1290 WORLD LLC | TWELVE NINETY CONNECTIONS

TNC Security & Acceptable Use Terms

Version 1.3

Document ID: TNC-SECURITY-ACCEPTABLE-USE-2026-08-23-002
Entity: 1290 World LLC, acting through 1290 World Connections and publicly known as Twelve Ninety Connections ("TNC")
Audience: All persons accessing TNC systems, data, communications, files, or functions
Effective Date: The date this version is accepted for a new account.
Prior versions: This version applies to new acceptances. Earlier accepted versions, signed copies, decisions, and receipts remain valid and retrievable.

1. PURPOSE, SCOPE, AND INCORPORATION

These TNC Security & Acceptable Use Terms ("Security Terms") establish security responsibilities and prohibited conduct for TNC public websites, T.E.A., accounts, Network Portals, community functions, files, communications, APIs, integrations, payment interfaces, devices, and other TNC-controlled or TNC-connected systems.

These Security Terms supplement the TNC Ecosystem Participation Terms & Conditions, Account & Platform Terms, Privacy Notice, Communications Notice, applicable Network terms, and action-specific instruments.

The Integrated TNC Platform is the single end-to-end TNC-controlled system through which public and authenticated interactions are delivered and administered. The Website, public pages, forms, T.E.A., and authenticated portal interfaces are its public-facing frontend. The governed private CRM backend is its administrative, workflow, record, permission, audit, and command surface. The two surfaces are not separate providers or separate participant relationships. A person receives only the access authorized for that person; public interaction never grants backend access.

2. SECURITY GOVERNANCE AND CONTROL

TNC retains administrative and governance control over the integrated platform and private backend. Privileged access must be restricted to authorized persons, logged where appropriate, protected by strong authentication, reviewed, and revoked when no longer required.

Security controls should be risk-based and aligned with recognized practices such as the NIST Cybersecurity Framework 2.0, while remaining proportionate to TNC's actual systems, data, providers, contracts, and operations.

A policy statement is not proof that a control is implemented. TNC must not claim a certification, encryption property, monitoring capability, backup state, or security guarantee that has not been implemented and tested.

3. SHARED RESPONSIBILITY

TNC is responsible for controls within its authority. Participants are responsible for protecting their credentials, devices, contact methods, local copies, authorized users, instructions, and use of TNC information.

An organization must promptly update administrators, users, roles, departures, compromised devices, and revoked authority. A Participant must report suspected compromise, phishing, misdirected data, unauthorized access, or other security concern without unreasonable delay.

4. IDENTITY, AUTHENTICATION, AND CREDENTIALS

Participants must use accurate identity and authority information and only the Account, role, device, and permission assigned to them.

Passwords, passkeys, authentication codes, recovery codes, API keys, tokens, secrets, session cookies, and credentials must be protected and must not be shared except through an approved delegated-access method that preserves individual accountability.

TNC may require multi-factor authentication, passkeys, reauthentication, device verification, session termination, credential rotation, step-up verification, or manual review based on risk.

5. LEAST PRIVILEGE AND RELATIONSHIP COMPARTMENTATION

Access is limited by identity, organization, Network, Relationship Chapter, role, matter, search, Candidate, Client, Partner, service, Circle, Room, Event, document, communication, payment function, confidentiality, audience, consent, and current authorization.

A senior title, organization ownership, administrator role, Executive or Influencer classification, membership, Investor Relationship, Enterprise relationship, payment, prior access, or technical availability does not authorize unrestricted access.

Participants must not use information from one Relationship Chapter for another purpose merely because they can see or infer it.

6. PRIVATE-ACCOUNT NON-ENUMERATION

A person must not probe, enumerate, infer, confirm, or disclose whether another person or organization has a private Account, Client relationship, administrator, workspace, search, Candidate, document, billing record, communication, or other restricted state.

TNC may use neutral responses, consistent timing, generic errors, step-up verification, rate limits, manual review, and fail-closed routing to prevent disclosure through account recovery, organization resolution, invitation, search, route, support, or error behavior.

7. AUTHORIZED USE

TNC systems may be used only for lawful purposes within the Participant's current identity, relationship, role, scope, and permission. A Participant must follow the applicable terms, instructions, laws, confidentiality, privacy, communications, recording, intellectual-property, and security requirements.

Use that is technically possible but not authorized remains prohibited.

