# ACCEPTABLE USE POLICY (AUP)

OneEstateOS Platform

*Effective Date: June 1, 2026 | Version 1.0*

---

## INTRODUCTION

This Acceptable Use Policy ("Policy" or "AUP") governs the access and use of the OneEstateOS software-as-a-service platform (the "Service") operated by One Estate, Inc. ("Provider," "OneEstateOS," "we," or "our"). This Policy applies to all users of the Service, including property owners, asset managers, entity administrators, fund operators, authorized collaborators, and any third-party service providers granted access to a Vault (collectively, "Users" or "you").

By accessing or using the Service, you agree to comply with this Policy. This Policy is incorporated by reference into and forms part of the OneEstateOS Terms of Service. Capitalized terms used but not defined herein have the meanings given in the Terms of Service.

---

## 1. PURPOSE

The purpose of this Policy is to ensure the lawful, ethical, and secure use of the OneEstateOS platform by all Users. OneEstateOS provides tools for real estate asset management, document intelligence, entity governance, and related operational workflows. This Policy protects the integrity, availability, and confidentiality of the Service, its infrastructure, and the interests of all Users and third parties whose information may be stored within the platform.

---

## 2. PROHIBITED CONDUCT

Users are expressly prohibited from using the Service to engage in any of the following:

### 2.1 Unlawful and Fraudulent Activity

(a) Engage in any unlawful, fraudulent, deceptive, or misleading activity;

(b) Upload, transmit, or store documents that are forged, falsified, or materially altered without disclosure, including but not limited to deeds, purchase contracts, operating agreements, loan documents, or title instruments;

(c) Impersonate any person, entity, or legal organization, including creating Vaults under false or unauthorized entity names; or

(d) Use the Service to facilitate money laundering, wire fraud, mortgage fraud, deed fraud, or any other financial crime.

### 2.2 Intellectual Property and Privacy Violations

(a) Upload or distribute content that infringes any third-party intellectual property rights, including copyrights, trademarks, or trade secrets;

(b) Upload documents containing another person's personally identifiable information without appropriate legal authorization or consent; or

(c) Use the Service to collect or process personal data in violation of applicable U.S. federal or state privacy laws, including the CCPA/CPRA.

**2.3 Security and Technical Violations**

(a) Attempt to gain unauthorized access to any account, Vault, system, or network component of the Service;

(b) Introduce, transmit, or distribute viruses, malware, ransomware, trojans, or any other malicious or harmful code;

(c) Reverse-engineer, decompile, disassemble, or otherwise attempt to derive the source code or underlying algorithms of the Service;

(d) Circumvent, disable, or interfere with any security, authentication, or access-control feature of the Service; or

(e) Use automated bots, crawlers, scrapers, or data extraction tools to access, harvest, or collect data from the Service without the prior written consent of OneEstateOS.

**2.4 Regulated Activities**

(a) Use the Service to provide regulated investment advisory, broker-dealer, mortgage lending, or money transmission services unless you hold all required federal and state licenses and registrations for such activities; or

(b) Use Platform Outputs — including any analyses, reports, or summaries generated by the Service — as the sole or primary basis for providing regulated investment, legal, appraisal, or financial advisory services to third parties.

**2.5 Harmful and Abusive Content**

Transmit, store, or distribute material that is unlawfully obscene, defamatory, threatening, harassing, or abusive toward any individual or group.

---

## 3. USER RESPONSIBILITIES

All Users must:

(a) Maintain the security of their Google account used to authenticate with the Service, including enabling two-factor authentication, and promptly notify OneEstateOS at compliance@oneestateos.com if they believe their account has been compromised;

(b) Ensure that all documents and data uploaded to the Service are accurate to the best of the User's knowledge and comply with applicable laws and any applicable organizational policies;

(c) Maintain appropriate independent backups of any critical documents stored in the Service;

(d) Use the Service only for legitimate business purposes consistent with its nature as a real estate operations and document management platform;

(e) Ensure that all Authorized Users and collaborators added to their account or Vaults have read and agreed to comply with this Policy; and

(f) Promptly revoke access for any Authorized User who no longer requires it or whose authorization has been withdrawn.

