MAGNET4WATER End-User License Agreement (EULA)
Effective Date: August 18, 2025
Last Updated: October 2, 2025
Governing Law: State of Michigan, United States
Company Incorporation: Hydrosimulatics, Inc., incorporated in the State of Delaware, United States

INTRODUCTION

This End-User License Agreement ("Agreement" or "EULA") is a legally binding contract between Hydrosimulatics, Inc., a Delaware corporation ("Hydrosimulatics"), and the individual or entity ("User") that accesses or uses the MAGNET4WATER platform ("Platform"). This Agreement governs all access to and use of the Platform and its associated services.

MAGNET4WATER is designed to ensure that user work—including hydrosimulatics models, telemetry inputs, and simulation outputs—is secure, private, and under the user's control. The platform enforces this protection through a multi-layered security architecture that includes:

- **End-to-end encryption**: All user content is encrypted in transit (TLS 1.3), at rest (AES-256), and during active processing in memory (confidential computing).
- **Confidential computing**: Secure enclave technologies ensure that even runtime data remains encrypted and inaccessible to platform operators and infrastructure providers.
- **Multi-factor authentication (MFA)**: Unauthorized access is blocked—even if login credentials are compromised.
- **Encryption key management**: Users control their encryption keys. Hydrosimulatics does not store, access, or recover user-managed or third-party provisioned keys.
- **Operational inaccessibility**: Hydrosimulatics personnel cannot view, modify, or extract user content under any supported configuration.

These protections are enforced by architecture, cryptographic controls, and operational boundaries—not by discretionary access or policy exceptions. These protections apply exclusively to **Premium Tier** accounts. Free Tier accounts are subject to baseline protections and do not include encryption at rest, confidential computing, or customizable key management.

By accessing, subscribing to, or using the Platform, the User expressly agrees to be bound by all terms and conditions set forth herein. If the User does not agree to these terms, the User must not access or use the Platform.

1. AGREEMENT SCOPE

1.1 This Agreement governs all access to and use of the MAGNET4WATER Platform, including all sub-platforms (IGW-NET, SwaNET, DataNET, StormNET, ConduitNET), services, interfaces, and associated infrastructure.

1.2 This Agreement applies to all tiers of access, including Free Tier and Premium Tier subscriptions. Tier-specific features, protections, and limitations are described in Section 2 (Definitions) and Section 6 (Privacy, Data Ownership, and Security Architecture).

1.3 Hydrosimulatics reserves the right to update, modify, or discontinue any part of the Platform at its sole discretion, provided that such changes do not retroactively alter the terms of this Agreement without notice.

1.4 Users may be subject to additional terms and conditions if accessing the Platform through an institutional deployment, enterprise license, or third-party integration. Such terms shall be deemed incorporated into this Agreement by reference.

2. DEFINITIONS

2.1 Platform

The MAGNET4WATER software system, including all sub-platforms (IGW-NET, SwaNET, DataNET, StormNET, ConduitNET), services, interfaces, and associated infrastructure.

2.2 Protected Data of the User (PDY)

All files, inputs, outputs, models, configurations, telemetry, metadata, and any other content uploaded, generated, or processed by the User within the Platform. This includes personally identifiable information (PII), modeling artifacts, and simulation outputs. PDY is encrypted at all times and inaccessible to Hydrosimulatics under all supported configurations available to Premium Tier users.

2.3 Subscription

A paid license granting time-limited access to the Platform, subject to the terms of this Agreement.

2.4 Free Tier

A limited-access version of the Platform provided without charge, subject to usage restrictions and feature limitations. Free Tier accounts do not include encryption at rest, confidential computing, or customizable encryption key management.

2.5 End-to-End Encryption (E2EE)

A security protocol in which data is encrypted during transmission (TLS 1.3), storage (AES-256), and active processing (confidential computing). E2EE ensures that user content remains unintelligible to unauthorized parties—including Hydrosimulatics and infrastructure providers—throughout its lifecycle. E2EE is available only to Premium Tier users.

2.6 Confidential Computing

A security model in which data remains encrypted during active processing in memory, using secure enclave technologies (e.g., Intel SGX, AMD SEV) that prevent access by hypervisors, cloud operators, and privileged system processes. Confidential computing is available only to Premium Tier users.

2.7 Multi-Factor Authentication (MFA)

A mandatory access control mechanism requiring two or more forms of verification before granting access to modeling environments or encrypted content. MFA blocks unauthorized access—even if login credentials are compromised.

2.8 Encryption Key

A cryptographic key used to encrypt and decrypt PDY. MAGNET4WATER supports three modes of key management for Premium Tier users:

- **User-Managed Key**: A key generated and controlled by the User. Hydrosimulatics does not store, access, or recover this key.
- **Third-Party Provisioned Key**: A key managed by an enterprise IT provider or cloud service under the User's control.
- **Platform-Generated Key**: A key automatically generated and managed by MAGNET4WATER if no other method is selected. Hydrosimulatics enforces strict operational controls to prevent access to content encrypted with this key.

