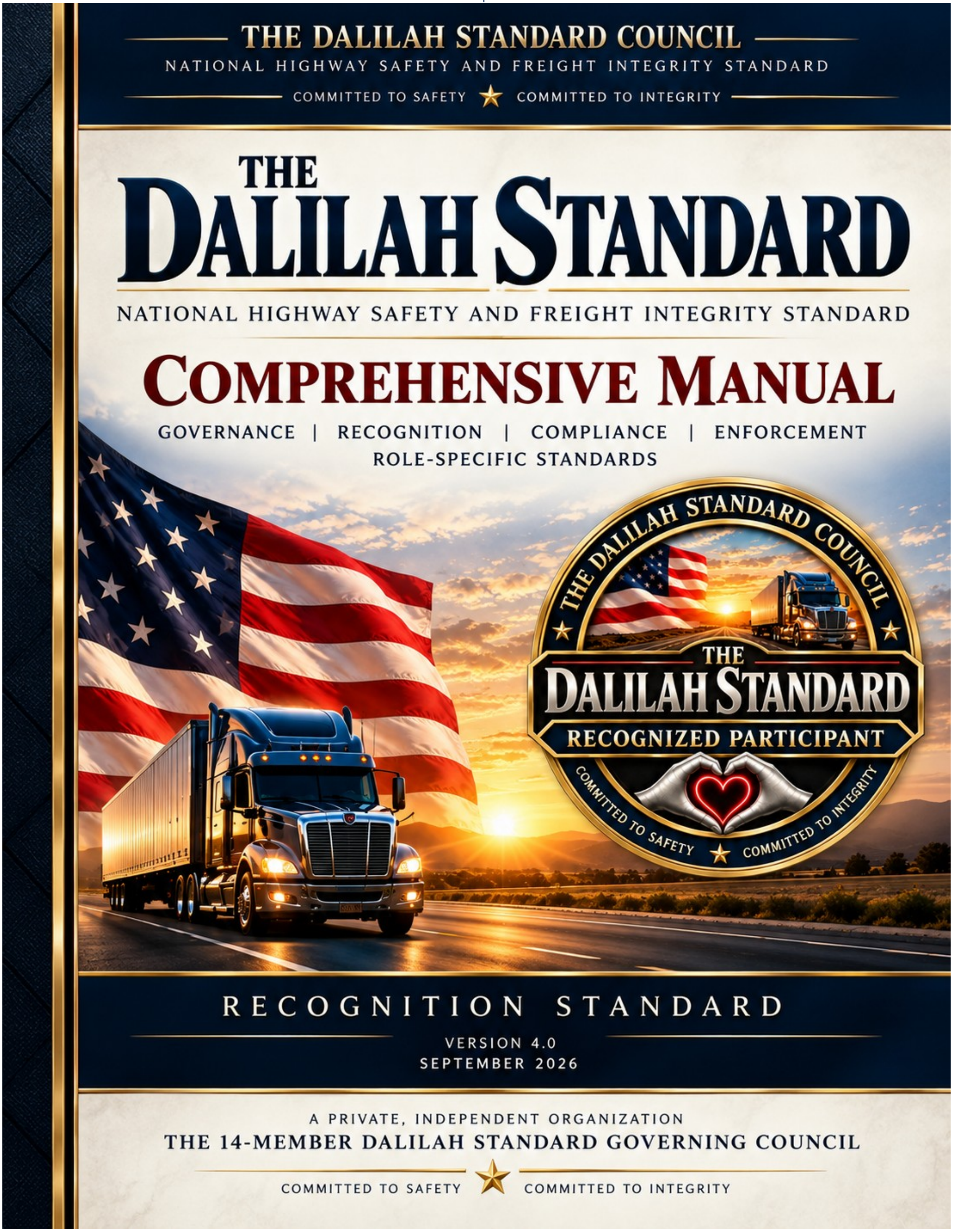
THE DALILAH STANDARD COUNCIL
NATIONAL HIGHWAY SAFETY AND FREIGHT INTEGRITY STANDARD
COMMITTED TO SAFETY ★ COMMITTED TO INTEGRITY
THE DALILAH STANDARD
NATIONAL HIGHWAY SAFETY AND FREIGHT INTEGRITY STANDARD
COMPREHENSIVE MANUAL
GOVERNANCE | RECOGNITION | COMPLIANCE | ENFORCEMENT
ROLE-SPECIFIC STANDARDS
THE DALILAH STANDARD COUNCIL
THE DALILAH STANDARD
RECOGNIZED PARTICIPANT
COMMITTED TO SAFETY ★ COMMITTED TO INTEGRITY
RECOGNITION STANDARD
VERSION 4.0
SEPTEMBER 2026
A PRIVATE, INDEPENDENT ORGANIZATION
THE 14-MEMBER DALILAH STANDARD GOVERNING COUNCIL
COMMITTED TO SAFETY ★ COMMITTED TO INTEGRITY

Document Status, Purpose and Legal Character

Administered by The Dalilah Standard Council | Governed by the 14-Member Dalilah Standard Governing Council

THE DALILAH STANDARD COUNCIL

The Dalilah Standard Council (the "Organization") is the private organization responsible for establishing, administering, maintaining, developing and protecting the integrity of The Dalilah Standard and its Recognition Program. The Organization acts through the governance structure, committees, policies and delegated administrative functions established in this Manual.

The Dalilah Standard Governing Council (the "Governing Council") is the independent fourteen-member voting body within the Organization. It adopts and amends the Standard, protects the independence and integrity of recognition decisions, oversees enforcement policy, appoints committees and decides matters reserved to it. Administrative staff, sponsors, vendors, technology providers and funders may support the program but may not override a properly constituted Governing Council decision.

Program identity. All public recognition marks, pledge materials, agreements, Registry entries and official communications shall identify The Dalilah Standard Council as the administering organization. A participant's status is recognition by the private program; it is not governmental approval, a safety rating, a warranty, or a guarantee of future conduct.

THE ORGANIZATION	THE GOVERNING BODY
The Dalilah Standard Council	**Dalilah Standard Governing Council**
Administers, maintains and protects The Dalilah Standard and Recognition Program.	Independent 14-member voting body overseeing governance, recognition integrity and enforcement.

This is a comprehensive manual for development, legal review, stakeholder review, pilot testing, and adoption by The Dalilah Standard Council. It is written as an operational recognition manual rather than a marketing pledge. The requirements are intended to be capable of being audited, documented, enforced, appealed, and publicly verified through a defined recognition status.

The Dalilah Standard is a private, voluntary industry standard. It does not issue governmental operating authority, licenses, safety ratings, criminal penalties, regulatory findings, or legal opinions. Recognition does not guarantee future conduct, eliminate independent due diligence, or establish that every participant is appropriate for every shipment or business decision.

