1290 WORLD LLC

TWELVE NINETY CONNECTIONS

TNC Security & Acceptable Use Terms

Version 1.1

Document ID	TNC-STD-SECURITY-2026-08-18-001
Entity	1290 World LLC, acting through 1290 World Connections and publicly known as Twelve Ninety Connections (“TNC”)
Audience	All TNC site, account, portal, and system users
Effective Date	Upon valid acceptance after TNC designates this exact version for controlled external use.

This document is part of the TNC Ecosystem Standard Protocol. It must be presented with the exact incorporated versions identified in the acceptance receipt. A visible portal state without a durable receipt is not acceptance.

1. PURPOSE

These Security & Acceptable Use Terms establish baseline security duties and prohibited conduct for TNC public sites, accounts, portals, communications, uploads, integrations, and other systems.

2. USER SECURITY DUTIES

Users must:

- protect credentials, passkeys, verification codes, and authenticated devices;
- use multi-factor authentication when required;
- use only accounts and records the user is authorized to access;
- keep contact and authority information current;
- verify unusual requests through an established channel;
- use approved secure channels for restricted information;
- avoid unnecessary sensitive data; and
- promptly report suspected compromise, unauthorized access, or misdirected information.

3. ORGANIZATIONAL SECURITY DUTIES

Organizations are responsible for authorized users, access assignments, endpoints, downloads, exports, local storage, and prompt revocation. An organization should use least-privilege access and promptly notify TNC when a user's role or authority changes.

4. PROHIBITED ACCESS AND INTERFERENCE

A user may not:

- access or attempt to access an unauthorized account, record, system, or Network;
- bypass authentication, authorization, rate limits, approvals, or technical controls;
- probe, scan, test, or exploit a vulnerability without written authorization;
- introduce malware, destructive code, or harmful content;
- interfere with availability, integrity, logging, monitoring, or another user;
- conceal source, identity, authority, or material activity; or
- help another person perform prohibited conduct.

5. PROHIBITED DATA USE

A user may not scrape, bulk extract, sell, republish, improperly enrich, surveil, reidentify, or use TNC information for an unrelated database, competitive service, discriminatory practice, or unlawful purpose.

Candidate Data, private communications, confidential searches, security information, and restricted records may be used only for the authorized relationship and purpose.

6. HARASSMENT, DISCRIMINATION, AND ABUSE

Users may not threaten, harass, exploit, impersonate, discriminate unlawfully, retaliate, or use TNC systems to facilitate abuse. TNC may restrict or suspend access to protect participants and preserve evidence.

7. FILES, LINKS, AND UPLOADS

Users must have authority to upload files and links. Users may not upload malware, stolen data, unauthorized confidential information, illegal content, or unnecessary sensitive personal information. TNC may scan, quarantine, restrict, or reject content to protect the ecosystem.

A successful upload does not establish that the content is safe, accurate, authorized, or incorporated into a canonical record.

8. INTEGRATIONS AND CONNECTED SERVICES

An integration or connected provider must be expressly authorized and scoped. Connection does not authorize unrestricted access, two-way synchronization, writeback, record merging, or deletion. TNC may suspend an integration that presents security, privacy, authority, or integrity risk.

9. MONITORING AND LOGGING

TNC may log and monitor authentication, access, activity, communications metadata, system events, security signals, and administrative actions as disclosed and reasonably necessary for security, fraud prevention, legal compliance, audit, quality, and incident response.

10. SECURITY INCIDENTS

TNC may investigate suspected incidents, preserve evidence, restrict access, rotate credentials, isolate providers, notify affected persons, and make legally required reports. A suspected incident is not a confirmed incident until verified.

Users must cooperate reasonably with incident containment and must not publicly disclose restricted security details in a way that increases risk.

11. VULNERABILITY REPORTING

Security concerns should be reported privately through the contact method below. Testing is prohibited without written authorization. TNC may establish a separate vulnerability-disclosure process in the exact release copy.

12. ENFORCEMENT

TNC may warn, require verification, restrict functionality, suspend or terminate access, preserve evidence, correct records, or refer a matter for legal review when reasonably necessary. No automated system may mark an external enforcement action completed without the required owner authority and source record.

13. NO SECURITY GUARANTEE

TNC uses safeguards appropriate to the information and risk, but no system is perfectly secure. These Terms do not waive any security or incident duty that cannot lawfully be waived.

14. CHANGES

Material changes must be versioned and presented for reacceptance when required. Prior records and receipts remain preserved.

15. CONTACT

Suspected compromise or security concerns may be reported through the authenticated portal or to:

Terrance Sullivan

Founder | Twelve Ninety Connections

Office: (316) 832-7700 ext. 1290

Direct: (702) 670-1290

Email: tsullivan@1290worldconnections.com

The report should state “Security Report” and avoid including unnecessary credentials or sensitive data.