



1290 WORLD LLC | TWELVE NINETY CONNECTIONS

TNC Account & Platform Terms

Version 1.3

Document ID: TNC-ACCOUNT-PLATFORM-2026-08-23-002

Entity: 1290 World LLC, acting through 1290 World Connections and publicly known as Twelve Ninety Connections ("TNC")

Audience: Public-site visitors, account holders, authorized organization users, portal users, and other platform participants

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 Account & Platform Terms ("Account Terms") govern access to and use of the Integrated TNC Platform, including TNC public websites and pages, T.E.A., authenticated accounts, Network Portals, organization workspaces, community functions, communications interfaces, document and file workflows, payment and service interfaces, the private governed CRM backend, and other TNC-controlled digital functions.

These Account Terms are part of the universal TNC legal package and supplement the TNC Ecosystem Participation Terms & Conditions, TNC Privacy Notice, TNC Communications Notice, TNC Electronic Records & Signature Consent, TNC Security & Acceptable Use Terms, and the other incorporated universal terms and notices. The applicable Network terms and action-specific instruments continue to govern their own subjects.

Creating credentials, receiving an invitation, viewing an interface, paying an amount, or seeing an account state does not by itself activate a Network, authorize a consequential action, grant organization or Client access, create a service entitlement, or establish a binding receipt.

2. DEFINITIONS

"Account" means the authenticated identity, organization, relationship, role, permission, device, session, and workspace structure through which a Participant may use authorized TNC functions.

"Authorized User" means a verified person assigned a current role and scope under an Account or organization relationship.

"Organization Administrator" means a person whose authority to administer specified organization access has been separately verified and recorded. Administrative status does not create unlimited authority.

"Relationship Chapter" means the separately governed record of a Participant's role, purpose, permissions, confidentiality, consent, agreements, receipts, and activity within a particular Network or relationship context.

"T.E.A." means the public-facing identity and interaction layer of TNC's integrated end-to-end platform. A visitor or Participant may encounter T.E.A. through TNC-controlled websites, public pages, forms, assistants, portals, and other frontend surfaces. T.E.A. is not a separate account provider or independent platform.

"1290 CRM" means TNC's private governed relationship and operational backend. It is the administrative, record, workflow, permission, audit, and command surface corresponding to TNC's public-facing frontend. It may preserve validated identity, organization, relationship, authority, activity, communication, agreement, receipt, event, service, opportunity, payment-reference, and outcome records according to applicable purposes, permissions, confidentiality, and retention rules. Public interaction with T.E.A. or another frontend surface does not grant access to the backend.

"Integrated TNC Platform" means the single end-to-end system comprising TNC-controlled public websites and pages, T.E.A., authenticated portals and participant-facing functions, and the private governed CRM backend. The public-facing frontend and the private backend are two operational faces of one TNC-controlled system, not separate platforms, providers, or participant relationships. From the time a visitor accesses a TNC-controlled website or page, the request and resulting interaction may be received, secured, routed, processed, contextualized, and recorded as described in the TNC Privacy Notice and other applicable instruments. TNC retains exclusive administrative control of the private backend. Integration



does not merge Relationship Chapters, broaden an audience, create access, widen permissions, or authorize a new purpose or consequential action.

3. ELIGIBILITY, AGE, AND LEGAL CAPACITY

A Participant must have the legal capacity required for the applicable Account, Network, agreement, service, or action. TNC's general-audience services are not directed to children under 13, and TNC does not knowingly create independent Accounts for children under 13.

A person who has not reached the age of legal majority may use a TNC function only when TNC expressly permits the use, the activity is lawful and appropriate, and a parent, guardian, or other legally authorized representative completes any required consent, representation, supervision, or agreement. TNC may restrict or disable functions that are inappropriate for a minor or for which required authority is absent.

TNC may require age, identity, capacity, sanctions, jurisdiction, or other eligibility verification before creating or continuing an Account or enabling a higher-risk function.

4. ACCURATE IDENTITY AND INFORMATION

Participants must provide materially accurate, current, and complete identity, contact, organization, role, authority, payment, and relationship information and must promptly correct material changes.