Participation is voluntary. Once an organization voluntarily applies for and accepts recognition, the requirements applicable to its approved role and scope become mandatory contractual conditions of maintaining the recognition. A participant may withdraw subject to its agreement, but withdrawal does not erase historical conduct, pending matters involving prior conduct, record-preservation duties, or restrictions on continued use of recognition claims and marks.

The Standard may intentionally be more restrictive than minimum law. When it is more restrictive, the requirement is a condition of private recognition unless the same obligation is independently imposed by law. Final regulatory citations and contractual provisions should be validated by qualified counsel before the first official version is adopted.

How to Use This Manual

- Part I contains requirements common to every recognized participant unless a role-specific appendix states otherwise.
- Appendix A is the Governance Charter. Appendix B governs investigations, sanctions and appeals. Appendices C through G and Appendix O contain role-specific recognition requirements. Appendices H through N govern recognition operations, marks, registry, complaints, agreements, evidence and implementation.
- A participant is responsible only for requirements applicable to its recognized role and scope, plus the common requirements. An organization operating in multiple roles must separately satisfy each applicable role-specific appendix.
- Terms such as SHALL and MUST state mandatory recognition requirements. SHOULD states a strong recommended practice unless a role-specific provision makes it mandatory. MAY states permission or discretion.

Contents

L	Master Participation and Recognition Agreement
M	Definitions, Records, Evidence and Documentation Framework
N	Implementation, Transition, Change Control and Future Standards
O	Third Party Vetting Platform Recognition Standard

PART I - MASTER DALILAH STANDARD

1. Mission

The Dalilah Standard exists to raise the level of responsibility applied to commercial transportation by making verification, documentation, lawful operation, public safety, freight integrity and accountability visible and measurable. The central question is not merely whether a shipment moved. It is whether the people and organizations responsible for the decision took reasonable steps to know who was involved, whether the people and companies were qualified and authorized for their roles, whether meaningful warning signs were investigated, and whether the decision can be reconstructed from a reliable record.

2. Foundational Principle

The Standard begins with a simple idea: verify before hire, dispatch, tender, load, release, contract or represent. Verification must be appropriate to the participant's role. It is not a promise that every future event can be predicted. It is a documented process for identifying facts that matter, recognizing inconsistencies, escalating meaningful red flags and refusing to normalize known serious noncompliance.

3. Core Principles

- Compliance Before Capacity. Capacity shortages, price pressure, deadlines and customer demands do not excuse knowingly unsafe, fraudulent or disqualifying conduct.
- Verify Before Engagement. Material identity, authority, insurance, qualification and transaction facts are checked before reliance when the participant controls that decision.
- The Score Is Not the Story. A score, status or automated flag is an input. The underlying evidence, context and documented response determine the recognition conclusion.
- A Red Flag Starts the Inquiry. Unless a condition is expressly disqualifying, a red flag requires additional screening rather than automatic condemnation.
- Public Safety Comes First. Commercial vehicles share the road with families, communities and every other road user.
- Legitimate Businesses Deserve Protection. Fraudulent and intentionally noncompliant operations should not gain an advantage over qualified drivers and lawful companies.

- Accountability Follows Responsibility. Each participant is accountable for its own role, decisions, representations and knowing facilitation of prohibited conduct.
- Continuous Monitoring. Recognition is not a one-time snapshot. Material changes can require review, correction, suspension or revalidation.
- Documentation Matters. A defensible decision requires a record of what was checked, what was found, what was done and why.
- Independent Governance. Recognition and enforcement cannot be purchased, controlled by a sponsor, or manipulated by a single company or individual.

4. Common Mandatory Requirements

Truthfulness

A participant shall not intentionally submit, create, alter, conceal or use materially false information to obtain, maintain, restore or represent recognition.

Identity integrity

A participant shall use reasonable controls to verify the legal and operational identity of parties material to its recognized role and shall not knowingly conceal or materially misrepresent ownership, control, identity, credentials or authority.

Authority and insurance

When authority or insurance is legally required for the participant's activity, the participant shall maintain the required authority/coverage and shall not knowingly represent inactive, revoked, canceled, nonexistent or materially different authority/coverage as valid.

Cooperation

A participant shall cooperate with authorized recognition reviews, audits and investigations subject to applicable law, privilege, confidentiality and the published data-handling rules.

Material-change reporting

A participant shall report material changes that could affect recognition within the time established by the applicable appendix or recognition procedure.

Evidence integrity

After notice of a recognition matter, a participant shall preserve relevant records and shall not intentionally fabricate, destroy, conceal or materially alter evidence.

Non-retaliation

A participant shall not retaliate against a person for a good-faith safety, fraud, compliance or recognition report or for truthful participation in a recognition investigation.

Mark integrity

A participant shall use recognition marks and claims only for the approved entity, role, scope and active recognition period.

No circumvention

A participant shall not accomplish through an affiliate, contractor, dispatch service, shell entity, employee or other arrangement what the Standard directly prohibits the participant from doing.

Lawful conduct

Recognition does not authorize conduct prohibited by law. When law and a private recognition requirement differ, the participant must comply with law and, to remain recognized, also satisfy any lawful additional private requirement.

5. Recognition Status Framework

Status	Meaning	Business effect under the Standard
Recognized / Validated	Applicable requirements satisfied for stated role and scope.	Recognition claim and approved mark may be used.
Additional Screening Required	Material information is unresolved.	No new recognition decision until required screening is completed; existing status handled under Appendix H.
Correction Required	Correctable nonconformity identified.	Participant must cure within the ordered period; recognition may be conditioned.
Unable to Validate	Required evidence cannot be established or a disqualifying condition prevents validation.	Application cannot be approved for the affected scope.
Suspended	Recognition temporarily inactive.	Current recognition claims and mark use cease during suspension.
Revoked	Recognition withdrawn after final action.	Recognition claims cease; reapplication only under reinstatement rules.
Expired	Recognition period ended without completed renewal/revalidation.	Recognition claims cease until renewed.
Permanently Disqualified	Highest private recognition sanction.	No ordinary reapplication; extraordinary review only under published rule.

6. Non-Negotiable Conditions

- Intentional recognition fraud or fabrication of material evidence.
- Knowingly using or representing a materially false identity, authority, insurance record, driver credential or recognition status.
- For a recognized motor carrier, knowingly dispatching a driver who lacks a required valid CDL/license or who is known to be disqualified or subject to an applicable out-of-service condition.
- For a recognized motor carrier, use of dispatch activity performed outside the United States of America. This is a private Dalilah Standard requirement and is intentionally more restrictive than any less restrictive legal arrangement that may otherwise be permitted.
- Intentional concealment of ownership or control when disclosure is required for recognition.
- Knowing participation in cargo theft, identity theft, fraudulent brokerage, fictitious pickup, payment diversion or other material transportation fraud.
- Serious retaliation against a good-faith reporter, witness, investigator or decision-maker.
- Continued use of a recognition mark or representation of active recognition after final revocation or after notice of a suspension that prohibits such use.

