



WORKS TECH
CAPITAL INTERNATIONAL L.L.C.

ACCEPTABLE USE POLICY

WORKS TECH CAPITAL
INTERNATIONAL L.L.C.

Last Updated:
September 7, 2026





ACCEPTABLE USE POLICY

- WORKS TECH CAPITAL INTERNATIONAL L.L.C.
- Last Updated: September 7, 2026

❖ Table of Contents

No.	Section
1	Introduction
2	Scope of this Policy
3	General Acceptable Use Principles
4	Lawful Use
5	Prohibited Content
6	Prohibited Activities
7	Security, Abuse & Unauthorized Access
8	Malware, Harmful Code & Technical Misuse
9	Fraud, Misrepresentation & Impersonation
10	Intellectual Property & Third-Party Rights
11	Privacy, Data & Confidential Information
12	Communications, Messaging & Spam
13	Automated Access, Scraping & Bots
14	Platform, Infrastructure & Resource Abuse
15	High-Risk, Restricted & Regulated Uses
16	Third-Party Services & External Platforms
17	User Responsibility
18	Monitoring, Investigation & Enforcement
19	Suspension, Restriction & Termination
20	Reporting Violations
21	Changes to this Policy
22	Languages & Governing Version
23	Contact Us



1. Introduction

This Acceptable Use Policy (“Policy”) sets out the rules and standards governing the acceptable use of the websites, digital services, systems, platforms, applications, communications channels, technical resources, and other digital or technology-related services provided, operated, managed, or made available by **WORKS TECH CAPITAL INTERNATIONAL L.L.C.** (“WORKS”, “we”, “us”, or “our”).

This Policy is intended to protect WORKS, its clients, users, partners, systems, infrastructure, data, intellectual property, and legitimate business interests from misuse, unlawful activity, security threats, abuse, and other inappropriate conduct.

By accessing or using any WORKS website, digital service, platform, system, application, communication channel, or technical resource, you agree to comply with this Policy together with any applicable contractual terms, service conditions, security requirements, and legal obligations.

This Policy should be read together with our **Terms of Business & Website Use**, **Privacy Policy**, and any other policies, notices, agreements, or service-specific rules applicable to the relevant use.

2. Scope of this Policy

This Policy applies to the use of any website, digital service, platform, application, system, account, communication channel, technical resource, hosted environment, software-enabled service, or other technology resource provided, operated, managed, or made available by **WORKS TECH CAPITAL INTERNATIONAL L.L.C.**

It applies, where relevant, to:

- website visitors and users;
- clients and prospective clients;
- authorized users of WORKS services, systems, or platforms;
- contractors, consultants, suppliers, partners, and other third parties with access to WORKS resources;
- users accessing services through accounts, credentials, integrations, APIs, or other technical interfaces; and
- any other person or organization using or interacting with WORKS digital or technical resources.

This Policy applies together with any applicable agreement, licence, subscription, statement of work, service terms, security requirements, technical documentation, or other service-specific conditions.

Where a specific service or contract contains stricter or more detailed acceptable-use requirements, those requirements will apply to the relevant service or engagement.



3. General Acceptable Use Principles

Users must use **WORKS TECH CAPITAL INTERNATIONAL L.L.C.** websites, systems, platforms, services, and technical resources responsibly, lawfully, securely, and in a manner consistent with their intended purpose.

Use must not:

- violate applicable law, regulation, contractual obligations, or third-party rights;
- compromise the security, integrity, availability, performance, or reliability of WORKS systems or services;
- interfere with or disrupt the use of WORKS resources by other users;
- expose WORKS, its clients, users, partners, systems, or data to unreasonable legal, security, operational, reputational, or compliance risk;
- misuse access rights, credentials, technical capabilities, data, or resources provided in connection with a service or engagement; or
- use WORKS resources for deceptive, abusive, harmful, fraudulent, unlawful, or otherwise inappropriate purposes.

Users must act in good faith and take reasonable steps to protect accounts, credentials, devices, data, and access methods used in connection with WORKS services.

Where WORKS provides service-specific instructions, security controls, technical limits, or usage requirements, users must comply with those requirements as part of acceptable use.

4. Lawful Use

All use of **WORKS TECH CAPITAL INTERNATIONAL L.L.C.** websites, systems, platforms, services, applications, communication channels, and technical resources must comply with applicable laws, regulations, contractual obligations, and lawful instructions.

