BLOCKWILL

Data Archival and

Data Retention Policy

Customer and Partner Trust Document

Version 1.0

Effective Date: 12 May 2026

Next Review: 12 May 2027

BlockWill Analytical Technologies Limited

DIFC Innovation One, Dubai International Financial Centre

www.blockwill.io · deepaksaini@blockwill.io · +971 52 545 1081

Document Control

Field	Detail
Document Title	BlockWill Data Archival and Data Retention Policy
Version	1.0
Effective Date	12 May 2026
Document Owner	Head of Security, BlockWill Analytical Technologies Limited
Approved By	Board of Directors, BlockWill Analytical Technologies Limited
Review Cycle	Annual, or upon material change in law, product, or corporate structure
Classification	Public (Customer and Partner Facing)
Issuing Entity	BlockWill Analytical Technologies Limited, DIFC, Dubai, UAE

1. Introduction and Our Promise to You

BlockWill is a digital inheritance infrastructure provider. The data you trust to us, ranging from the keys that protect your digital assets to the documents that record your final wishes, is the most personal data anyone can hold. This Policy explains, in plain language, exactly how we archive it, how long we keep it, when and how we delete it, and what we will do to protect it if, for any reason, BlockWill itself should cease to exist.

This is a public document. It is published as part of our customer and partner trust commitments. If anything we describe here changes, we will tell you, and we will do so before the change takes effect. Our promise is simple: your data outlives our company, and your continuity is engineered, not assumed.

2. Scope and Applicability

This Policy applies to all personal data, account data, and cryptographic material processed by BlockWill in the course of providing the SecureVault, DigiWish, and VaultRelay services, whether you access us as an individual user, an Asset Owner, an Asset Manager, a Guardian, an Executor, a Beneficiary, or as a partner organisation embedding BlockWill into a client offering.

It applies to every BlockWill system, employee, contractor, and processor, and it applies wherever in the world we process data. Where local law imposes a stricter standard than what is set out here, the stricter standard prevails. The terms of this policy are subject to the events mentioned in Section 12.

3. Defined Terms

- **Active Account** means an account with ongoing subscription, including annual subscription and lifetime subscription under any plan.
- **Cryptographic Erasure** means the irreversible destruction of all keys required to decrypt ciphertext, rendering the underlying data unrecoverable.
- **Trigger Event** means a verified death, incapacity, dead-man-switch expiry, or inactivity threshold that activates a VaultRelay release.
- **Vault Content** means data you store in your SecureVault, encrypted client-side under keys that only you and your designated stakeholders control. BlockWill does not have access to plaintext Vault Content at any time.

4. Guiding Principles

Five principles govern every retention and archival decision we make:

- Privacy by design. Vault Content is encrypted with keys we cannot read. Cryptographic erasure and data deletion is the default end state.
- Minimum necessary data. We collect only what is required to deliver the service and to meet legal duties. We do not monetise personal data.
- Defensible storage limitation. Every category of data has a defined active retention period, an archival period, and a final disposition step.
- Auditability. Every retention, archival, and deletion action is logged immutably and is available to regulators and to you on request.

5. Data Classification

We classify data into nine categories. The retention table in Section 6 applies the relevant treatment to each.

- Vault Content. End-to-end encrypted; zero-knowledge to BlockWill.
- Identity and KYC Data. Government identification, sanctions screening results, proof-of-address.
- DigiWish Documents. Legally-vetted proof-of-intent templates and the user's completed instances.
- VaultRelay Trigger and Release Logs. Records of trigger conditions, verifications, and release events.
- Audit Logs and Security Telemetry. Authentication events, administrative actions, anomaly detections.
- Payment, Subscription and Billing Records. Invoices, receipts, payment processor references.
- Marketing and Communications. Subscriptions, consents, communications history.
- Support, Complaint and Legal Correspondence. Tickets, dispute history, regulator correspondence.
- Anonymized Analytics and Product Telemetry. Aggregated, irreversibly anonymized usage statistics.

6. Retention Schedule

The following schedule is the master reference for how long we hold each category of data. Where multiple jurisdictions apply, the longest mandatory retention applies, after which data is archived or deleted in accordance with the disposition column.