7. Documentation Standard

The recognition record should permit an independent reviewer to reconstruct the decision. At minimum, the record should identify the entity and scope reviewed; the date and reviewer; the sources consulted; material records collected; inconsistencies found; additional screening performed; explanations obtained; corrective actions; conflicts/recusals; the final decision; and the next monitoring or revalidation date. The program shall not require collection of sensitive information that is unnecessary to the recognition purpose.

APPENDIX A

Governance Charter and Dalilah Standard Governing Council

This Charter establishes the governing body, independence safeguards, voting rules, committees, ethics, financial independence and accountability of the private recognition program.

A1. Organization and Governing Body

The Dalilah Standard Council (the "Organization") is the private organization responsible for establishing, administering, maintaining, developing and protecting The Dalilah Standard and the integrity of its Recognition Program. The Dalilah Standard Governing Council is the independent fourteen-member voting body within the Organization that adopts and amends the Standard, oversees recognition integrity and enforcement policy, appoints committees, and decides matters reserved to it.

- Administrative staff may perform delegated functions but may not override a properly constituted Governing Council decision.
- A founder, sponsor, administrator, vendor or technology provider has no veto merely because it provides funding, technology, staff or intellectual property.
- Council members owe their program duty to the integrity of the Standard rather than to the commercial interests of the stakeholder category from which they were selected.

A2. Fourteen Voting Seats

The Council is intentionally cross-functional so no single sector controls the Standard.

- 1. Established motor carrier representative.
- 2. Owner-operator or small-fleet motor carrier representative.
- 3. Licensed property freight broker representative.
- 4. Freight forwarder representative.
- 5. Shipper, manufacturer, retailer or beneficial cargo owner representative.
- 6. Factoring, transportation-finance or commercial-credit representative.
- 7. Transportation insurance, underwriting, claims or risk-management representative.
- 8. Attorney with substantial transportation, regulatory, insurance, employment or commercial-law experience.
- 9. Commercial driver, driver-safety or professional driver-training representative.
- 10. Current or former law-enforcement, cargo-theft, highway-safety enforcement or transportation-investigations representative.
- 11. Fraud, cybersecurity, identity-verification or organized-crime prevention specialist.
- 12. Transportation compliance, credentialing, licensing, regulatory, data, telematics, TMS or verification specialist.
- 13. Public/highway-safety or crash-survivor advocate.
- 14. Family Member Representative - a family member of a person killed or seriously injured in a commercial-motor-vehicle crash.

A3. Family Member Representative

The Family Member Representative is a full voting member. The purpose of the seat is to ensure that the human consequences of commercial-vehicle safety decisions remain present in governance.

- Industry employment is not required.
- Selection should consider lived experience, judgment, willingness to review evidence, confidentiality and commitment to constructive safety improvement.
- The seat is not controlled by an industry sponsor, plaintiff or defense interest, advocacy organization or administrator.
- The representative is subject to the same conflict, recusal, confidentiality and ethics rules as every other member.

A4. Eligibility and Vetting

Before appointment, each candidate should complete a governance application and disclosure sufficient to assess qualifications, independence and conflicts.

- Identity and professional background verification appropriate to the seat.
- Disclosure of current employers, material transportation clients, board memberships and financial interests relevant to the Standard.
- Disclosure of pending litigation or enforcement matters that reasonably create a program conflict.
- Agreement to ethics, confidentiality, competition and recusal policies.
- No person should be appointed solely because the person or employer is a major sponsor or customer.

A5. Terms and Rotation

Council continuity should be balanced against the need to prevent permanent control.

- Three-year terms, staggered so approximately one-third of seats expire each year.
- Normally no more than two consecutive full terms.
- A partial term of less than eighteen months does not count as a full term for term-limit purposes.
- A former member may become eligible again after at least one full year off the Council unless the Governance and Ethics Committee recommends a longer period.

A6. Officers

The Council elects a Chair and Vice Chair from eligible voting members. A Secretary or governance officer maintains the official record.

- Chair and Vice Chair should not come from the same stakeholder category.
- The Chair facilitates meetings and has one vote only.
- The Chair has no second vote and no tie-breaking vote.
- The Vice Chair acts when the Chair is absent or recused.

A7. Meetings and Notice

The Council should meet at least quarterly and may conduct special meetings for urgent matters.

- Ordinary meeting materials should be distributed sufficiently in advance for meaningful review.
- Emergency meetings may use shortened notice when delay would threaten safety, evidence, recognition integrity or program operations.
- Minutes record attendance, recusals, motions, vote results and resolutions without unnecessarily disclosing protected case information.

A8. Quorum

Quorum is a majority of filled, eligible voting seats and must include at least five distinct stakeholder categories. Recused members are not counted as eligible for the affected matter.

- If recusals destroy quorum, the matter is deferred or handled under a published alternate-panel procedure.
- Staff and nonvoting advisers do not count toward quorum.

A9. Voting and Tie Votes

Ordinary motions require a majority of eligible votes cast unless a higher threshold is specified.

- Each eligible voting member has one vote.
- A tie vote means the motion fails.
- A 7-7 vote does not become approval, recognition, revocation or another action through unilateral intervention by the Chair, Administrator, founder, sponsor or staff.
- A failed motion may be reconsidered only under a published reconsideration procedure or after material new information.
- Changes to non-negotiable requirements, Council composition, permanent-disqualification policy or core due-process protections require at least two-thirds of the full eligible Council.

A10. Conflicts and Recusal

Independence requires both disclosure and action when a conflict exists.

- Annual written conflict and independence disclosure.
- Immediate supplemental disclosure when circumstances change.
- Mandatory recusal for the member’s employer, client, insured, vendor, material financial interest, close family relationship or another relationship reasonably capable of affecting impartiality.
- A recused member does not deliberate, vote, lobby decision-makers or receive nonpublic deliberative materials for that matter.
- Recusals are documented in the official record.

A11. Standing Committees

The Council may create committees but may not delegate away protections that the Standard reserves to the full Council.

- Compliance and Enforcement Committee.
- Dalilah Standard Appeals Panel.
- Standards and Technical Committee.
- Governance and Ethics Committee.
- Family and Public Safety Advisory Committee.
- Finance/Audit Committee if program scale warrants.

A12. Competition Safeguards

Because competitors may participate in governance, meetings must remain focused on objective recognition administration.

- No discussion or coordination of freight rates, pricing strategy, customers, bids, capacity allocation, wages, market division or competitively sensitive plans unrelated to the Standard.
- Recognition decisions are individual conformity decisions under published criteria, not collective agreements to boycott lawful nonparticipants.
- Counsel should review meeting protocols and competition safeguards before launch and periodically thereafter.