Users must not use WORKS resources to:

- engage in, facilitate, promote, or support unlawful activity;
- violate sanctions, export-control, trade, financial, privacy, data protection, intellectual property, cybersecurity, communications, or other applicable legal requirements;
- obtain, access, use, disclose, transfer, or distribute information, data, software, content, or technology unlawfully;
- evade, circumvent, disable, or interfere with legal, regulatory, contractual, security, or technical restrictions;
- assist another person or organization in carrying out unlawful or prohibited conduct; or
- use any WORKS service or resource in a manner that would cause WORKS to violate applicable law or expose the Company to unlawful conduct or regulatory action.



Users are responsible for ensuring that their use of WORKS resources is lawful in the jurisdictions relevant to their activities.

Where the legality of a proposed use is uncertain, WORKS may require clarification, additional information, authorization, or other reasonable evidence before allowing or continuing the relevant use.

5. Prohibited Content

Users must not use **WORKS TECH CAPITAL INTERNATIONAL L.L.C.** websites, systems, platforms, services, or technical resources to create, upload, transmit, store, publish, distribute, promote, or facilitate content that is unlawful, harmful, abusive, deceptive, infringing, or otherwise prohibited.

Prohibited content may include:

- content that violates applicable law or regulation;
- fraudulent, deceptive, misleading, or impersonating content;
- content that infringes intellectual property, privacy, confidentiality, contractual, or other third-party rights;
- content containing malware, malicious code, harmful files, or other technical threats;
- content intended to facilitate unauthorized access, cyber abuse, fraud, or other unlawful conduct;
- unlawful discriminatory, threatening, harassing, defamatory, or abusive content;
- content that unlawfully exposes, exploits, or misuses personal, confidential, sensitive, or protected information;
- content that promotes or facilitates prohibited, restricted, or unlawfully regulated activities; and
- any other content that may materially compromise the security, integrity, lawful operation, rights, or legitimate interests of WORKS, its clients, users, partners, or third parties.

WORKS may restrict, remove, block, or require the removal of prohibited content where reasonably necessary and permitted by applicable law or the relevant contractual terms.

6. Prohibited Activities

Users must not use **WORKS TECH CAPITAL INTERNATIONAL L.L.C.** websites, systems, platforms, services, applications, communication channels, or technical resources to engage in, facilitate, or support activities that are unlawful, abusive, deceptive, disruptive, harmful, or otherwise prohibited.

Prohibited activities include:



- attempting to gain unauthorized access to accounts, systems, networks, applications, data, credentials, or technical resources;
- bypassing, disabling, defeating, or interfering with authentication, access controls, security measures, technical restrictions, rate limits, or monitoring mechanisms;
- scanning, probing, testing, exploiting, or attempting to exploit vulnerabilities without explicit authorization;
- disrupting, degrading, overloading, damaging, or interfering with the availability, performance, or operation of any system, service, network, or infrastructure;
- using WORKS resources to conduct fraud, phishing, impersonation, social engineering, deceptive practices, or other unlawful schemes;
- transmitting, distributing, or facilitating malware, malicious code, ransomware, spyware, harmful scripts, or other destructive or intrusive technologies;
- collecting, extracting, harvesting, scraping, or using data in an unauthorized, unlawful, excessive, or abusive manner;
- sending unsolicited, deceptive, abusive, or unlawful communications;
- infringing intellectual property, privacy, confidentiality, contractual, or other rights;
- circumventing payment, licensing, subscription, usage, access, or technical restrictions;
- using WORKS resources to conceal, facilitate, or support prohibited conduct by another person or organization; and
- engaging in any activity that may materially harm WORKS, its clients, users, partners, systems, reputation, legal position, or legitimate business interests.

WORKS may take reasonable technical, contractual, administrative, or other measures to prevent, investigate, restrict, or stop prohibited activities in accordance with this Policy, applicable agreements, and applicable law.

7. Security, Abuse & Unauthorized Access

Users must not attempt to compromise, bypass, interfere with, or misuse the security, integrity, availability, or access controls of any website, system, platform, application, network, account, data environment, or technical resource operated or made available by **WORKS TECH CAPITAL INTERNATIONAL L.L.C.**

Prohibited conduct includes:

- accessing or attempting to access accounts, systems, data, credentials, or resources without authorization;
- using another person's credentials, account, token, key, or access rights without permission;
- attempting to bypass authentication, multi-factor authentication, access controls, security restrictions, rate limits, or other protective measures;
- probing, scanning, testing, exploiting, or attempting to exploit vulnerabilities without explicit authorization;



- interfering with logging, monitoring, detection, alerting, or other security controls;
- attempting to obtain elevated privileges or unauthorized administrative access;
- disrupting or attempting to disrupt the confidentiality, integrity, availability, or performance of systems, services, or data; and
- encouraging, assisting, or enabling another person or organization to engage in unauthorized access or security abuse.