Data Category	Active Retention	Post-Account-Closure Archival	Final Disposition
Vault Content (encrypted at rest under user-controlled keys)	For the life of the active account	Retained for up to 7 years post-trigger release, then 90-day quarantine	Cryptographic erasure of ciphertext and data deletion
Identity and KYC Data	For the life of the active account	7 years post-closure (UAE AML and DIFC retention obligations)	Secure deletion with audit-trail
DigiWish Documents and Proof-of-Intent Records	For the life of the active account	10 years post-trigger event (succession evidentiary value)	Release to designated Executor or escrow custodian; then secure deletion
VaultRelay Trigger and Release Logs	Active during contract lifecycle	10 years post-release (immutable, hashed on Polygon)	On-chain hash remains; off-chain payload securely deleted
Audit Logs and Security Telemetry	Hot storage for 13 months	Cold archival for 7 years (SOC 2, AML, DPL audit defensibility)	Automated cryptographic erasure
Payment, Subscription and Billing Records	For the life of the active account	10 years post-closure (UAE VAT, Indian Companies Act, EU/UK tax law)	Secure deletion
Marketing and Communications Preferences	Until consent is withdrawn	12 months post-withdrawal (proof of consent only)	Secure deletion
Support, Complaint and Legal Correspondence	3 years from last interaction	Up to 10 years where required by litigation hold or regulator	Secure deletion with retention log entry
Anonymised Analytics and Product Telemetry	Indefinite (no identifiers)	Not applicable (already irreversibly anonymised)	Retained for product improvement

Active retention runs from the date data is collected until your account is closed or the relevant processing purpose is concluded. Archival retention begins on account closure or trigger event,

whichever applies. Final disposition is executed by automated workflow, with a manual reviewer countersignature for vault and DigiWish data.

7. Archival Mechanisms

7.1 Tiered storage

Active data is held in hot, geographically redundant storage within the DIFC and primary regional clusters. On the dates set out in Section 6, data is moved to cold archival storage with stricter access controls, immutable retention locks, and separate cryptographic boundaries.

7.2 Immutable audit ledger

All access to archived data is recorded in an immutable audit ledger. Hashes of archival manifests are anchored to the Polygon network on a daily cadence so that the integrity of archived records can be independently verified at any future point.

7.3 Key custody

Vault Content remains under your cryptographic control throughout the archival lifecycle. BlockWill never escrows your private keys to itself. Recovery and stakeholder access rely on the multi-party key arrangements you configure inside SecureVault, not on any backdoor held by us.

8. Deletion and Erasure

When data reaches the end of its retention period, or when you exercise a valid erasure right, we apply cryptographic erasure first and data deletion thereafter. Cryptographic erasure destroys the keys necessary to decrypt the relevant ciphertext, rendering the data unintelligible even if the underlying storage media were ever recovered, and data deletion erases all the data stored on our servers.

Backups and disaster-recovery snapshots are subject to the same retention schedule. Where data has been deleted but still exists in an active backup set, it will be deleted on the next scheduled overwrite cycle, which occurs at intervals of no more than 35 days. Until then, the data is sealed and is not retrieved for any purpose other than disaster recovery.

9. Cross-Border Transfer and Data Sovereignty

Our primary data residency is in the DIFC and the United Arab Emirates. Onward transfers occur only to jurisdictions that provide adequate data protection, or under safeguards that meet the standards of the originating jurisdiction. These include DIFC Standard Contractual Clauses, EU and UK Standard Contractual Clauses, and the recognised adequacy mechanisms under DPDPA.

10. Trigger-Event Data Handling

When a VaultRelay Trigger Event occurs, BlockWill enters a defined release workflow. The workflow is intentionally designed so that BlockWill itself never views Vault Content at any stage.

- Notification. The Executor, Guardian, and named Beneficiaries are notified in the sequence you set.
- Release. Decryption keys flow through the multi-party arrangement you configured. Vault Content moves directly from the your vault to the Beneficiary's vault.
- Logging. A release record is written to the immutable audit ledger and a hashed reference is anchored to Polygon.
- Archival. The release record, the verification evidence, and the chain of custody are archived for specific years for evidentiary and probate purposes, as mentioned in Section 6.
- Final erasure. Once the archival period expires, the data on our servers and the encryption keys are subject to cryptographic erasure and permanent data deletion.