A13. Funding and Independence

The organization may be funded by recognition fees, administration fees, education, sponsorships, grants, donations and other lawful sources approved by policy.

- No funder receives a guaranteed seat, recognition outcome, waiver, confidential case access or enforcement preference.
- Fees should follow published or objectively governed schedules where practicable.
- Material financial relationships are disclosed and managed.

A14. Member Removal

A Council member may be removed for serious governance misconduct.

- Grounds include undisclosed material conflict, corruption, misuse of office, interference with an investigation, repeated nonparticipation, confidentiality breach, retaliation, material dishonesty or conduct seriously damaging program integrity.
- The member receives written notice and an opportunity to respond.
- Removal requires a two-thirds vote of eligible members not involved in the alleged misconduct.

A15. Transparency and Annual Review

The Council should publish enough information to make governance credible without exposing protected case data.

- Current Standard and amendment history.
- Council composition and stakeholder seats.
- Governance, conflict and enforcement framework.
- Aggregate annual statistics for applications, recognitions, complaints, suspensions, revocations, appeals and reinstatements.
- Annual review of stakeholder balance, funding independence and program risks.

A20. Governing Council Member Oath and Pledge

Every voting Governing Council member shall execute this pledge before participating in Council business and renew it as required by Council policy.

- I will place the integrity of the Dalilah Standard, highway safety, lawful commerce, and fair administration above the commercial interests of my employer, sector, sponsor, customer, or personal relationships.
- I will disclose conflicts promptly, recuse when required, protect confidential information, and never seek or accept preferential recognition or enforcement treatment.

- I will not interfere with an investigation, pressure an investigator or decision-maker, retaliate against a good-faith reporter, or use Council service to obtain competitive intelligence.
- I will apply published requirements consistently and will support strict enforcement when reliable evidence establishes a material, serious, egregious, or intentional violation.

Program Administrator: The Dalilah Standard Council

By signing below, I attest that I am authorized to bind the organization identified below, that the representations made for this recognition are truthful and materially complete, and that the organization voluntarily accepts the Dalilah Standard requirements applicable to this role, including monitoring, self-reporting, investigation, corrective action, suspension, revocation, permanent disqualification where authorized, Registry publication, and cessation of mark use when required.

Organization / Participant Legal Name: ____

DBA (if applicable): ____

USDOT / MC / Other Identifier (if applicable): ________________________________

Authorized Representative: ____

Title: ____

Signature: ____ Date: ____________________

Compliance, Investigations, Enforcement, Sanctions and Appeals

This Appendix establishes the complete private enforcement lifecycle from intake through final appeal. Its purpose is to protect public safety and recognition integrity while providing fair notice, reliable evidence and independent review.

B1. Enforcement Principles

A complaint is an allegation, not a finding. Enforcement must be fast enough to contain credible immediate risks and disciplined enough to avoid arbitrary reputational harm.

- Presumption of no final violation until the required process is completed.
- Emergency protective action may precede final adjudication.
- Investigators seek inculpatory and exculpatory evidence.
- Decision-makers disclose conflicts and recuse where required.
- Sanctions are tied to published criteria and documented findings.

B2. Intake

Every complaint or internally generated concern receives a case identifier and initial triage record.

- Record source, date, entities, allegations, affected recognition, available evidence and urgency.
- Identify immediate safety, driver, identity, authority, insurance, cargo-theft, fraud, offshore-dispatch, falsification or retaliation concerns.
- Preserve submitted evidence in its received form where practicable.
- Identify duplicate, frivolous, facially impossible or out-of-scope matters and document closure reason.

B3. Preliminary Assessment

A preliminary assessment determines whether the matter should be closed, referred for routine correction, opened as an investigation or escalated for emergency action.

- Confirm jurisdiction under the Standard.
- Identify provisions potentially implicated.
- Check conflicts before assigning personnel.
- Determine whether external reporting obligations may exist; the Standard does not replace legal reporting duties.

B4. Investigation Plan

For material matters, the investigator prepares a proportionate plan defining issues, sources, preservation needs and anticipated interviews.

- Avoid collecting unrelated personal data.
- Use original or independently verifiable records where reasonably available.
- Document unsuccessful attempts to obtain material evidence.
- Separate facts, allegations, inference and expert opinion.

B5. Evidence Sources

Reliable evidence can include government/public records, authenticated business records, insurance records, credential records, contracts, invoices, rate confirmations, dispatch records, electronic communications, interviews, photographs, transaction records, lawful device/location records, technology logs and other probative material.

- No single source is automatically conclusive in every matter.
- Conflicts between sources are investigated rather than silently ignored.
- Screenshots should preserve source/date/context when possible.
- AI-generated or manipulated media concerns require authentication before reliance.

B6. Participant Notice

Except where emergency action is authorized, a participant receives written notice before a final adverse decision.

- Identify the provisions at issue.
- Provide a reasonable factual summary without exposing protected sources unnecessarily.
- State response deadline and submission method.
- Explain possible sanctions and appeal rights.

B7. Participant Response

The participant may submit documents, declarations, explanations, corrective actions and identification of contrary evidence.

- Failure to respond may be considered but does not transform an unsupported allegation into proof.
- Extensions may be granted for good cause when they do not create unacceptable risk.
- Knowingly false responses are separate potential violations.

B8. Emergency Interim Suspension

An authorized officer may temporarily suspend recognition when credible information indicates an immediate or substantial threat to public safety, driver qualification, identity, authority, insurance, cargo integrity or recognition integrity.

- Interim suspension is protective, not a final finding.
- Written reasons are issued promptly.
- Independent review occurs promptly under a defined timetable.
- Mark use and active-recognition claims cease while suspended.
- A tie on final merits does not convert an interim suspension into a final sanction.

B9. Corrective Action

Correctable nonconformities may be resolved through a written corrective-action plan.

- Identify root cause where appropriate.
- Specify action owner and completion date.
- Require objective evidence of completion.
- Verify effectiveness when the issue could recur.
- Repeated failure of the same control may justify escalation.

B10. Sanction Matrix

Sanctions are proportionate to seriousness, intent, harm, repetition, concealment, cooperation and remediation.

- Level I - Correction Required.
- Level II - Suspension.
- Level III - Revocation.
- Level IV - Permanent Disqualification.

B11. Aggravating Factors

Aggravating factors increase seriousness or demonstrate reduced trustworthiness.

- Intentional conduct.
- Concealment or fabricated evidence.
- Leadership direction or approval.
- Actual or substantial potential harm.
- Repeated conduct after warning.
- Retaliation or obstruction.
- Financial gain from prohibited conduct.

B12. Mitigating Factors

Mitigation can affect sanction but cannot make an unresolved non-negotiable condition acceptable.