Users must promptly notify WORKS if they become aware of suspected unauthorized access, compromised credentials, security weaknesses, misuse, or other incidents that may affect WORKS systems, services, data, or users.

WORKS may restrict or suspend access, reset credentials, isolate systems, preserve relevant records, or take other reasonable protective measures where necessary to investigate, contain, or respond to actual or suspected security incidents or abuse.

8. Malware, Harmful Code & Technical Misuse

Users must not use **WORKS TECH CAPITAL INTERNATIONAL L.L.C.** websites, systems, platforms, applications, services, networks, or technical resources to create, upload, introduce, transmit, execute, distribute, host, or facilitate malware, harmful code, destructive software, or other malicious or disruptive technologies.

Prohibited conduct includes:

- introducing viruses, worms, trojans, ransomware, spyware, rootkits, keyloggers, malicious scripts, or similar harmful code;
- deploying code or tools designed to damage, disable, disrupt, corrupt, alter, intercept, or interfere with systems, networks, devices, data, or communications;
- using exploits, payloads, scripts, or automation for unauthorized technical activity;
- attempting to bypass, disable, or interfere with security controls, malware protections, monitoring, logging, or technical safeguards;
- using WORKS infrastructure or services to distribute, host, command, control, or support malicious software or harmful technical activity;
- causing excessive, abusive, or unauthorized consumption of computing, bandwidth, storage, processing, or other technical resources; and
- conducting any technical activity that materially compromises the confidentiality, integrity, availability, stability, or lawful operation of WORKS systems or services.

Security testing, vulnerability assessment, penetration testing, scanning, or similar technical activity may only be conducted where expressly authorized by WORKS and within the approved scope, methods, timing, and conditions.



WORKS may block, isolate, remove, disable, suspend, or otherwise contain harmful code, malicious activity, compromised resources, or related access where reasonably necessary to protect its systems, users, data, or services.

9. Fraud, Misrepresentation & Impersonation

Users must not use **WORKS TECH CAPITAL INTERNATIONAL L.L.C.** websites, systems, platforms, services, applications, communication channels, or technical resources to engage in fraud, deception, misrepresentation, impersonation, or other misleading conduct.

Prohibited conduct includes:

- impersonating another person, company, organization, employee, representative, client, authority, or service provider;
- creating, using, or presenting false, misleading, forged, altered, or unauthorized identities, documents, credentials, accounts, records, or communications;
- making false or misleading statements regarding affiliation, authority, ownership, qualifications, approvals, licences, certifications, products, services, transactions, or business relationships;
- using WORKS resources to conduct phishing, social engineering, credential theft, payment fraud, identity theft, or other deceptive schemes;
- submitting false or misleading information in connection with registrations, enquiries, orders, payments, verifications, projects, or services;
- disguising the origin, destination, ownership, purpose, or nature of communications, transactions, data, or activity in order to mislead others or evade controls; and
- using the name, identity, branding, systems, or communications of WORKS in a way that falsely suggests authorization, endorsement, representation, partnership, or affiliation.

Users must ensure that information they provide to WORKS and to other parties through WORKS services is accurate, truthful, and not misleading in any material respect.

WORKS may suspend access, preserve relevant records, reject transactions or requests, require additional verification, or take other reasonable measures where fraud, impersonation, misrepresentation, or related abuse is suspected.



10. Intellectual Property & Third-Party Rights

Users must respect the intellectual property, proprietary, contractual, privacy, confidentiality, and other lawful rights of **WORKS TECH CAPITAL INTERNATIONAL L.L.C.** and all third parties.

