

DEFYLD

COMPLIANCE & TRANSPARENCY REPORT

Service	DEFYLD Self-Custody Blockchain DeFi Wallet
Website	http://defyld.com
Status	Public
Last Updated	20 April 2026

Self-custody first: users retain responsibility for private keys, recovery phrases, wallet credentials, transactions, and decisions to interact with independent blockchain networks and DeFi protocols.

1. PURPOSE OF THIS REPORT

This Compliance & Transparency Report describes the general compliance, governance, risk-management, privacy, security, and operational principles applicable to DEFYLD. DEFYLD is designed as a self-custody blockchain DeFi wallet through which users may interact with supported blockchain networks, digital assets, decentralized applications, smart contracts, and decentralized-finance protocols. The purpose of this report is to provide transparency concerning the principles under which DEFYLD seeks to operate. This report does not represent that DEFYLD is licensed, registered, authorized, supervised, or regulated by a particular governmental or financial authority unless such status is expressly confirmed through official DEFYLD disclosures.

2. SERVICE OVERVIEW

DEFYLD provides software and digital interfaces designed to enable users to manage and interact with supported blockchain assets and decentralized-finance services. Depending on availability, jurisdiction, blockchain support, and technical integrations, functionality may include self-custody wallet functionality, blockchain transfers, multi-chain asset management, token swaps, cross-chain functionality, staking, DeFi yield opportunities, decentralized lending and borrowing, wallet connectivity, smart-contract interaction, and access to supported decentralized applications and protocols. DEFYLD is designed around the principle that users retain control over their private keys, recovery phrases, wallet credentials, and blockchain assets.

3. SELF-CUSTODY MODEL

DEFYLD operates on a self-custody design principle. DEFYLD does not intend to take possession or control of a user's private keys or recovery phrase as part of ordinary self-custody wallet functionality. Users remain responsible for protecting private keys, recovery phrases, wallet credentials and devices; reviewing transactions before authorization; understanding smart-contract interactions; and maintaining appropriate backups where applicable. Loss or compromise of credentials may result in permanent loss of access to digital assets. Blockchain transactions may be irreversible once confirmed.

4. COMPLIANCE PRINCIPLES

DEFYLD seeks to operate consistently with applicable laws and regulatory requirements relevant to the services it actually provides. Because blockchain and decentralized-finance regulation differs substantially between jurisdictions, regulatory treatment may depend on the user's jurisdiction, the digital asset, blockchain, functionality, third-party protocol, transaction structure, and changes in law or regulatory interpretation. DEFYLD may modify, restrict, suspend, or discontinue functionality where reasonably necessary to address legal, regulatory, security, technical, or operational requirements.

5. REGULATORY APPROACH

DEFYLD seeks to monitor material regulatory developments affecting self-custody wallets, blockchain technology, decentralized finance, digital assets, privacy, cybersecurity, and related services. Relevant areas may include virtual-asset regulation, anti-money-laundering and counter-terrorist-financing requirements, sanctions, consumer protection, financial-services regulation, data protection, cybersecurity, tax-reporting frameworks, and other digital-asset regulation. Nothing in this report should be interpreted as a claim that DEFYLD is subject to, registered with, or authorized by a particular regulator unless expressly stated in an official regulatory disclosure.

6. DECENTRALIZED PROTOCOLS

DEFYLD may provide interfaces through which users can interact with independent blockchain protocols and decentralized applications, including decentralized exchanges, staking protocols, liquidity pools, lending and borrowing protocols, blockchain bridges, smart contracts, oracle networks, wallet-connectivity protocols, and other blockchain infrastructure. Unless expressly stated otherwise, such protocols are independent from DEFYLD.

7. RISK MANAGEMENT FRAMEWORK

DEFYLD seeks to identify and manage material technical, operational, security, legal, and blockchain-related risks. Principal categories include cybersecurity risk, smart-contract risk, blockchain network risk, liquidity risk, bridge and cross-chain risk, market risk, operational risk, regulatory risk, and user security risk. Risk-management measures may include secure development practices, encryption, access controls, monitoring, authentication safeguards, vulnerability management, incident-response procedures, and ongoing review.

8. SECURITY FRAMEWORK

Security is a fundamental component of the DEFYLD service model. DEFYLD seeks to apply reasonable technical and organizational security measures appropriate to the nature of its services, which may include encryption, secure software-development practices, authentication controls, access management, security monitoring, infrastructure hardening, vulnerability assessment, transaction verification mechanisms, incident response, third-party security assessments, and ongoing security improvements. No software, wallet, blockchain network, smart contract, device, or internet-connected system can be guaranteed to be completely secure.

9. PRIVACY AND DATA PROTECTION

DEFYLD seeks to apply principles of data minimization, transparency, security, and responsible processing of personal information. Public blockchain information is fundamentally different from information maintained within conventional private databases. Blockchain transactions may permanently expose wallet addresses, transaction hashes, asset movements, timestamps, smart-contract interactions, and other public blockchain information. DEFYLD generally cannot alter or erase information independently recorded on a decentralized blockchain.

10. COOKIES AND DIGITAL TECHNOLOGIES

DEFYLD may use cookies, local storage, session technologies, security technologies, analytics, and similar digital mechanisms where reasonably necessary to provide, secure, maintain, or improve its services. DEFYLD seeks to minimize unnecessary data collection. Further information is provided in the DEFYLD Cookies Policy.

11. AML, SANCTIONS AND FINANCIAL-CRIME CONSIDERATIONS

The regulatory obligations applicable to self-custody wallet software may differ from those applicable to custodial exchanges, centralized financial institutions, or other virtual-asset service providers. Where legally required in connection with particular DEFYLD services or activities, DEFYLD may implement appropriate measures relating to sanctions compliance, fraud prevention, financial-crime risk, transaction-risk assessment, legal requests, and other mandatory compliance obligations. The presence of such measures does not change the self-custodial nature of wallet functionality where users retain control over their private keys.