- Prompt self-reporting.
- Immediate containment.
- Full cooperation.
- Credible root-cause correction.
- Isolated human error despite otherwise effective controls.
- Voluntary restitution or remediation where relevant.

B13. Decision Standard

Final findings must be supported by reliable evidence under the program’s adopted evidentiary standard. Before launch, counsel should finalize whether ordinary sanctions use preponderance and whether permanent disqualification uses a heightened standard.

- Written decision separates findings of fact, rule conclusions and sanction.
- Decision-makers must not have investigated the matter they adjudicate.

B14. Voting and Ties

Suspension or revocation requires the affirmative vote specified by the adopted panel rules. Permanent disqualification requires at least a two-thirds affirmative vote of eligible assigned decision-makers.

- A tie fails to establish the proposed adverse final action.
- The panel chair has no second or tie-breaking vote.
- Recused members are not counted as eligible decision-makers.

B15. Written Disposition

A final disposition states the participant, scope, findings, provisions, sanction, effective date, corrective conditions, registry treatment and appeal rights.

- Public wording follows Appendix J and does not publish unsupported allegations as facts.

B16. Appeal

A participant may appeal a final adverse action within the stated deadline, ordinarily ten business days.

- Grounds: material factual error, material procedural error, misapplication of the Standard, material new evidence not reasonably available earlier, or sanction inconsistent with published rules.
- Appeal panel members did not investigate or decide the original merits.
- The appeal record identifies the standard of review.

B17. Reinstatement

Suspended or revoked participants may seek reinstatement only under published conditions.

- Correction and verification of the underlying cause.
- Re-audit when ordered.
- Demonstrated control improvement.
- Any waiting period completed.
- Permanent disqualification has no ordinary reinstatement path.

B18. Referral and Cooperation

The Council may refer suspected unlawful conduct to appropriate authorities or cooperate with lawful requests, consistent with law, privilege, privacy and program policy.

- Recognition investigators do not represent themselves as law enforcement.
- Program findings do not substitute for government findings.

B19. Enforcement Records

The case file preserves the evidence and process necessary to explain the outcome.

- Intake and triage.
- Evidence inventory.
- Notices and responses.
- Conflict checks and recusals.
- Interim orders.
- Decision and vote record.
- Appeal and final status.
- Corrective action and reinstatement records.

APPENDIX C

Motor Carrier Recognition Standard

Appendix C establishes auditable requirements for motor carriers. The carrier remains responsible for its drivers, equipment and operations and may not outsource responsibility through dispatch, leasing, contractors or affiliates.

C1. Recognition Scope

Recognition attaches to the specifically identified legal motor-carrier entity and authority. Affiliates, sister companies and separate USDOT/MC entities are not recognized unless included through an approved multi-entity scope.

- Application lists legal name, DBA, USDOT, MC/authority identifiers, physical business location, ownership/control information required by policy, insurance, BOC-3 where applicable and principal contacts.
- The public Registry identifies the recognized entity and scope.

C2. Principal Place of Business and Identity

The carrier shall maintain a real, truthful business identity and physical principal place of business consistent with applicable requirements and recognition evidence.

- Verify address using multiple sources when risk warrants.
- Investigate virtual office, mail drop, shared-address or unverifiable-location indicators rather than automatically treating every shared location as disqualifying.
- Maintain current phone/email/domain and report material changes.
- Investigate suspected cloning or unauthorized use of the carrier identity.

C3. Ownership and Control

The carrier shall disclose owners/controllers to the level established by recognition policy and shall not conceal material control.

- Identify persons/entities meeting the program ownership threshold.
- Identify material management/control relationships.
- Investigate sudden ownership/control changes, repeated affiliations with revoked/fraudulent entities, unexplained shared contact data or authority-transfer concerns.
- A red flag starts an inquiry; affiliation alone is not automatic guilt.

C4. Authority, Registration and Insurance

The carrier shall maintain authority, registration and insurance required for its operations.

- Monitor authority status and material insurance changes.
- Do not tender or operate under inactive/revoked authority when authority is required.
- Investigate conflicting insurer, policy, VIN/equipment or entity information.
- Maintain evidence of required filings where applicable.

C5. Driver Identity

The carrier shall use controls reasonably designed to establish that the person hired and dispatched is the person represented by the driver credentials.

- Government-issued identity/credential review.
- Reasonable anti-impersonation controls appropriate to risk.
- Escalation for mismatched names, photographs, dates, license data or contact information.
- No use of another person's credential or driver identity.

C6. Driver Qualification File

The carrier shall maintain the driver qualification records required for each driver and any additional evidence required by the Standard.

- Application/employment information as required.
- Motor vehicle/driving record checks as applicable.
- CDL/license and endorsements.
- Medical qualification where applicable.
- Prior-employer/safety-history inquiries where required.
- Road test or equivalent qualification evidence where required.
- Annual or recurring review required by law/program.

C7. CDL and License Monitoring

The carrier shall verify required driving credentials before dispatch and monitor for material status changes.

- No dispatch of a driver known to have a suspended, revoked, canceled, expired or otherwise invalid required credential.
- No dispatch when the carrier knows the driver is disqualified or subject to an applicable out-of-service order.
- Use lawful recurring monitoring or notification systems where available and proportionate.
- Document stop-dispatch and reinstatement decisions.

C8. English-Language Proficiency

Where operational English-language proficiency is legally required, the carrier shall treat credible inability to satisfy the applicable requirement as a qualification issue.

- Training cannot be used to paper over an unresolved legal qualification requirement.
- Document assessment, corrective action and return-to-service basis when a credible concern is raised.
- Do not discriminate on national origin or accent; evaluate the actual applicable operational requirement.

C9. Entry-Level Driver Training

When ELDT requirements apply, the carrier shall verify required completion through appropriate evidence and investigate credible evidence of fraudulent training records.

- Training-provider status where relevant.
- Completion evidence.

- Escalation for impossible dates, fabricated certificates or identity mismatch.

C10. Drug and Alcohol Compliance

The carrier shall maintain applicable drug/alcohol testing and Clearinghouse obligations.

- Pre-employment and other required testing.
- Required queries and follow-up.
- Removal from safety-sensitive functions when required.
- Return-to-duty/follow-up documentation when applicable.

C11. Hours of Service and Fatigue

The carrier shall maintain controls reasonably designed to prevent and detect unlawful hours-of-service operation.

- Required ELD/log records.
- Review of material violations.
- No coercion to falsify or exceed legal limits.
- Fatigue reporting and escalation process.
- Corrective action for repeated patterns.

C12. U.S.-Only Dispatch

All dispatch activity for a recognized motor carrier shall be performed within the United States of America. This is a private recognition requirement and is intentionally strict.