Users must not:

- copy, reproduce, modify, distribute, publish, display, transmit, license, sell, commercially exploit, or otherwise use protected content, software, data, trademarks, logos, designs, documents, code, methodologies, or other proprietary materials without appropriate authorization;
- remove, alter, conceal, or interfere with copyright notices, trademarks, proprietary legends, digital rights controls, licence notices, attribution requirements, or other rights-management information;
- upload, submit, store, transmit, distribute, or use materials that infringe or misappropriate intellectual property or other proprietary rights;
- use third-party content, software, data, APIs, platforms, licences, or technologies in a manner inconsistent with the applicable permissions, terms, or restrictions;
- represent WORKS or third-party intellectual property as owned by, created by, licensed to, or authorized for another person where that is not true; or
- use WORKS resources to facilitate infringement, counterfeiting, unauthorized distribution, piracy, or other unlawful exploitation of intellectual property.

Users are responsible for ensuring that they have the necessary rights, licences, consents, and permissions for any content, data, software, materials, or technologies they provide, upload, integrate, or authorize for use through WORKS services.

Where WORKS receives a credible allegation of infringement or misuse of intellectual property or other third-party rights, it may investigate, restrict access, remove or disable relevant materials, preserve records, or take other reasonable action consistent with applicable law and contractual requirements.

11. Privacy, Data & Confidential Information

Users must respect the privacy, confidentiality, data protection, security, and lawful information-handling requirements applicable to **WORKS TECH CAPITAL INTERNATIONAL L.L.C.**, its clients, users, partners, and third parties.

Users must not:

- access, collect, use, copy, disclose, transfer, share, store, or process personal, confidential, proprietary, sensitive, or protected information without appropriate authorization or lawful basis;



- attempt to obtain information through deception, unauthorized access, credential misuse, surveillance, interception, scraping, or other improper means;
- disclose confidential or restricted information to unauthorized persons or use it for purposes unrelated to the authorized service or engagement;
- upload, transmit, or store information in violation of applicable privacy, data protection, confidentiality, contractual, professional, or security requirements;
- use WORKS resources to identify, profile, track, monitor, or target individuals unlawfully or without appropriate authorization;
- expose personal or confidential information through insecure systems, public channels, weak access controls, or other inappropriate handling practices; or
- retain, reproduce, or distribute information beyond what is reasonably necessary or permitted for the relevant purpose.

Users are responsible for ensuring that any personal or confidential information they provide to or process through WORKS services has been obtained and may be used lawfully.

Where WORKS provides specific data-handling, security, confidentiality, retention, access-control, or privacy requirements, users must comply with those requirements.

WORKS may restrict access, require corrective action, preserve records, remove exposed information, or take other reasonable measures where misuse, unauthorized disclosure, or improper handling of personal, confidential, or protected information is suspected.

12. Communications, Messaging & Spam

Users must not use **WORKS TECH CAPITAL INTERNATIONAL L.L.C.** websites, systems, platforms, services, applications, communication channels, or technical resources to send, distribute, facilitate, or support unlawful, deceptive, abusive, unsolicited, or otherwise inappropriate communications.

Prohibited conduct includes:

- sending unsolicited bulk messages, spam, or other communications in violation of applicable law or platform rules;
- sending deceptive, fraudulent, misleading, threatening, harassing, abusive, defamatory, or unlawful messages;
- using false, misleading, forged, or concealed sender identities or contact information;
- conducting phishing, credential harvesting, social engineering, impersonation, or other deceptive communication schemes;
- sending communications to individuals who have opted out or withdrawn consent where applicable law requires such preferences to be honored;
- using automated messaging or mass-distribution tools in an abusive, excessive, unauthorized, or unlawful manner;



- distributing malware, malicious links, harmful attachments, or other dangerous content through communications;
- interfering with or abusing messaging, email, notification, support, or communication systems; and
- using WORKS resources to facilitate communications that violate privacy, data protection, intellectual property, contractual, or other third-party rights.

Users are responsible for ensuring that communications sent through or in connection with WORKS services comply with applicable law, consent requirements, recipient preferences, contractual terms, and relevant platform policies.

WORKS may restrict, suspend, filter, block, or investigate communications where reasonably necessary to prevent spam, fraud, abuse, security threats, unlawful activity, or other violations of this Policy.

13. Automated Access, Scraping & Bots

Users must not use automated tools, bots, crawlers, scrapers, scripts, agents, or other automated methods to access, extract, copy, monitor, interact with, or otherwise use **WORKS TECH CAPITAL INTERNATIONAL L.L.C.** websites, systems, platforms, services, applications, data, or technical resources in an unauthorized, excessive, abusive, or unlawful manner.