2.9 Secure Enclave

A hardware-isolated execution environment that encrypts data in memory and prevents inspection or extraction by system-level processes.

2.10 Operational Inaccessibility

The architectural guarantee that Hydrosimulatics personnel, infrastructure providers, and third-party services cannot access, inspect, or extract user content under any supported configuration.

2.11 Session Token

A time-bound, encrypted credential used to authenticate user sessions. Session tokens auto-terminate after inactivity and are governed by MFA.

2.12 Metadata

Non-content data such as timestamps, file size, and transmission logs used for performance monitoring and audit. Metadata is stored separately and cannot be used to reconstruct or interpret user work.

2.13 Dissemination Tools

Platform features that allow users to publish, share, or collaborate on modeling outputs. Dissemination is governed by user-selected visibility settings and access permissions.

2.14 Institutional Deployment

A configuration of MAGNET4WATER operated under the control of an academic, governmental, or enterprise entity, with custom encryption, audit, and compliance policies.

2.15 AI Support

Artificial intelligence tools embedded within the Platform to assist Users with modeling, data interpretation, and navigation. AI modules operate within encrypted containers and do not retain or transmit user content beyond the scope of the session.

2.16 Premium Tier

A paid subscription tier that includes full security architecture: end-to-end encryption (in transit, at rest, and in memory), confidential computing, multi-factor authentication (MFA), and user-controlled encryption key management. Only Premium Tier accounts benefit from these protections.

3. LICENSE GRANT

3.1 Subject to the terms of this Agreement, Hydrosimulatics grants the User a non-exclusive, non-transferable, revocable license to access and use the Platform during the Subscription term or Free Tier period.

3.2 The license granted herein is limited to the User's internal research, modeling, and educational use. Commercial use, redistribution, or sublicensing is prohibited unless expressly authorized in writing by Hydrosimulatics.

3.3 The license does not grant any rights to inspect, reverse-engineer, or extract the Platform's source code, algorithms, or internal architecture.

3.4 The license does not include access to encrypted user content by Hydrosimulatics. All Protected Data of the User (PDY) remains inaccessible to Hydrosimulatics under all supported configurations available to Premium Tier users.

4. RESTRICTIONS

4.1 The User shall not:

- Copy, modify, or create derivative works of the Platform;
- Distribute, sell, lease, or sublicense the Platform to third parties;
- Use the Platform to violate applicable laws, regulations, or third-party rights;
- Attempt to gain unauthorized access to any portion of the Platform or its infrastructure;
- Circumvent or disable any security features, including MFA, encryption boundaries, or access controls.

4.2 Free Tier users shall not attempt to simulate or replicate Premium Tier protections, including encryption at rest, confidential computing, or key management features.

4.3 Hydrosimulatics reserves the right to suspend or terminate access for violations of these restrictions, without refund or liability.

5. FEES AND PAYMENT

5.1 Subscription fees for Premium Tier access shall be paid in accordance with the pricing schedule published by Hydrosimulatics or agreed upon in writing.

5.2 All fees are non-refundable except as required by law or explicitly stated in this Agreement.

5.3 Hydrosimulatics may modify pricing or billing terms with thirty (30) days' notice. Continued use of the Platform after such notice constitutes acceptance of the new terms.

5.4 Failure to pay applicable fees may result in suspension or termination of access to Premium Tier features, including encryption, confidential computing, and key management.

6. PRIVACY, DATA OWNERSHIP, AND SECURITY ARCHITECTURE

MAGNET4WATER is built on the principle that user work—including hydrosimulatics models, telemetry inputs, and simulation outputs—must remain secure, private, and under the user's control. This section explains how that protection is achieved through a layered security architecture that governs every stage of the data lifecycle: transmission, storage, computation, access, and sharing.

Hydrosimulatics does not rely on discretionary access policies or trust-based permissions. Instead, it enforces security through cryptographic design, confidential computing, and operational isolation—ensuring that even platform operators cannot access user content under any supported configuration.

Unless otherwise stated, the protections described in this section apply exclusively to **Premium Tier** accounts. Free Tier accounts are subject to baseline protections and do not include encryption at rest, confidential computing, or customizable key management.

6.1 Security Foundations: What Makes User Work Secure

MAGNET4WATER protects user work through five interlocking safeguards:

1. **End-to-end encryption**: Data is encrypted in transit, at rest, and in memory.
2. **Confidential computing**: Data remains encrypted even during active processing.
3. **Multi-factor authentication (MFA)**: Unauthorized access is blocked—even if credentials are compromised.
4. **Encryption key management**: Only the user (or their designated provider) can decrypt their data.
5. **Operational inaccessibility**: Hydrosimulatics cannot view, modify, or extract user content—even during breach scenarios.