A Participant may not create a false identity, impersonate another person or organization, misstate employment or affiliation, conceal a material conflict, falsify authority, use another person's credentials, or create an Account to evade a restriction, suspension, block, moderation decision, or legal obligation.

TNC may request supporting evidence and may preserve conflicting, duplicate, or source-variant records until identity and authority are validated. A visible duplicate does not authorize silent deletion, merger, or transfer of rights.

5. ONE GLOBAL IDENTITY; SEPARATE RELATIONSHIP CHAPTERS

TNC may maintain one verified global identity for a person and one validated structure for an organization. A returning Participant entering another Network should receive an additional Relationship Chapter or workspace rather than a duplicate identity when the identity match is sufficiently verified.

One login, global identity, organization affiliation, or technical record does not create access to every Network, organization, workspace, matter, search, Candidate, service, communication, Event, Circle, Room, payment record, or other information.

Every Relationship Chapter remains limited by its source, purpose, Network, organization, role, authority, audience, confidentiality, consent, sensitivity, agreement, effective date, and action-specific permission. Technical availability does not create legal or operational entitlement.

6. ORGANIZATION ACCOUNTS AND AUTHORITY

A person acting for an organization represents that the person has authority appropriate to the requested action. TNC may separately verify the organization, affiliation, title, signatory authority, administrator authority, payment authority, matter scope, and any delegation or revocation.

An organization is responsible for timely and accurate Authorized User designations, role assignments, administrator changes, departures, access-review requests, and revocation notices. TNC may require direct confirmation from an authorized representative before relying on a requested change.

An Organization Administrator may administer only the roles, people, modules, matters, and data within the administrator's recorded authority. Organization status does not create authority over affiliates, portfolio companies, business units, executives, employees, contractors, Candidates, or other persons unless the applicable instrument expressly establishes that authority.



7. ACCOUNT CREATION, ACTIVATION, AND STATE INTEGRITY

Account creation and Account activation are separate states. An Account may remain pending until the required universal terms, Network terms, identity and authority verification, payment or participation status where applicable, approvals, and durable receipts are complete.

A valid Account-activation record must identify the authenticated actor, represented organization if any, verified relationship, applicable document IDs and versions, decision, timestamp, authority and scope, and the exact Account or Network state created.

A payment authorization, payment receipt, invitation, email-domain match, identity classification, support message, or visual success screen is not Account activation unless the required activation receipt exists and can be retrieved.

8. CREDENTIALS, DEVICES, AND SESSION SECURITY

Participants are responsible for protecting passwords, passkeys, authentication applications, verification codes, recovery methods, authenticated devices, sessions, and other credentials. Credentials may not be shared except through an expressly authorized organizational access method that preserves individual accountability.

Participants must promptly report suspected compromise, unauthorized access, phishing, lost or transferred devices, unexpected authentication prompts, incorrect organization access, or a person who should no longer have access.

TNC may require multi-factor authentication, reauthentication, device verification, password or credential reset, session termination, step-up verification, or manual review based on risk, role, requested action, or applicable requirements.

9. ROLE-BASED ACCESS, LEAST PRIVILEGE, AND MATTER COMPARTMENTATION

TNC may grant, restrict, and revoke access by Network, organization, Relationship Chapter, role, matter, Client, Candidate, search, service, Event, Circle, Room, communication, document, payment function, confidentiality class, consent state, and other relevant attributes.

Access must be no broader than reasonably necessary for the authorized purpose. A senior title, organization ownership, administrator role, elevated WC relationship, payment, or prior access does not automatically authorize every organizational matter or confidential record.

TNC may require renewed verification or approval before exposing a sensitive record, exporting data, changing payment or signatory authority, granting administrator status, entering a confidential search, or taking another consequential action.

10. PRIVATE-ACCOUNT AND ORGANIZATION NONDISCLOSURE

TNC may privately resolve whether a person or organization already has an Account, Client relationship, administrator, workspace, or other relationship. TNC will not unnecessarily disclose the existence of a private Account, its administrators, searches, Candidates, documents, billing, activity, or other restricted facts to an unauthorized requester.