Prohibited conduct includes:

- scraping, harvesting, indexing, copying, or extracting website content, data, metadata, contact information, or other information without appropriate authorization;
- using bots, scripts, crawlers, or automated agents to bypass access controls, rate limits, technical restrictions, consent mechanisms, or security measures;
- generating excessive or disruptive automated traffic;
- using automation to create, access, operate, or control accounts in violation of applicable rules or authorization;
- using automated methods to collect personal, confidential, proprietary, restricted, or protected information unlawfully;
- using WORKS content, data, systems, or services to train, test, benchmark, replicate, or develop automated systems where such use is unauthorized or violates applicable rights or terms; and
- using automated access in a manner that interferes with the availability, performance, security, integrity, or lawful operation of WORKS resources.

Automated access may be permitted where expressly authorized by WORKS, provided through an approved API or integration, or otherwise allowed under applicable law and relevant contractual or technical requirements.

WORKS may apply rate limits, access controls, bot detection, traffic filtering, authentication requirements, blocking, or other reasonable technical measures to protect its systems and enforce this Policy.



14. Platform, Infrastructure & Resource Abuse

Users must not use **WORKS TECH CAPITAL INTERNATIONAL L.L.C.** platforms, systems, infrastructure, hosted environments, networks, applications, accounts, storage, computing resources, bandwidth, APIs, or other technical resources in a manner that is excessive, abusive, unauthorized, disruptive, or inconsistent with their intended purpose.

Prohibited conduct includes:

- consuming excessive computing, processing, storage, bandwidth, API, or other technical resources in a manner that materially affects system performance or availability;
- using shared or hosted resources in a way that interferes with other users, clients, services, or workloads;
- attempting to bypass technical quotas, usage limits, resource allocations, licensing restrictions, or service controls;
- using WORKS infrastructure for unauthorized hosting, relay, proxy, tunneling, mining, scanning, traffic generation, or other unapproved technical activity;
- creating unnecessary, abusive, or excessive automated requests, connections, processes, workloads, or transactions;
- using resources for purposes materially different from those agreed, authorized, or technically intended;
- attempting to monopolize, degrade, destabilize, overload, or exhaust shared infrastructure or services; and
- using WORKS resources in a manner that creates unreasonable operational, security, financial, legal, or compliance risk.

Users must comply with any applicable service quotas, technical limits, fair-use rules, subscription conditions, resource allocations, capacity limits, and performance requirements communicated by WORKS.

WORKS may apply usage controls, throttling, rate limits, capacity restrictions, resource isolation, temporary suspension, or other reasonable measures where necessary to protect service stability, security, availability, and fair access.

Where materially excessive or abusive resource consumption results in additional cost, WORKS may address such costs in accordance with the applicable agreement, service terms, or commercial arrangement.



15. High-Risk, Restricted & Regulated Uses

Users must not use **WORKS TECH CAPITAL INTERNATIONAL L.L.C.** websites, systems, platforms, services, applications, infrastructure, data, APIs, or other technical resources for activities that are prohibited by law, subject to legal restriction, or require specific authorization, licensing, registration, professional qualification, or regulatory approval unless all applicable requirements have been satisfied.

Restricted or high-risk uses may include, where applicable:

- regulated financial, investment, payment, lending, securities, insurance, or other financial activities;
- legal, tax, accounting, audit, certification, accreditation, medical, engineering, or other regulated professional services;
- processing, transfer, storage, or use of highly sensitive, confidential, regulated, or protected data;
- activities involving sanctions, export controls, controlled technologies, restricted jurisdictions, or regulated cross-border transfers;
- high-risk artificial intelligence, automated decision-making, biometric, surveillance, identity, or profiling activities;
- services or technologies used in critical infrastructure, safety-critical systems, or other environments where failure could create material harm;
- activities requiring governmental, regulatory, professional, industry, contractual, or third-party approval; and
- any other use that **WORKS** reasonably determines presents material legal, regulatory, security, ethical, operational, reputational, or compliance risk.

Users are responsible for determining whether their proposed use is subject to any licence, approval, registration, qualification, consent, restriction, or other legal or regulatory requirement.

WORKS may require additional information, documentation, due diligence, safeguards, contractual controls, technical restrictions, or proof of authorization before permitting or continuing any restricted, regulated, or high-risk use.

WORKS may refuse, restrict, suspend, or terminate any use that it reasonably determines is unlawful, insufficiently authorized, materially high-risk, or inconsistent with applicable law, regulatory requirements, professional standards, contractual obligations, or this Policy.