These protections are enforced by architecture—not by policy exceptions or administrative discretion.

6.2 End-to-End Encryption

All user content is encrypted across its entire lifecycle:

- **In Transit**: TLS 1.3 encrypts all data exchanged between user devices and MAGNET4WATER servers.
- **At Rest**: AES-256 encryption secures stored data, including models, telemetry, and outputs.
- **In Memory**: Confidential computing environments encrypt data during active processing, ensuring that even runtime content remains inaccessible.

End-to-end encryption is available only to Premium Tier users.

6.3 Confidential Computing and Runtime Protection

MAGNET4WATER uses secure enclave technologies (e.g., Intel SGX, AMD SEV) to protect data during computation:

- All sensitive operations—including model calibration and telemetry parsing—occur within hardware-isolated environments.
- These enclaves prevent access by hypervisors, cloud operators, and privileged system processes.
- Hydrosimulatics personnel cannot inspect or interact with in-memory data under any operational scenario.

Confidential computing is available only to Premium Tier users.

6.4 Multi-Factor Authentication (MFA)

MAGNET4WATER requires MFA to access modeling environments and encrypted data:

- MFA blocks unauthorized access—even if login credentials are compromised.
- Session tokens are encrypted, time-bound, and auto-terminate after inactivity.
- Anomalous login behavior triggers automated containment and alerts.

MFA is enforced across all tiers, but only Premium Tier users benefit from MFA-protected access to encrypted content.

6.5 Encryption Key Management

MAGNET4WATER supports three modes of encryption key management for Premium Tier users:

- **User-Managed Keys**: Users generate and control their own keys. Hydrosimulatics cannot store, access, or recover these keys.
  Key Loss Disclosure: If the key is lost, access to encrypted content is permanently lost.
- **Third-Party Provisioning**: Enterprise IT or cloud providers manage keys via secure vaults. Hydrosimulatics does not retain visibility.
- **Platform-Generated Keys (Default)**: MAGNET4WATER generates and manages keys on behalf of the user.
  Access Boundaries: While technically accessible by infrastructure, Hydrosimulatics enforces strict contractual and operational controls that prohibit access. All access is governed by cryptographic enforcement and legal safeguards.

Free Tier accounts do not support encryption key customization or isolation.

6.6 Operational Inaccessibility

MAGNET4WATER is architected to ensure that:

- Hydrosimulatics cannot view, modify, or extract user content under any supported configuration.
- Infrastructure providers cannot inspect or extract data from secure enclaves or encrypted containers.
- Encrypted data remains unintelligible and unrecoverable without the corresponding key.
- No backdoor access exists. All access is governed by cryptographic enforcement and user consent.

These guarantees apply only to Premium Tier accounts.

6.7 Breach Response Protocols

Hydrosimulatics maintains a proactive, transparent approach to breach prevention and response:

- Continuous monitoring detects unauthorized access attempts and anomalies.
- Affected containers are immediately isolated upon breach confirmation.

- Users are notified within 24 hours and provided with:
- A summary of the incident
- A detailed incident report
- Recommended remediation steps

For Premium Tier users, encrypted data remains inaccessible even during breach scenarios. Free Tier users may be subject to different containment boundaries.

6.8 Metadata Handling and Isolation

MAGNET4WATER may store limited metadata (e.g., timestamps, file size, transmission logs) for performance monitoring and audit purposes:

- Metadata is stored separately and never linked to decrypted content.
- Hydrosimulatics does not use metadata for behavioral profiling or inference.
- Metadata cannot be used to reconstruct or interpret user work.

6.9 AI Privacy and Model Isolation

AI-powered tools operate within encrypted containers and do not retain or transmit user content:

- AI modules do not store, replicate, or learn from user work.
- All AI-assisted computation respects encryption boundaries.
- Hydrosimulatics does not use user content to train external models or third-party systems.

Encrypted container protections apply only to Premium Tier users.

6.10 Legal Compliance and Governance

Hydrosimulatics complies with all applicable data protection laws and institutional frameworks:

- GDPR, CCPA, CPRA, and other U.S. state and international privacy laws
- Jurisdiction-specific frameworks required by institutional contracts
- Internal audit and external review upon request

Governance is overseen by Hydrosimulatics' Data Stewardship Board.

6.11 Audit Logging and Transparency

All system-level interactions with Protected Data are logged and subject to audit:

- Logs include access attempts, session events, and key management actions.
- Users may request audit summaries for their own accounts.
- Hydrosimulatics does not retain logs that expose decrypted content.

6.12 Termination and Data Retention

Upon termination of a user account:

- Encrypted content is retained for a limited period unless deletion is requested.
- Hydrosimulatics cannot decrypt or access retained content without the user's key.
- Users may request immediate deletion of all encrypted content and metadata.