### 3.1 Collaborator and Authorized User Obligations

Account holders are solely responsible for the conduct of all Authorized Users and collaborators granted access to their Vaults, regardless of whether the account holder directed or was aware of such conduct. When inviting collaborators — including attorneys, lenders, title agents, property managers, or any other third party — the account holder represents that such persons are authorized to access the relevant documents and data, and that their access complies with all applicable laws and contractual obligations.

### 3.2 Document Authenticity

Users represent and warrant that all documents uploaded to the Service are genuine, unaltered originals or authorized copies, unless explicitly noted otherwise in the document record. Uploading falsified, forged, or materially altered legal instruments — including but not limited to deeds, mortgage documents, operating agreements, or purchase contracts — is a material violation of this Policy and may constitute a criminal offense under applicable federal and state law.

---

## 4. COMPLIANCE WITH LAW

All Users shall comply with all applicable U.S. federal and state laws in connection with their use of the Service, including without limitation:

(a) U.S. Securities Act of 1933, as amended, and the Securities Exchange Act of 1934, as amended, to the extent applicable to fund formation and investor activities;

(b) Anti-Money Laundering (AML) regulations and Bank Secrecy Act requirements, where applicable;

(c) U.S. federal and state data privacy laws, including the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA);

(d) Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030;

(e) FinCEN Beneficial Ownership reporting requirements under the Corporate Transparency Act (CTA), where applicable; and

(f) All applicable U.S. export control laws and sanctions programs administered by OFAC.

---

## 5. INVESTMENT AND FINANCIAL DISCLAIMER

The Service is provided solely as a technology, workflow, and document management platform. OneEstateOS does not:

(a) provide investment advice or recommendations regarding any real estate asset, security, or investment opportunity;

(b) act as a registered investment adviser under the Investment Advisers Act of 1940;

(c) act as a broker-dealer under the Securities Exchange Act of 1934;

(d) provide licensed real property appraisal services;

(e) provide legal, tax, or accounting advice; or

(f) accept, hold, transmit, or manage customer funds or investor capital.

All investment-related activities, financial transactions, legal filings, and professional advisory functions related to User's real estate operations must be executed solely by duly licensed entities or advisors, independent of the platform. Users are solely responsible for all decisions made in connection with their use of the Service.

---

## 6. ENFORCEMENT

OneEstateOS reserves the right to investigate any suspected violation of this Policy. Upon determining that a violation has occurred or is reasonably likely to have occurred, OneEstateOS may:

(a) provide written notice and a reasonable opportunity to cure for minor violations that do not pose a security or legal risk;

(b) immediately suspend or terminate access to the Service for serious violations, including violations that threaten platform security, involve fraudulent or illegal activity, or cause harm to other Users or third parties;

(c) preserve and retain evidence of the alleged violation; and

(d) cooperate with law enforcement and regulatory authorities as required by applicable law.

Enforcement actions are in addition to, and not in lieu of, any other rights or remedies available to OneEstateOS under these Terms, applicable law, or in equity.

---

## 7. REPORTING VIOLATIONS

Users who become aware of any violation of this Policy, suspected security incident, or unauthorized use of the Service should report such activity promptly to:

Email: compliance@oneestateos.com

Subject Line: "AUP Violation Report"

OneEstateOS's Compliance Team will acknowledge receipt within two (2) business days and investigate promptly. All reports are treated as confidential to the extent permitted by applicable law.

## 8. UPDATES TO THIS POLICY

OneEstateOS may update this Policy from time to time to reflect legal, regulatory, or operational changes. OneEstateOS will notify Users of updates via email and through the Service interface. For updates that constitute Material Changes (as defined in the Terms of Service), affirmative re-acceptance will be required through the platform's disclosure acceptance mechanism before continued use of the Service. For non-material updates, continued use of the Service after the effective date of the update constitutes acceptance.

---

## 9. GOVERNING LAW

This Policy shall be governed by and construed in accordance with the laws of the State of Delaware, without regard to conflicts of law principles, consistent with the Terms of Service.

---

## 10. CONTACT INFORMATION

One Estate, Inc.

9169 W State Street #1121

Garden City, ID 83714

Email: compliance@oneestateos.com

---

## ACKNOWLEDGMENT

By accessing or using the OneEstateOS platform, you acknowledge that you have read, understood, and agree to comply with this Acceptable Use Policy. A timestamped record of your acceptance, including the document version hash, is stored in your account footprint.

*— END OF ACCEPTABLE USE POLICY —*