- Applies to employees, contractors, affiliates, subcontractors, call centers and remote personnel performing dispatch functions.
- Carrier documents dispatch provider identity, physical operating location and material contacts.
- Carrier maintains evidence reasonably sufficient to establish where dispatch work is actually performed.
- Intentional routing of communications through U.S. numbers, VPNs or nominal U.S. entities to conceal offshore dispatch is prohibited.
- The carrier retains lawful operational control and safety responsibility.
- A dispatch provider may not perform regulated brokerage activity without required authority.

C13. Dispatch Access and Cybersecurity

Dispatch and TMS access shall be controlled to reduce identity fraud and unauthorized operational control.

- Named user accounts where practicable.
- MFA for privileged access where supported.
- Prompt removal of former users.
- Review of anomalous login/location activity when available.
- Protection of rate confirmations, driver data and payment instructions.

C14. Equipment Identity

The carrier shall maintain reliable records connecting tractors/trailers to the carrier’s operations and investigate unexplained equipment substitutions.

- VIN/unit information.
- Registration/lease evidence as applicable.
- Driver-to-equipment assignment records appropriate to operation.
- Escalation for inconsistent plates, VINs or unit identity.

C15. Inspection, Repair and Maintenance

The carrier shall maintain required inspection, repair and maintenance programs and shall not knowingly dispatch equipment with unresolved material safety defects.

- Preventive maintenance schedule.
- Driver vehicle inspection/defect process where applicable.
- Repair documentation.
- Periodic/annual inspection evidence.
- Controls for brakes, tires, lights, steering, coupling, visibility, cargo securement and other safety-critical systems.

C16. Out-of-Service and Defect Escalation

Known out-of-service conditions or material safety defects must be resolved before prohibited operation resumes.

- Document who placed equipment/driver out of service.
- Document repair/correction and authorization to return.
- No management override based solely on delivery pressure or capacity.

C17. Leases and Operational Control

Leasing arrangements shall be documented and shall not be used to conceal identity, responsibility or operational control.

- Maintain required lease documentation.
- Identify who owns/leases equipment.
- Investigate arrangements that appear to rent authority or obscure the actual carrier.
- Recognition does not validate an unlawful lease merely because paperwork exists.

C18. Safety Management and Training

The carrier shall maintain safety policies proportionate to its operations and risk.

- Driver orientation.
- Hazard/cargo-specific training where applicable.
- Accident/incident reporting.
- Corrective coaching and discipline.
- Management review of repeated violations or preventable events.

C19. Crash and Incident Review

Serious crashes and material safety incidents require timely internal review and recognition notification when they meet the program's material-event criteria.

- Preserve relevant records.

- Do not make unsupported admissions of legal fault in recognition reporting; report facts and known status.
- Identify immediate containment and corrective actions.

C20. Cargo Security

The carrier shall maintain reasonable cargo-security controls appropriate to commodities, lanes and known fraud risks.

- Verify pickup instructions and changes.
- Protect driver/load information from unnecessary disclosure.
- Escalate suspicious pickup/delivery changes.
- Report suspected cargo theft promptly to appropriate parties.

C21. Payment and Identity Fraud

The carrier shall use independent verification for material changes to payment, banking or contact instructions.

- Do not rely solely on an email requesting a bank change.
- Maintain callback/known-channel verification.
- Escalate newly created domains, changed phone numbers or inconsistent signatures when material.

C22. Subcontractors and Service Providers

The carrier remains accountable for recognition requirements applicable to functions it outsources.

- Vendor due diligence proportionate to function.
- Written requirements for dispatch, compliance, safety or technology vendors where appropriate.
- No outsourcing to evade the Standard.

C23. Self-Reporting Timeframes

The final program should adopt explicit reporting timeframes. Until finalized, the working rule is prompt reporting, with the most serious safety, identity, authority, insurance and offshore-dispatch events escalated immediately or within one business day when practicable.

- Counsel and pilot testing should finalize exact 24-hour/three-business-day categories before official adoption.

C24. Required Carrier Evidence

Initial and revalidation evidence should be sufficient to verify the carrier rather than merely accept self-attestation.

- Registration/authority records.
- Insurance evidence.
- Ownership/control evidence required by policy.
- PPOB evidence.
- Driver qualification sample/audit evidence.
- Dispatch location/control evidence.
- Maintenance/inspection sample.

- Safety and fraud-control policies.
- Material-change and incident records.

C25. Carrier Audit

Carrier audits use risk-based sampling and may expand when exceptions are found.

- Sample drivers across hire dates and operations.
- Sample equipment and maintenance records.
- Sample dispatch users/providers and access locations.
- Sample shipments/transactions to test identity and control.
- Document population, sample rationale, exceptions and corrective action.

C26. Carrier Recognition Agreement

The carrier agreement incorporates this Appendix and identifies the recognized legal entity and authority.

- Truthful application.
- Continuing compliance.
- U.S.-only dispatch.
- Monitoring and audit consent.
- Material-change reporting.
- Self-reporting.
- Registry publication.
- Mark rules.
- Enforcement and appeal.
- Withdrawal and surviving obligations.

C. Motor Carrier Dalilah Standard Pledge and Recognition Acknowledgment

A motor carrier seeking or maintaining Dalilah Standard recognition shall execute this pledge as part of Appendix C.

- Compliance comes before capacity, price, speed, convenience, or profit when a material safety or lawful-operation issue is known.
- We will verify drivers before dispatch and continuously monitor qualification, licensing, disqualification, out-of-service status, and other material eligibility information required by the Standard.
- We will use only dispatch operations and dispatch personnel located within the United States of America as required by the Dalilah Standard, including contractors, subcontractors, affiliates, and remote personnel.
- We will maintain lawful operational control, truthful identity and ownership/control information, required authority and insurance, a verifiable principal place of business, safe equipment, and auditable records.
- We will stop dispatch or operation when a non-negotiable disqualifying condition is known and will not conceal, falsify, destroy, or manipulate evidence or recognition information.

Program Administrator: The Dalilah Standard Council

By signing below, I attest that I am authorized to bind the organization identified below, that the representations made for this recognition are truthful and materially complete, and that the organization voluntarily accepts the Dalilah Standard requirements applicable to this role, including monitoring, self-reporting, investigation, corrective action, suspension, revocation, permanent disqualification where authorized, Registry publication, and cessation of mark use when required.

Organization / Participant Legal Name: ____

DBA (if applicable): ____

USDOT / MC / Other Identifier (if applicable): ________________________________

Authorized Representative: ____

Title: ____

Signature: ____ Date: ____________________

Freight Broker Recognition Standard

Appendix D establishes requirements for licensed property brokers seeking recognition. The focus is broker identity, carrier selection, transaction integrity, fraud prevention, documentation and knowing facilitation of prohibited conduct.

D1. Recognized Entity and Authority

Recognition attaches to the identified brokerage entity and authority, not automatically to affiliates.