6.13 Institutional Contracts and Sovereignty

Institutional deployments may define custom encryption, audit, and compliance configurations:

- Institutions control key management, access policies, and audit protocols.
- Hydrosimulatics enforces contractual controls that prohibit inspection or export of institutional data.

6.14 Security Architecture Summary

MAGNET4WATER protects user work through architecture—not just policy. The platform ensures that:

- All user content is encrypted in transit, at rest, and in memory
- Hydrosimulatics cannot access user work under any supported configuration
- Encryption keys are never stored or accessible unless explicitly provisioned by the user
- Confidential computing prevents access during runtime—even by privileged system processes
- MFA blocks unauthorized access—even if credentials are compromised
- Metadata is isolated and cannot be used to reconstruct user content

- No backdoor access exists. All access is governed by cryptographic enforcement and user consent

These protections apply exclusively to Premium Tier accounts. Free Tier users are subject to baseline protections but do not benefit from encrypted storage, confidential computing, or key customization.

7. TERMINATION

7.1 This Agreement shall remain in effect until terminated by either party.

7.2 The User may terminate this Agreement at any time by ceasing use of the Platform and, if applicable, requesting deletion of their account and associated Protected Data.

7.3 Hydrosimulatics may terminate this Agreement or suspend access to the Platform immediately, without prior notice, if:

- The User breaches any provision of this Agreement;
- Required fees are unpaid or disputed;
- Continued access poses a security, legal, or operational risk.

7.4 Upon termination:

- All licenses granted under this Agreement shall immediately cease;
- Encrypted content associated with Premium Tier accounts shall remain inaccessible without the user's encryption key;
- The User may request deletion of all retained data, subject to applicable retention policies and legal obligations.

8. DISCLAIMERS

8.1 The Platform is provided "as is" and "as available," without warranties of any kind, express or implied.

8.2 Hydrosimulatics does not warrant that:

- The Platform will be uninterrupted, error-free, or free of harmful components;
- Modeling outputs or simulations will be accurate, complete, or suitable for any specific purpose;

- Encryption or security features will prevent all forms of unauthorized access or data loss.

8.3 Hydrosimulatics disclaims all implied warranties, including merchantability, fitness for a particular purpose, and non-infringement.

9. LIMITATIONS OF LIABILITY

9.1 To the maximum extent permitted by law, Hydrosimulatics shall not be liable for:

- Indirect, incidental, special, consequential, or punitive damages;
- Loss of data, revenue, profits, or business opportunities;
- Damages arising from unauthorized access, use, or disclosure of Protected Data.

9.2 Hydrosimulatics' total liability under this Agreement shall not exceed the amount paid by the User for the Subscription during the twelve (12) months preceding the claim.

9.3 The User acknowledges that:

- Encryption key loss may result in permanent data inaccessibility;
- Free Tier accounts do not include full security protections;
- Use of the Platform is at the User's own risk.

10. GOVERNING LAW AND JURISDICTION

10.1 This Agreement shall be governed by and construed in accordance with the laws of the **State of Michigan**, without regard to its conflict of law principles.

10.2 Any disputes arising under or in connection with this Agreement shall be resolved exclusively in the state or federal courts located in **Michigan**, and the parties consent to personal jurisdiction therein.

10.3 The United Nations Convention on Contracts for the International Sale of Goods shall not apply to this Agreement.

11. USER RESPONSIBILITIES

11.1 The User is responsible for safeguarding their account credentials, encryption keys (if self-managed), and access permissions.

11.2 Hydrosimulatics shall not be liable for:

- Data loss resulting from forgotten, lost, or mismanaged encryption keys;
- Unauthorized access resulting from credential sharing, weak passwords, or MFA bypass;
- Misuse of dissemination tools or visibility settings by the User or their collaborators.

11.3 Users agree to notify Hydrosimulatics immediately of any suspected breach, compromise, or unauthorized access to their account.

12. EXPORT CONTROLS AND INTERNATIONAL USE

12.1 The Platform may be subject to U.S. export control laws and other applicable regulations. Users agree to comply with all such laws and not to export, re-export, or transfer the Platform or its components in violation thereof.

12.2 Users accessing the Platform from outside the United States are responsible for compliance with local laws and regulations, including data protection, encryption, and software usage restrictions.

13. INSTITUTIONAL TERMS

13.1 Institutional Deployments may be governed by separate agreements negotiated between Hydrosimulatics and the institution. Such agreements may override or supplement the terms of this EULA.

13.2 Institutional administrators may define:

- Custom encryption key policies;
- Audit and logging protocols;
- Access boundaries and user provisioning rules.

13.3 Hydrosimulatics shall not inspect, export, or modify institutional data except as explicitly authorized under the governing institutional agreement.