Account-recovery, organization-resolution, invitation, error, search, route, timing, and support responses should use neutral language and fail closed where a more specific response could reveal restricted information.

A verified person may initiate a new Client relationship or request access to an existing Client relationship, but identity, affiliation, organization, authority, purpose, role, permission scope, approval, and revocation must be separately evaluated and receipted.

11. ACCOUNT RECOVERY, CHANGES, AND REVOCATION

Recovery requires evidence proportionate to the Account and requested access. TNC may require authentication, identity proofing, organization confirmation, administrator review, device checks, prior receipt evidence, or manual review.

TNC may refuse or delay recovery where the request is inconsistent, unverifiable, disputed, unsafe, unlawful, or likely to expose another person or organization. Recovery must not silently transfer ownership, merge identities, change organization authority, or disclose private Account information.



Access grants and administrator roles may be time-limited, matter-limited, suspended, or revoked. A revocation should remove dependent permissions without destroying valid historical evidence, accepted agreements, security records, or receipts.

12. PLATFORM FUNCTIONS, MODIFICATIONS, AND AVAILABILITY

TNC may add, modify, restrict, suspend, replace, or retire a platform function to maintain security, legality, accessibility, quality, provider compatibility, contractual performance, or business operations.

TNC will use commercially reasonable efforts to preserve active obligations, source records, accepted copies, receipts, data-rights processes, and reasonable transition or export needs where applicable. A technical change does not silently modify a separately accepted commercial agreement or expand a Participant's rights.

Platform availability, data transmission, integrations, communications, third-party services, and provider functions may be interrupted. TNC does not guarantee uninterrupted or error-free operation. An outage does not erase a validly accepted obligation, accrued payment, confidentiality duty, or required record.

13. USER CONTENT AND INSTRUCTIONS

"User Content" includes information, documents, messages, images, recordings, instructions, job information, résumés, Candidate data, Client information, Partner information, service materials, community content, and other material supplied through an authorized TNC channel.

A Participant retains the rights the Participant lawfully holds in User Content, subject to third-party rights and the applicable agreements. The Participant grants TNC a limited, nonexclusive right to receive, host, copy, transmit, process, format, secure, back up, display to the authorized audience, analyze, and otherwise use User Content only as reasonably necessary for the authorized relationship, disclosed purposes, security, support, legal compliance, and applicable records.

A Participant must have authority to provide User Content and must not submit unnecessary sensitive data, unlawful or infringing material, malicious code, another person's confidential information without authority, fabricated records, or instructions that exceed the Participant's authority.

14. T.E.A. AND TECHNOLOGY-ASSISTED FUNCTIONS

T.E.A. and other technology-assisted functions may support research, drafting, summarization, classification, retrieval, comparison, matching, quality control, fraud and abuse detection, moderation support, and preparation of governed actions.

Technology-assisted output may be incomplete, outdated, inferred, or incorrect. TNC may distinguish verified facts, Participant statements, evidence, inference, recommendations, drafts, approvals, and unknowns. An inference or recommendation is not a verified fact or approved action.

T.E.A. may not independently accept an agreement, impersonate a Participant, widen an audience, grant organization or Client access, create payment authority, authorize recruiting or Candidate submission, make a final employment or investment decision, open a mutual introduction without the required permissions, or override a required human or organization approval.

15. 1290 CRM AND CONTEXTUAL RECORDS

Access to and authorized activity across TNC websites and public pages, T.E.A., Services, Network Portals, World Connections, Events, introductions, communications, documents, agreements, payment references, and outcomes may be processed through the Integrated TNC Platform and may create source-tagged records in the 1290 CRM backend.

The 1290 CRM backend may preserve identity, organization, Relationship Chapters, authority, permissions, confidentiality, agreement and receipt history, access grants, security events, interactions, and outcomes. Because the public and private surfaces are one integrated system, authorized context may move through the system for the stated purpose; however, centralized operational oversight does not create Participant cross-visibility, organization cross-visibility, unrestricted cross-context use, or public access to the backend.