11. Your Rights

Whatever jurisdiction you sit in, the following rights apply to your relationship with BlockWill. Where local law gives you a broader right, the broader right prevails.

Right	How BlockWill Honours It
Access	Self-service export of all metadata held about you, available in your account at any time. Zero-knowledge ciphertext can only be decrypted by your own keys.
Rectification	In-product editing for profile, SecureVault data, DigiWish documents, and stakeholder assignments. Verified support assistance for system-managed records.
Erasure	Account closure triggers cryptographic erasure and data deletion on a 30-day rolling schedule.
Portability	Structured export in machine-readable JSON and PDF formats; DigiWish documents in original drafting format in PDF and Word document.
Restriction and Objection	Granular processing controls in account settings; marketing opt-outs honoured within 24 hours.
Withdraw Consent	Withdrawable at any time without affecting prior lawful processing. Withdrawal does not revoke contractually required retention.

Right	How BlockWill Honours It
Lodge a Complaint	Directly with our Data Protection Officer (privacy@blockwill.io) and, in parallel, with the supervisory authority of your jurisdiction.

Most rights are exercised directly inside your account. For any request that cannot be self-served, write to privacy@blockwill.io. We will acknowledge within 72 hours and substantively respond within 30 days, or such shorter period as local law requires.

12. Business Continuity and Cease-to-Exist Provisions

This section is the part of the Policy that matters most. A digital inheritance platform that ceases to exist without continuity arrangements would be worse than no platform at all. The entire architecture below is designed so that your data, your DigiWish documents, and your designated successor access do not depend on BlockWill remaining operational.

12.1 Three Scenarios, One Outcome

Whatever the circumstances of a BlockWill wind-down, the outcome for you is the same: continuous access, continuous archival, and a defined path for your designated stakeholders to recover what they are entitled to recover.

Scenario	Trigger	Primary Obligation
Scenario A: Graceful Shutdown	Voluntary cessation by Board resolution, exit from market, or product sunset.	Minimum 180 days customer notice; full data export window; orderly handover to Independent Data Escrow Agent.
Scenario B: Insolvency or Regulatory Revocation	Court-ordered liquidation, DFSA or DIFC ROC licence revocation, or material regulatory action.	Immediate activation of Custodial Trustee Agreement; vault custody transfers to DIFC-licensed trustee; user funds and data ring-fenced from creditors.
Scenario C: Acquisition or Change of Control	Merger, acquisition, or transfer of more than 50 percent of voting equity.	30-day prior written notice to users; right to export, port, or delete before transition; binding successor obligations.

12.3 Portability Mechanism if BlockWill Shuts Operations

In the event of BlockWill ever shutting down its operations, owing to any reasons whatsoever, all the active account users shall be notified immediately by registered email and phone number, and a period of 12 months shall be provided to every user for structured export and download of SecureVault data in machine-readable JSON and PDF formats and DigiWish documents in original drafting format in PDF and Word document.

12.8 Cryptographic Continuity

The cryptographic schemes used by BlockWill are designed to be portable to a successor operator. Specifically:

- All Vault Content is encrypted with user-controlled keys; no key material held by BlockWill is sufficient to decrypt Vault Content.
- On-chain anchoring on Polygon guarantees that the integrity of historical archival and release records can be independently verified even after BlockWill is dissolved.

13. Governance and Accountability

The Head of Security is the document owner of this Policy and is responsible for keeping it current. The Board of Directors of BlockWill Analytical Technologies Limited approves every version. The Data Protection Officer, reachable at privacy@blockwill.io, is the day-to-day point of contact for users, partners, and supervisory authorities.

This Policy is reviewed at least annually, and additionally on any material change in applicable law, in the company's corporate structure, in the product, or in the underlying cryptographic schemes. Material changes are notified to users at least 30 days before they take effect.

14. How to Reach Us

- Data Protection Officer: privacy@blockwill.io
- Legal and corporate inquiries: support@blockwill.io
- Registered office: DIFC Innovation One, Dubai International Financial Centre, United Arab Emirates
- Phone: +971 52 545 1081
- Website: www.blockwill.io

End of Policy.