8. PROHIBITED ACCESS AND CIRCUMVENTION

A Participant may not:

- obtain or attempt unauthorized access to an Account, organization, Network, Relationship Chapter, matter, record, system, provider, administrative function, or backend;
- bypass authentication, identity proofing, authorization, payment, rate limits, message limits, moderation, blocks, safety controls, approval gates, or receipts;
- share credentials, impersonate, falsify authority, create deceptive Accounts, or evade a restriction, suspension, revocation, or legal obligation;
- use another person's session, device, invitation, recovery method, or organization relationship without authorization; or
- exploit a defect, race condition, stale response, cache error, same-name collision, provider failure, or interface inconsistency to obtain or change a state.

9. SCRAPING, AUTOMATION, EXPORT, AND DATA MISUSE

Without express written authorization, a Participant may not scrape, crawl, spider, enumerate, mirror, bulk extract, download, export, republish, sell, lease, enrich, correlate, or create an unrelated database, contact list, surveillance product, model-training set, or competing service from TNC or Participant information.

Automation must use an approved interface, purpose, identity, rate, scope, data set, and action. Bots, agents, scripts, browser automation, and integrations may not create cold bulk outreach, evade controls, impersonate a person, or take consequential action without required authorization.

An authorized export remains subject to confidentiality, purpose, retention, deletion, and security obligations.

10. MALWARE, INTERFERENCE, AND ABUSE

Participants must not introduce malware, ransomware, spyware, destructive code, credential-harvesting content, malicious files, denial-of-service traffic, or other harmful material; interfere with availability or integrity; or use TNC systems to attack, scan, exploit, or disrupt another system.

Harassment, threats, stalking, trafficking, exploitation, fraud, unlawful discrimination, sanctions evasion, spam, deception, extortion, and abuse of messaging, introductions, Events, or community functions are prohibited.

11. SOCIAL ENGINEERING, PHISHING, AND IMPERSONATION

A Participant must not impersonate TNC, T.E.A., a Client, Candidate, Partner, organization, administrator, payment provider, government, or another person; create misleading login or payment pages; or solicit credentials, secrets, full payment-card data, or sensitive information through an unapproved method.

Unexpected payment, access, signing, urgent-data, or credential requests should be verified through an established TNC channel.

12. DATA CLASSIFICATION AND HANDLING

TNC and Participants must handle information according to its relationship, purpose, source, audience, confidentiality, sensitivity, legal requirement, and current authorization.

Credentials, secrets, private keys, raw authentication data, full payment-card information, government identifiers, medical information, biometric information, and other restricted data must not be submitted through ordinary fields or messages unless specifically requested through an approved secure process.

Copies, downloads, screenshots, printouts, recordings, exports, and backups must receive protection appropriate to the source data.

13. FILES, UPLOADS, DOWNLOADS, AND LINKS

A Participant must have authority to upload or share a file and must not submit malicious, unlawful, infringing, deceptive, excessively sensitive, or unrelated material.

TNC may scan, quarantine, restrict, reject, sanitize, redact, transcode, or preserve a file for security, privacy, compatibility, legal, evidence, or operational reasons.

A file name, extension, preview, link, hash, or successful upload state does not prove that the file is safe, authorized, complete, or approved for use.

14. APIS, INTEGRATIONS, PROVIDERS, AND SECRETS

API and integration access requires approved identity, scope, environment, purpose, permissions, credentials, rate limits, logging, provider terms, security review, and action authority.

API keys, provider credentials, tokens, secrets, connection strings, and private endpoints must remain server-side or in an approved secret-management system. They must not appear in client bundles, browser storage, HTML, screenshots, ordinary logs, prompts, public documents, or receipts.

A connected provider does not authorize every provider capability, production write, deletion, export, model, sender identity, campaign, data set, or environment.

15. VULNERABILITY RESEARCH AND REPORTING

Security testing, scanning, penetration testing, reverse engineering, load testing, or vulnerability validation requires prior written authorization defining the systems, methods, accounts, dates, data handling, stop conditions, reporting method, and prohibited actions.

A good-faith researcher should report a suspected vulnerability through the designated security method and avoid accessing unnecessary data, changing records, establishing persistence, disrupting service, extorting TNC, publicly disclosing before remediation coordination, or testing third-party systems without permission.

TNC may publish a separate vulnerability-disclosure or safe-harbor policy. No safe harbor is implied beyond its exact scope.