12. THIRD-PARTY SERVICE PROVIDERS

DEFYLD may rely upon independent third-party providers for technical or operational functions such as blockchain infrastructure, hosting, cybersecurity, analytics, communications, data services, wallet connectivity, blockchain routing, decentralized protocols, and other technology services. Third-party services may be subject to their own terms, privacy policies, security models, and regulatory obligations. DEFYLD cannot guarantee the continuous operation or security of independent third-party services.

13. USER RESPONSIBILITY

Self-custody provides users with direct control but also places significant responsibility on the user. Users are responsible for securing wallet credentials and recovery phrases, maintaining device security, verifying wallet addresses, reviewing transaction information, understanding network fees, evaluating smart contracts and third-party protocols, understanding applicable tax obligations, and determining whether their activities comply with applicable law. DEFYLD cannot reverse a blockchain transaction merely because a user made an error or later changed their decision.

14. TRANSACTION TRANSPARENCY

Blockchain transactions may be permanently recorded on public distributed ledgers. Information recorded on a blockchain may include wallet addresses, transaction hashes, asset types, transaction amounts, smart-contract interactions, timestamps, network fees, and other transaction information. Public blockchain information may be analyzed by third parties and potentially associated with other information. Use of DEFYLD does not make public blockchain activity anonymous.

15. GOVERNANCE AND ACCOUNTABILITY

DEFYLD seeks to maintain appropriate governance and accountability mechanisms proportionate to its operations. These may include defined operational responsibilities, security oversight, risk assessment, policy management, incident-response procedures, legal and regulatory monitoring, third-party risk assessment, privacy controls, and periodic review of operational practices. Specific corporate officers, directors, regulatory registrations, licenses, audit arrangements, or certifications should be identified only through official DEFYLD corporate or regulatory disclosures where applicable.

16. CONTINUOUS COMPLIANCE REVIEW

The regulatory environment for blockchain technology and decentralized finance continues to evolve. DEFYLD may periodically review its compliance framework, Terms of Service, Privacy Policy, Cookies Policy, security controls, risk-management procedures, supported jurisdictions, supported assets, blockchain integrations, and DeFi functionality. DEFYLD may make changes where necessary to address regulatory, technical, security, or operational developments.

17. INTERNATIONAL OPERATIONS

Blockchain networks operate internationally, while laws and regulatory requirements remain jurisdiction-specific. Certain DEFYLD functionality may therefore be unavailable, restricted, or modified for users in particular jurisdictions. Users remain responsible for determining whether their use of DEFYLD, particular digital assets, and decentralized-finance protocols is lawful in their jurisdiction.

18. NO INVESTMENT ADVICE

DEFYLD does not provide investment, financial, legal, accounting, or tax advice. Information provided through DEFYLD services is intended for general informational and technical purposes unless expressly stated otherwise. Users should obtain independent professional advice where appropriate.

19. DIGITAL-ASSET RISK DISCLOSURE

Digital assets and decentralized finance involve significant risk, including loss of some or all digital assets, extreme market volatility, smart-contract vulnerabilities, protocol exploits, blockchain failures, bridge exploits, liquidity failures, oracle failures, transaction errors, cybersecurity incidents, regulatory changes, and loss or compromise of wallet credentials. Past performance, protocol history, displayed rates, estimated yields, or other historical information does not guarantee future results.

20. COMPLIANCE TRANSPARENCY

DEFYLD seeks to communicate its regulatory and operational status accurately. Accordingly, DEFYLD does not intend to claim a license, registration, regulatory approval, insurance arrangement, audit certification, or governmental endorsement unless the relevant claim is accurate, current, and capable of appropriate verification. Users should rely on official DEFYLD communications and applicable regulatory registers when verifying regulatory status.

21. RELATIONSHIP WITH DEFYLD POLICIES

This report should be read together with applicable DEFYLD policies, including the DEFYLD Terms of Service, DEFYLD Privacy Policy, DEFYLD Cookies Policy, and other applicable risk or service disclosures. If mandatory law conflicts with a provision of this report, applicable mandatory law will prevail to the extent required.

22. UPDATES

DEFYLD may update this report periodically to reflect changes in services, technology, blockchain integrations, security practices, risk-management practices, regulatory requirements, applicable laws, or DEFYLD operations. Users should review the current version published through official DEFYLD channels.

23. CONTACT AND VERIFICATION

Information concerning DEFYLD should be verified through official DEFYLD communication channels. Website: <http://defyld.com>. Users should exercise caution regarding fraudulent websites, impersonation attempts, phishing communications, and individuals falsely claiming to represent DEFYLD. DEFYLD representatives should never require a user to disclose a private key or recovery phrase in order to provide ordinary wallet support.

24. FINAL COMPLIANCE STATEMENT

DEFYLD is designed around self-custody, user control, responsible blockchain access, security, transparency, and appropriate compliance with applicable legal requirements. DEFYLD's role as a self-custody blockchain DeFi wallet should be distinguished from traditional custodial financial services. Users maintain responsibility for their private keys, recovery phrases, transactions, devices, and decisions to interact with independent blockchain networks and decentralized protocols. DEFYLD seeks to continue adapting its compliance, security, privacy, and risk-management framework as blockchain technology and applicable regulatory requirements evolve.

END OF COMPLIANCE & TRANSPARENCY REPORT

DEFYLD

Self-Custody Blockchain DeFi Wallet

Website: <http://defyld.com>