- Verify legal name, DBA, authority, bond/trust, physical business information, ownership/control information required by policy and material contacts.
- Report material changes promptly.

D2. Broker Identity Security

The broker shall maintain controls against unauthorized use of its identity and credentials.

- Protect load-board/TMS accounts.
- Use MFA where supported for privileged systems.
- Remove former-user access promptly.
- Monitor suspicious login/contact changes where available.

D3. Carrier Onboarding

The broker shall use documented carrier onboarding procedures appropriate to risk.

- Verify carrier identity.
- Verify active authority when required.
- Verify insurance appropriate to transaction.
- Verify material contact information through independent sources when risk warrants.
- Review meaningful ownership/contact/authority anomalies.

D4. Carrier Selection

Carrier selection is a documented decision, not a single score.

- Define minimum requirements.
- Identify disqualifying conditions.
- Define red flags requiring additional screening.
- Document material overrides and approving authority.
- Do not represent an automated score as a governmental safety determination.

D5. Actual Carrier Verification

The broker shall maintain reasonable controls to identify the carrier that actually transports the load.

- Rate confirmation identifies contracted carrier.
- Pickup controls support confirmation of driver/equipment where appropriate.
- Unauthorized substitutions are escalated.
- Records preserve the identity of the transporting carrier.

D6. Double Brokering

The broker shall maintain controls to detect and prevent unauthorized re-brokering or double brokering.

- Contract terms.
- Carrier identity verification.
- Pickup verification.
- Payment/assignment review where relevant.
- Escalation for mismatched carrier/driver/equipment or unusual communications.

D7. Cargo Theft and Fictitious Pickup

High-risk freight and suspicious transactions require enhanced controls.

- Independent callback/known-channel verification.
- Driver/equipment confirmation appropriate to risk.
- Facility coordination for last-minute changes.
- Prompt incident escalation and evidence preservation.

D8. Payment Diversion

Material bank/payment changes require independent verification.

- Do not redirect payment based solely on inbound email.
- Verify through a known channel.
- Document approver and verification.

D9. Dispatch and Operational Control

The broker shall not knowingly participate in arrangements that obscure the carrier’s identity or unlawfully transfer carrier operational control.

- A transaction represented as Dalilah Standard compliant shall not knowingly rely on a recognized carrier violating the U.S.-only dispatch requirement.
- Broker personnel should remain within the broker’s lawful role.

D10. Shipper and Facility Communications

The broker shall communicate material carrier changes accurately and promptly when required by contract, risk or recognition policy.

- Do not conceal unauthorized carrier substitution.
- Provide sufficient information for facility verification when the shipper controls release.

D11. Records

The broker shall retain records sufficient to reconstruct carrier selection and transaction identity.

- Onboarding evidence.
- Authority/insurance checks.
- Rate confirmation.
- Material communications.
- Override/escalation record.
- Pickup/delivery identity evidence where applicable.

D12. Monitoring

The broker shall monitor material changes in carriers it uses according to risk and program policy.

- Authority/insurance changes.
- Identity/contact changes.
- Fraud/cargo-theft indicators.
- Recognition status if relied upon.

D13. Incident Response

Suspected identity theft, cargo theft, fraudulent brokerage or payment diversion triggers documented response.

- Containment.
- Customer/carrier notification as appropriate.
- Preserve evidence.
- Report to appropriate authorities/insurers when required or reasonably necessary.

D14. Broker Audit

Audits sample onboarding files and completed transactions.

- Population and sampling rationale.
- High-risk transaction sample.
- Override sample.
- Fraud-control testing.
- Corrective-action verification.

D15. Broker Agreement

The role-specific agreement incorporates this Appendix.

- Recognized entity/authority.
- Audit/monitoring.
- Self-reporting.
- Registry.
- Marks.
- Enforcement/appeal.
- Withdrawal.

D. Freight Broker Dalilah Standard Pledge and Recognition Acknowledgment

A freight broker seeking or maintaining Dalilah Standard recognition shall execute this pledge as part of Appendix D.

- We will verify the identity, authority, insurance where applicable, and material contact information of transportation providers before relying on them.
- We will use documented carrier-selection and transaction-integrity procedures and investigate material substitutions, identity conflicts, or other red flags before proceeding.
- We will not knowingly facilitate unlawful brokerage, identity fraud, cargo theft, credential fraud, prohibited dispatch arrangements, concealed control, or known serious safety noncompliance.

- We will preserve records sufficient to reconstruct material carrier-selection and load-transaction decisions and will cooperate with authorized Dalilah Standard reviews.

Program Administrator: The Dalilah Standard Council

By signing below, I attest that I am authorized to bind the organization identified below, that the representations made for this recognition are truthful and materially complete, and that the organization voluntarily accepts the Dalilah Standard requirements applicable to this role, including monitoring, self-reporting, investigation, corrective action, suspension, revocation, permanent disqualification where authorized, Registry publication, and cessation of mark use when required.

Organization / Participant Legal Name: ____

DBA (if applicable): ____

USDOT / MC / Other Identifier (if applicable): ________________________________

Authorized Representative: ____

Title: ____

Signature: ____ Date: ____________________

Freight Forwarder Recognition Standard

Appendix E addresses forwarders whose responsibilities may include arranging transportation, consolidation, custody, transfer and shipment documentation. Recognition requires role clarity and chain-of-custody integrity.

E1. Role and Authority

The forwarder shall accurately identify the legal entity, authority and role under which each covered service is performed.

- No misrepresentation as carrier/broker when acting in another role.
- Multi-role entities must satisfy each applicable appendix.

E2. Identity and Ownership

Verify legal identity, physical business information, ownership/control required by policy, material contacts and applicable insurance/financial responsibility.

- Report material changes.
- Investigate unexplained control or contact anomalies.

E3. Carrier Selection

When the forwarder selects carriers, it shall use documented identity, authority, insurance and risk screening comparable to the responsibility it assumes.

- Enhanced review for red flags.
- Document exceptions.

E4. Transportation Chain

The forwarder shall maintain records identifying each transportation leg and responsible provider.

- Origin provider.
- Transfer/consolidation points.
- Final-mile provider where applicable.
- Material substitutions.

E5. Custody and Release

Where the forwarder or its facility has custody, release controls shall reasonably establish who receives the freight.

- Authorized pickup information.
- Identity/equipment checks proportionate to risk.
- Exception escalation.
- Chain-of-custody record.

E6. Consolidation Controls

Consolidation shall not obscure shipment identity or responsible parties.

- Shipment identifiers.
- Handling records.
- Exception/damage records.

E7. Cargo Security

Security controls shall reflect commodity, location and known theft risk.

- Facility access.
- High-value freight procedures.
- Suspicious pickup/change escalation.

E8. Fraud and Payment Controls

Forwarders shall use independent verification for material payment and identity changes.