Information may be used only for an authorized purpose supported by its source, relationship, audience, confidentiality, consent or other lawful authority, organization role, sensitivity, and action-specific permission. More intelligence does not create more entitlement.



16. ACCEPTABLE USE AND PROHIBITED CONDUCT

A Participant may use TNC systems only for lawful, authorized purposes within the Participant's current relationships and permissions.

A Participant may not:

- obtain or attempt unauthorized access to an Account, Network, organization, matter, record, system, or provider;
- bypass authentication, identity proofing, rate limits, access controls, payment gates, approvals, moderation, blocks, or receipts;
- share credentials, impersonate, misrepresent authority, create deceptive Accounts, or evade a restriction;
- scrape, crawl, enumerate, mirror, bulk extract, export, copy, republish, sell, or create an unrelated database from TNC or Participant information without written authorization;
- introduce malware, automate abusive traffic, interfere with service operation, or test security without written authorization;
- reverse engineer protected software, prompts, models, workflows, source mappings, scoring, system architecture, or confidential methods except where law expressly permits and waiver is prohibited;
- harass, threaten, exploit, unlawfully discriminate, defraud, stalk, traffic, surveil, or misuse personal or confidential information;
- submit false jobs, Candidates, placements, invoices, receipts, reviews, identities, organizations, authority claims, or other records;
- use Candidate, Client, Partner, Services, World Connections, Event, communication, or payment information for an unrelated or unauthorized purpose;
- remove or falsify source, attribution, consent, confidentiality, audience, integrity, or receipt information; or
- use TNC systems to violate law, another agreement, another person's rights, or a valid TNC restriction.

17. THIRD-PARTY SERVICES, INTEGRATIONS, AND LINKS

TNC may use or link to approved third-party providers for hosting, authentication, communications, payments, scheduling, document delivery, analytics, accessibility, security, and other functions. Third-party terms and privacy practices may apply to a Participant's direct use of those services.

A connection, integration, or linked service does not authorize TNC or the Participant to write, delete, merge, export, disclose, or change third-party records unless the applicable agreement, authority, permission, security review, and action approval allow it.

TNC is not responsible for an unrelated third-party service outside TNC's control, but TNC remains responsible for its own representations, contractual obligations, and legally required provider governance.

18. TNC MATERIALS, LICENSE, AND INTELLECTUAL PROPERTY

TNC and its licensors retain rights in TNC marks, designs, text, templates, methods, prompts, workflows, software, interfaces, source mappings, scoring, systems, relationship models, taxonomies, databases, reusable know-how, preexisting materials, and improvements.

Subject to current authorization, TNC grants a limited, revocable, nonexclusive, nontransferable, nonsublicensable right to use the released platform and materials solely for the Participant's authorized relationship. No ownership, source code, model, data, brand, or commercial exploitation right transfers merely because access or an output is provided.

Except as expressly authorized, a Participant may not use TNC marks or materials in a way that suggests endorsement, partnership, agency, sponsorship, certification, or public affiliation.



19. FEEDBACK

A Participant may provide suggestions or feedback. Unless otherwise agreed in writing, TNC may use nonconfidential feedback without restriction or compensation. TNC will not treat confidential User Content, private relationship information, or regulated information as feedback merely because it is submitted through the platform.

20. MONITORING, AUDIT, PRESERVATION, AND ENFORCEMENT

TNC may monitor and preserve access, authentication, security, activity, communications, moderation, agreement, payment-reference, and transaction evidence as disclosed and reasonably necessary for security, fraud prevention, legal compliance, quality, audit, dispute resolution, relationship continuity, and enforcement.

TNC may warn, require correction, restrict a function, revoke a session, suspend access, terminate an Account, preserve evidence, impose a legal hold, or refer a matter for review where it reasonably believes these Account Terms, another agreement, or law may have been violated.

TNC will not represent a proposed enforcement, payment, access, recruiting, or other consequential action as completed unless the required authority, source record, and receipt exist.

