

**HYPORI, INC.
ACCEPTABLE USE POLICY**

Last Updated: May 2026

This ACCEPTABLE USE POLICY (this “**AUP**”) identifies activities that you are prohibited from engaging in when using Hypori, Inc. (“**Hypori**,” “**we**,” “**us**”) software, cloud services, applications, and related services (collectively, the “**Products and Services**”). This AUP applies to all customers, Authorized Users, and any devices accessing Hypori Products and Services, including Hypori Mobile, Hypori Lyte for Secure Messaging, Hypori Lyte for Enterprise Browser, Hypori Lyte for Applications, and Hypori Secure Messaging.

This AUP is incorporated by reference into the Hypori End User License Agreement, Master Subscription Agreement, Terms of Service, and any applicable Order, and is available at www.hypori.com/legal. In the event of conflict between this AUP and any applicable agreement, the applicable agreement governs.

1. Permitted Use

The Products and Services may be used solely for lawful, authorized business purposes in accordance with the applicable agreement with Hypori and all applicable laws and regulations.

2. Prohibited Activities

Customers and authorized users must not, and must not permit others to:

Security and System Integrity

- Attempt to gain unauthorized access to the Products and Services, accounts, networks, or systems.
- Circumvent or disable security, authentication, or access controls.
- Probe, scan, or test the vulnerability of the Products and Services without Hypori’s prior written authorization, except where such testing is required by applicable federal cybersecurity programs or agency authorization processes and is conducted within the customer’s own environment.
- Introduce malware, malicious code, or harmful components.

Against Applicable Law:

- Engage in any activity that violates applicable law or regulation, including violations of copyright, trademark, or other intellectual property laws, computer fraud, unauthorized interception of communications, or export control violations.
- Access or authorize anyone to access the Products and Services from a jurisdiction subject to U.S. government sanctions, or permit access by any individual or entity identified on the OFAC Specially Designated Nationals List, BIS Entity List, or State Department Debarred Parties List.
- Invade anyone’s privacy by attempting to harvest, collect, store, or publish private or personally identifiable information without their knowledge and consent.
- Remove, modify, or tamper with any regulatory or legal notice or link that is incorporated into the Products and Services.

Misuse and Disruption

- Interfere with or disrupt the integrity or performance of the Products and Services or related systems.
- Use the Products and Services in a manner that degrades service for other users.

- Engage in automated usage that exceeds the Licensed Entitlements specified in the applicable Order or that materially degrades the performance of the Products and Services for other users.
- Use the Products and Services to transmit, distribute, or deliver any unsolicited bulk or unsolicited commercial e-mail (i.e., spam).

Unlawful or Harmful Content

- Transmit, store, or make available content that is unlawful, fraudulent, defamatory, obscene, abusive, or threatening.

Data and Privacy Violations

- Upload, transmit, or process personal data, regulated data, CUI, or other sensitive information in excess of what is authorized under the applicable agreement or in a deployment environment not designated for such data.
- Use Hypori Secure Messaging or Hypori Lyte for Secure Messaging to share, transmit, or store content that infringes the intellectual property rights of any third party, including copyrighted materials shared without authorization. Users who receive a notice of alleged copyright infringement in connection with their use of Hypori Secure Messaging should contact their organization's administrator and Hypori at contracts-legal@hypori.com.

Credential Misuse

- Share, sell, or transfer login credentials.
- Use another user's credentials to access the Products and Services, or allow your credentials to be used by another individual.

3. Government Cloud Specific Restrictions.

For users accessing Hypori Government Cloud, the following additional restrictions apply:

- The Products and Services may only be used for authorized government or government contractor purposes consistent with the applicable Authority to Operate and applicable compliance frameworks including CMMC and DFARS 252.204-7012 where applicable.
- CUI and Federal Contract Information may only be processed within the Government Cloud environment and may not be transmitted to or stored in non-authorized environments.
- Access is limited to individuals who satisfy applicable U.S. Person, citizenship, or security clearance requirements as determined by Customer's applicable compliance framework, agency policies, and the eligibility requirements set forth in the applicable agreement with Hypori.
- Any suspected unauthorized access to or disclosure of CUI must be reported to Hypori within 72 hours and to the applicable government agency in accordance with DFARS 252.204-7012.

4. Evaluation and Trial Use.

Customers and authorized users accessing the Products and Services under a trial, evaluation, proof of concept, or pre-release arrangement must not:

- Use the evaluation environment for production workloads or operational data.

- Process CUI, PII, or other regulated data in the evaluation environment unless expressly authorized in writing by Hypori.
- Use evaluation access to benchmark the Products against competing offerings, to develop a competitive product or service, or to provide access to any competitor of Hypori.

5. Customer Responsibilities

Customers are responsible for:

- All use of the Products and Services by their authorized users.
- Maintaining the confidentiality of credentials.
- Ensuring devices and networks used to access the Products and Services meet reasonable security standards.
- Promptly notifying Hypori of any unauthorized access or security incident.

6. Monitoring and Enforcement

Hypori may monitor use of the Products and Services to the extent reasonably necessary to:

- Operate and secure the Products and Services.
- Prevent fraud, abuse, or security incidents.
- Comply with legal obligations.

If Hypori believes that unauthorized or improper use is being made of the Products and Services, Hypori may, upon written notice, suspend or terminate access to the Products and Services for violations of this AUP. Hypori may suspend access immediately and without prior notice where the violation poses an immediate security risk to Hypori, the Products, or other customers, consistent with the suspension rights set forth in the applicable agreement.

In addition to suspension or termination, violations of this AUP may result in legal action and financial liability for damages caused to Hypori or third parties.

Reporting Violations. To report suspected violations of this AUP, security incidents, or unauthorized use of the Products and Services, contact Hypori at contracts-legal@hypori.com or privacy@hypori.com. Hypori will review all reports promptly and will not disclose the identity of the reporting party without their consent except as required by applicable law.

7. Third-Party Services and Connectivity

Customers are responsible for ensuring that all third-party networks, devices, connectivity, and services used to access the Products and Services comply with applicable security requirements and the terms of the applicable agreement. Hypori is not responsible for the availability, security, or performance of third-party networks or devices outside Hypori's control.

8. Changes to This Policy

Hypori may update this AUP at any time by posting a revised version at www.hypori.com/legal. Continued use of the Products and Services after the effective date of any update constitutes acceptance.

9. Contact Information

Questions regarding this AUP may be directed to:

Hypori, Inc.

contracts-legal@hypori.com

- * Nothing in this AUP is intended to grant any rights in the Products and Services beyond those expressly set forth in the applicable agreement.