16. MONITORING, LOGGING, AND AUDIT

TNC may monitor and preserve access, authentication, security, device, network, file, communication, moderation, agreement, payment-reference, and activity evidence as disclosed and reasonably necessary for security, fraud prevention, quality, legal compliance, audit, disputes, and relationship continuity.

Monitoring must remain purpose-limited and access-controlled. Security evidence is not a general license to inspect private content for unrelated purposes.

Logs, alerts, and automated classifications may be incomplete or wrong and require review proportionate to the consequence.

17. INCIDENT RESPONSE AND COOPERATION

TNC may investigate, contain, restrict, suspend, revoke, reset, preserve, recover, notify, remediate, and coordinate in response to suspected compromise, misuse, data loss, fraud, abuse, or other incident.

Participants and organizations must reasonably cooperate, preserve relevant evidence, stop ongoing misuse, reset credentials, confirm affected access, and provide accurate information. Cooperation does not require waiver of legal rights or disclosure beyond what is lawfully required.

TNC will provide legally required incident notices and must not represent an unverified event as a confirmed breach.

18. BACKUP, RECOVERY, AND BUSINESS CONTINUITY

TNC should maintain backup, recovery, continuity, and rollback controls appropriate to the system and data. Backups must be protected, tested, retained, and deleted according to the applicable policy and legal holds.

A backup is not a substitute for a current source record, accepted copy, receipt, financial authority, or validated relationship state.

19. ENCRYPTION AND SECURITY REPRESENTATIONS

TNC may use encryption in transit and at rest where supported and appropriate. No Participant-facing material may claim end-to-end encryption, zero knowledge, perfect security, unbreakable protection, or another technical property unless the released design actually provides and has tested that property.

The integrated platform may process content needed to provide the service, apply permissions, support T.E.A., preserve records, and comply with law. That capability must not be mislabeled as cryptographic end-to-end encryption.

20. DEVICES, REMOTE ACCESS, AND PHYSICAL SECURITY

Participants must use reasonable device security, supported software, screen locks, updates, malware protection, secure networks, and appropriate privacy when accessing confidential information.

Shared, public, or unmanaged devices should not be used for sensitive functions unless the risk is appropriately controlled. Participants must sign out, protect local downloads, and promptly report lost or transferred devices.

21. T.E.A. AND AUTOMATED SECURITY SUPPORT

T.E.A. may help identify suspicious patterns, missing authority, unsafe content, duplicate records, policy conflicts, or recommended security actions. T.E.A. may not independently accuse a person, make a final legal finding, create access, disclose restricted information, or take another consequential action without the required authority and review.

Automated detection may generate false positives and false negatives. High-impact enforcement requires appropriate human or organizational review unless immediate temporary restriction is reasonably necessary to protect safety or security.

22. SUSPENSION, TERMINATION, AND EVIDENCE PRESERVATION

TNC may limit or suspend a function, session, credential, Account, integration, content item, export, message, or relationship in response to security, legal, contractual, payment, authority, privacy, safety, or integrity risk.

TNC may preserve relevant evidence and impose a legal hold. Suspension or termination does not erase accepted agreements, payment obligations, confidentiality, audit records, security evidence, or other surviving duties.

23. NO SECURITY GUARANTEE

No system is perfectly secure or continuously available. TNC does not guarantee that every threat, error, unauthorized action, provider failure, or loss will be prevented or detected.

TNC does not disclaim security, privacy, notification, accessibility, or other duties that cannot lawfully be disclaimed.

24. CHANGES AND GOVERNING LAW

Material changes require versioning and notice or reacceptance as applicable. Prior acknowledgments, incidents, restrictions, accepted copies, and receipts remain preserved.

Kansas law governs unless a controlling instrument or mandatory law lawfully provides otherwise. Exclusive venue lies in the state or federal courts serving Sedgwick County, Kansas.

The public Security Terms do not disclose confidential system diagrams, provider secrets, detection thresholds, exploit details, credentials, or information that would materially weaken security.

CONTACT

Questions or requests may be submitted through the applicable authenticated portal or to tsullivan@1290worldconnections.com. Office: (316) 365-5546. Direct: (316) 374-4159.

CONTACT

Questions may be submitted through the applicable authenticated portal or to tsullivan@1290worldconnections.com. Office: (316) 365-5546. Direct: (316) 374-4159.