16. Third-Party Services & External Platforms

Certain **WORKS TECH CAPITAL INTERNATIONAL L.L.C.** services, systems, platforms, applications, websites, or technical resources may rely on, integrate with, link to, or provide access to third-



party services, platforms, software, infrastructure, APIs, communications tools, payment services, hosting environments, cloud services, or other external resources.

Users must comply with the applicable terms, policies, licence conditions, usage requirements, security rules, and restrictions of the relevant third-party provider when using such services through or in connection with WORKS.

Users must not:

- use third-party services through WORKS in a manner that violates the provider's terms, policies, or applicable law;
- attempt to bypass, interfere with, or misuse third-party security controls, technical limits, licensing conditions, or access restrictions;
- use WORKS integrations or access rights to obtain unauthorized access to third-party systems, data, services, or accounts;
- misrepresent WORKS's relationship with, authority over, ownership of, or endorsement by any third-party provider; or
- use third-party platforms or services in a manner that creates material legal, security, operational, financial, reputational, or compliance risk for WORKS.

WORKS does not control the independent operation, availability, security, policies, decisions, or enforcement actions of third-party providers.

Where a third-party provider restricts, suspends, modifies, or terminates access to its service, WORKS may take corresponding action where necessary to protect the relevant integration, service, system, or engagement.

Nothing in this Policy creates any right to use a third-party service beyond the scope of the permissions, licences, terms, and authorizations granted by the relevant provider.

17. User Responsibility

Users are responsible for their use of **WORKS TECH CAPITAL INTERNATIONAL L.L.C.** websites, systems, platforms, services, applications, accounts, credentials, data, and technical resources.

Users must:

- use WORKS resources only for authorized and legitimate purposes;
- comply with this Policy, applicable agreements, service terms, technical requirements, security instructions, and applicable law;
- protect account credentials, access keys, passwords, authentication methods, devices, and other means of access from unauthorized use;



- ensure that information, content, data, instructions, and materials they provide are accurate, lawful, and appropriately authorized;
- obtain any necessary licences, permissions, consents, registrations, or approvals required for their use of WORKS services;
- take reasonable precautions to prevent misuse, unauthorized access, security incidents, or harm arising from their activity;
- promptly report suspected compromise, misuse, security incidents, policy violations, or unauthorized activity; and
- cooperate reasonably with WORKS where investigation, verification, remediation, or corrective action is required.

Users are responsible for activities carried out through their accounts, credentials, systems, or authorized access to the extent permitted by applicable law and the relevant contractual arrangements.

Failure to comply with these responsibilities may result in restrictions, suspension, termination, corrective action, or other measures under this Policy, the applicable agreement, or applicable law.

18. Monitoring, Investigation & Enforcement

WORKS TECH CAPITAL INTERNATIONAL L.L.C. may monitor the use of its websites, systems, platforms, services, applications, accounts, networks, and technical resources to the extent reasonably necessary for security, operational integrity, compliance, abuse prevention, service management, and enforcement of this Policy.

Where WORKS reasonably suspects misuse, unlawful activity, security incidents, policy violations, fraud, abuse, or other prohibited conduct, it may investigate the relevant activity and review information reasonably necessary for that purpose.

Such measures may include:

- reviewing logs, access records, technical events, usage patterns, alerts, and related system information;
- requesting additional information, clarification, verification, or documentation from the relevant user;
- preserving relevant records or evidence;
- restricting, filtering, blocking, or isolating suspicious activity, content, accounts, connections, or resources;
- requiring corrective or remedial action;
- cooperating with service providers, professional advisers, competent authorities, or other authorized parties where appropriate or legally required; and
- taking other reasonable technical, administrative, contractual, or legal measures to protect WORKS, its users, systems, data, rights, and legitimate interests.



Any monitoring or investigation will be conducted subject to applicable law, contractual obligations, privacy requirements, and the nature of the relevant service or incident.

WORKS may enforce this Policy through warnings, restrictions, suspension, termination, removal of access, corrective measures, or other appropriate action proportionate to the nature and seriousness of the violation.

19. Suspension, Restriction & Termination

WORKS TECH CAPITAL INTERNATIONAL L.L.C. may suspend, restrict, limit, disable, or terminate access to any website, system, platform, service, application, account, integration, API, communication channel, or technical resource where reasonably necessary to protect its systems, users, data, services, rights, or legitimate business interests.