21. SUSPENSION, TERMINATION, AND CLOSURE

TNC may restrict, suspend, or terminate access for security risk, suspected compromise, unauthorized use, material misrepresentation, harassment, unlawful discrimination, confidentiality breach, payment default under an applicable instrument, circumvention, sanctions risk, repeated policy violations, or other material breach.

A Participant may request Account closure through an authorized process. Closure may require identity verification, organization review, resolution of active obligations, data-export or transfer decisions, administrator reassignment, and preservation of legally required records.

Closure or termination does not erase accrued payment obligations, Candidate or source protection, confidentiality duties, accepted agreements, public or commercial rights already validly exercised, audit records, security evidence, dispute records, legal holds, or other provisions that by their nature survive.

22. DISCLAIMERS AND NO GUARANTEE

TNC does not guarantee that an Account or platform function will produce a Candidate, interview, offer, hire, placement, Client, introduction, Event, service result, business result, funding, investment, audience, transaction, or other outcome.

Information and technology-assisted output should be verified before consequential use. To the maximum extent permitted by law, platform functions are provided on an “as available” basis. TNC does not disclaim warranties, duties, or rights that cannot lawfully be disclaimed.

TNC does not provide legal, tax, accounting, medical, background-screening, investment, securities, credit, insurance, or other licensed professional services unless a separate written agreement expressly states the service and the required qualifications and approvals are in place.

23. RESPONSIBILITY FOR MISUSE

To the extent permitted by law, a Participant or organization is responsible for losses, claims, and reasonable costs arising from its unlawful use, unauthorized User Content, infringement, material misrepresentation, credential sharing, unauthorized access, or breach of these Account Terms.

This provision does not require indemnification for TNC's own fraud, willful misconduct, gross negligence where the applicable law prohibits limitation, or other liability that cannot lawfully be shifted.

24. CHANGES, MATERIALITY, AND REACCEPTANCE

TNC may update these Account Terms. Material changes must be versioned and presented for notice or reacceptance when required by law, contract, risk, or TNC policy. Prior accepted versions, reproducible copies, and receipts remain preserved.

A technical or security update may be implemented without reacceptance where it does not materially alter legal rights or obligations. A new price, commitment, data use, access right, dispute term, consent scope, confidentiality rule, or other



material obligation must follow the applicable materiality and reacceptance process.

Until required acceptance or reacceptance occurs, dependent actions must remain blocked or limited to a truthful safe state.

25. ORDER OF PRECEDENCE

For an account or platform matter, a signed amendment, settlement, or TNC-approved written exception controls the specific matter; then the applicable action-specific instrument; then the applicable Network terms; then these Account Terms and the other exact accepted universal-package documents; then public summaries, help content, FAQs, or marketing materials.

These Account Terms control only account and platform subjects. They do not expand a fee, guarantee, remedy, indemnity, liability limitation, service entitlement, recruiting right, organization authority, or access scope beyond the controlling instrument.

26. GOVERNING LAW, VENUE, AND DISPUTE ESCALATION

Unless the applicable Network or action-specific instrument lawfully states otherwise, these Account Terms are governed by Kansas law, without regard to conflict-of-law principles. Exclusive venue lies in the state or federal courts serving Sedgwick County, Kansas.

Before filing a non-emergency action, authorized representatives should attempt a good-faith written escalation and reasonable conference within ten business days when practicable. This does not prevent urgent relief, government reporting, or exercise of a nonwaivable right.

Mandatory consumer, privacy, accessibility, employment, communications, venue, or other rights that cannot lawfully be waived remain applicable.

27. GENERAL TERMS

If a provision is invalid or unenforceable, it will be reformed to the minimum lawful extent where permitted, and the remainder remains effective. Failure to enforce once is not a waiver. Assignment requires consent except to a successor that assumes the applicable obligations in writing.

Electronic records and counterparts may be used to the extent permitted by law. Headings are for convenience. “Including” means including without limitation. A reference to law includes amendments and successor provisions.

28. CONTACT

Account, access, recovery, security, privacy, accessibility, communications, legal, or platform questions 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.