely and respectfully transferred after we're gone is crucial. Legacy Suite's Post-Death System Protocols provide a structured, secure process to manage and transition digital legacies.

Steps for Digital Executors:

Access our contact form.

Choose "I'm initiating the digital asset transfer process for a deceased Legacy Suite account owner".

Submit the Death Certificate.

Provide the Last Will and Testament or corresponding Probate Documents.

Show a government-issued photo ID of the designated Digital Executor.

A letter from the nominated Digital Executor or Executor in the Probate Documents directing Legacy Suite to commence the digital asset transfer process.

Note*: A 30-day processing period is standard. If documents are missing, or if there's unfamiliarity with our system, our dedicated team is here to help. Requirements might differ based on specific circumstances and locations.

Administrative Process:

Once the administration team verifies the provided documents, the account is marked deceased. The system mandates at least three admin signatures to initiate an AWS lambda-based notifier to verify the user's passing. Any login activity during a specified grace period halts asset transfers. Without a response, the system begins the transfer, permitting nominated beneficiaries access to assets. The sole super admin wallet ensures another security layer by being the only entity capable of updating administrators.

Life's unpredictability makes the task of safeguarding our digital legacies even more vital. Legacy Suite's Post-Death System Protocols are meticulously designed to ensure that the transition of your digital assets is seamless, secure, and in line with your wishes. Our protocols ensure that your legacy is managed with the utmost respect and integrity.