Such action may be taken where:

- this Policy, an applicable agreement, service term, security requirement, or legal obligation has been materially breached;
- unlawful, abusive, fraudulent, deceptive, harmful, or unauthorized activity is suspected or identified;
- a security incident, compromised account, malware, technical misuse, or other threat creates material risk;
- continued access may expose WORKS, its clients, users, partners, systems, or data to legal, regulatory, operational, financial, security, reputational, or compliance risk;
- required verification, authorization, payment, cooperation, or corrective action has not been completed;
- a relevant third-party provider, platform, licence, authorization, or technical dependency has been restricted, withdrawn, or terminated; or
- immediate action is otherwise reasonably necessary to prevent harm, preserve evidence, maintain service integrity, or comply with applicable law.

Where reasonably practicable, WORKS may provide notice, explanation, or an opportunity to remedy the issue before taking restrictive action, unless immediate action is required for legal, security, operational, risk, or other legitimate reasons.

The duration and scope of any restriction, suspension, or termination will depend on the nature, severity, and circumstances of the issue and may continue until the relevant concern has been resolved to WORKS's reasonable satisfaction.

Any contractual, financial, confidentiality, intellectual property, data protection, or other obligations that by their nature survive suspension or termination will remain in effect in accordance with the applicable agreement and law.



20. Reporting Violations

Users who become aware of suspected misuse, unlawful activity, security incidents, fraud, abuse, prohibited content, unauthorized access, intellectual property infringement, privacy violations, or other conduct that may breach this Policy should report the matter to **WORKS TECH CAPITAL INTERNATIONAL L.L.C.** as soon as reasonably possible.

A report should, where available, include sufficient information to help WORKS understand and assess the issue, such as:

- a description of the suspected violation;
- the relevant website, system, platform, service, account, or resource;
- dates, times, references, usernames, account details, or transaction information, where applicable;
- supporting screenshots, messages, logs, documents, or other evidence, where lawfully available; and
- the reporter's contact details, where appropriate.

Reports should be made in good faith and should not knowingly contain false, misleading, or malicious allegations.

WORKS may review, investigate, preserve relevant records, request additional information, restrict access, take corrective action, notify affected parties, or cooperate with competent authorities or service providers where appropriate and permitted by law.

Reporting a concern does not guarantee a particular outcome, but WORKS will seek to assess credible reports in a manner appropriate to the nature and seriousness of the issue.

21. Changes to this Policy

WORKS TECH CAPITAL INTERNATIONAL L.L.C. may update this Acceptable Use Policy from time to time to reflect changes in its websites, systems, platforms, services, technologies, security requirements, business practices, legal or regulatory obligations, or risk-management needs.

The latest version of this Policy will be published on the WORKS website and identified by the applicable **Last Updated** date.

Any changes will apply from the date they are published or from any later effective date expressly stated.

Where a material change affects the permitted or prohibited use of a service, platform, system, or technical resource, WORKS may provide additional notice where appropriate or required by applicable law or contractual arrangements.



22. Languages & Governing Version

This Acceptable Use Policy is published in English as the official and governing reference version of **WORKS TECH CAPITAL INTERNATIONAL L.L.C.**

An Arabic version, and any other translations that may be made available, are provided for convenience, accessibility, and communication purposes.

In the event of any inconsistency, ambiguity, or difference of interpretation between the English version and any translation, the English version shall prevail, unless otherwise required by applicable law or expressly agreed in writing.

Where any service-specific acceptable-use terms, technical rules, security requirements, notices, or related documents are issued in more than one language, the governing language shall be determined by the relevant document, agreement, or applicable legal requirement.

23. Contact Us

If you have any questions about this Acceptable Use Policy, wish to report suspected misuse or a violation, or need clarification regarding the permitted use of any **WORKS TECH CAPITAL INTERNATIONAL L.L.C.** website, system, platform, service, application, communication channel, or technical resource, please contact us through the following authorized channels:

WORKS TECH CAPITAL INTERNATIONAL L.L.C.

30 N Gould St Ste N
Sheridan, WY 82801
United States of America

Email: info@workstechcapital.com

Telephone / WhatsApp: +1 (307) 533-0882

Fax: +1 (307) 466-7144

Website: www.workstechcapital.com

Unified Electronic Window: www.workstechcapital.com/qr/

Please include sufficient information to help us identify the relevant service, system, account, activity, incident, or suspected violation and respond appropriately.