- Known-channel callback.
- Protection of customer/carrier data.

E9. Records and Audit

Audits sample shipments from booking through delivery/custody transfer.

- Carrier-selection evidence.
- Chain-of-custody evidence.
- Exception handling.
- Payment/fraud controls.

E10. Agreement

The agreement identifies entity, facilities/scope and incorporated obligations.

- Monitoring.
- Audit.
- Self-reporting.
- Registry/marks.
- Enforcement/appeal.

E. Freight Forwarder Dalilah Standard Pledge and Recognition Acknowledgment

A freight forwarder seeking or maintaining Dalilah Standard recognition shall execute this pledge as part of Appendix E.

- We will accurately identify the role in which we act and maintain the authority, insurance, identity, and operational records applicable to that role.
- We will use documented motor-carrier selection, custody, transfer, release, identity-verification, and cargo-security procedures appropriate to the freight handled.
- We will investigate unexplained substitutions and will not knowingly facilitate unlawful brokerage, cargo theft, identity fraud, prohibited dispatch arrangements, or other material violations.
- We will preserve an auditable chain of responsibility for each covered shipment or transportation leg.

Program Administrator: The Dalilah Standard Council

By signing below, I attest that I am authorized to bind the organization identified below, that the representations made for this recognition are truthful and materially complete, and that the organization voluntarily accepts the Dalilah Standard requirements applicable to this role, including monitoring, self-reporting, investigation, corrective action, suspension, revocation, permanent disqualification where authorized, Registry publication, and cessation of mark use when required.

Organization / Participant Legal Name: ____

DBA (if applicable): ____

USDOT / MC / Other Identifier (if applicable): ________________________________

Authorized Representative: ____

Title: ____

Signature: ____ Date: ____________________

Shipper / Beneficial Cargo Owner Recognition Standard

Appendix F establishes a voluntary standard for shippers and beneficial cargo owners that choose to subject their transportation procurement and freight-release controls. It does not transfer a carrier's legal safety obligations to the shipper; it defines the shipper's own recognition commitments.

F1. Scope

Recognition may apply enterprise-wide, to specified business units, or to identified facilities. The Registry must state the scope clearly.

- Unrecognized facilities may not imply recognition.

F2. Transportation Provider Verification

Before tender, the shipper shall verify the transportation provider to the level appropriate to its procurement role.

- Identity.
- Authority where applicable.
- Insurance where applicable.
- Material contact information.
- Enhanced screening for red flags.

F3. Broker Use

When using a broker, the shipper shall know the broker entity and maintain reasonable controls for authorized carrier changes when the shipper/facility must release freight.

- Do not assume broker use eliminates facility identity controls.

F4. Direct Carrier Procurement

When the shipper selects the carrier directly, it shall maintain documented carrier-selection requirements.

- Minimum requirements.
- Red-flag escalation.
- Exception approval.
- Record of decision.

F5. Pickup Verification

A recognized facility shall implement procedures reasonably designed to verify the arriving party before releasing freight.

- Carrier name/identifier.
- Driver identity appropriate to risk.
- Tractor/trailer information appropriate to risk.
- Pickup/reference information.
- Escalation for mismatches.

F6. Unauthorized Substitution

The facility shall not knowingly release freight to an unauthorized substituted carrier or driver.

- Obtain authorization through a known channel.
- Document who approved the change and why.

F7. High-Risk Freight

High-value, theft-targeted or otherwise sensitive freight may require enhanced verification.

- Pre-arrival confirmation.
- Restricted pickup changes.
- Seal/security procedures where appropriate.
- Escalation contacts.

F8. Procurement Pressure

Price, urgency and capacity do not excuse knowingly overriding a material identity, authority, insurance, fraud or safety concern.

- Exceptions require documented approval.
- Repeated emergency exceptions trigger management review.

F9. Facility Training

Personnel responsible for release should be trained on the facility's verification and escalation procedures.

- Recognizing mismatches.
- Known-channel verification.
- Fraud/social-engineering awareness.
- When to stop and escalate.

F10. Incident Response

Suspected fictitious pickup, cargo theft or identity fraud requires prompt containment and reporting.

- Preserve video/gate/communications records.
- Notify appropriate internal/security/broker/carrier/insurer/law-enforcement parties as applicable.

F11. Records

The shipper shall retain evidence sufficient to reconstruct covered provider selection and freight release.

- Provider verification.
- Facility release record.
- Exceptions/authorizations.
- Incident records.

F12. Shipper Audit

Audits sample facilities and transactions within recognized scope.

- Normal transactions.
- Exception transactions.
- High-risk freight.
- Training records.
- Incident response.

F13. Agreement

The agreement identifies recognized facilities/business units and the participant's own obligations.

- No implication that recognition guarantees carrier performance.
- Monitoring/audit.
- Registry/marks.
- Enforcement/appeal.

F. Shipper / Beneficial Cargo Owner Dalilah Standard Pledge and Recognition Acknowledgment

A shipper or beneficial cargo owner seeking or maintaining Dalilah Standard recognition shall execute this pledge as part of Appendix F.

- We will ask and document the essential question: Who actually moved the freight?
- We will verify the contracted transportation provider and establish risk-appropriate pickup controls for the arriving carrier, driver, tractor, trailer, and material substitutions.
- We will not knowingly release freight to an unauthorized substituted carrier or driver and will escalate suspicious identity changes, altered documents, unusual payment instructions, or other cargo-theft indicators.
- Price, urgency, or capacity pressure will not override a known material safety, identity, fraud, or lawful-operation concern.

Program Administrator: The Dalilah Standard Council

By signing below, I attest that I am authorized to bind the organization identified below, that the representations made for this recognition are truthful and materially complete, and that the organization voluntarily accepts the Dalilah Standard requirements applicable to this role, including monitoring, self-reporting, investigation, corrective action, suspension, revocation, permanent disqualification where authorized, Registry publication, and cessation of mark use when required.

Organization / Participant Legal Name: ______________________________________

DBA (if applicable): ____

USDOT / MC / Other Identifier (if applicable): ______________________________

Authorized Representative: ____

Title: ____

Signature: ______________________________________ Date: ___________________

Commercial Vehicle OEM Safety Standard and Commitment

Appendix G is a voluntary manufacturer commitment focused on evidence-based vehicle safety, crash avoidance and mitigation, maintenance support, cybersecurity, theft prevention and responsible safety claims. It is not a motor-carrier operating recognition.

G1. Scope

The agreement shall identify manufacturer and covered product lines or enterprise scope.

- Registry wording distinguishes OEM commitment from carrier recognition.

G2. Safety Engineering

The OEM should maintain documented processes for identifying and reducing reasonably foreseeable safety risks within its role.

- Design review.
- Validation/testing.
- Field data review.
- Corrective action.

G3. Crash Avoidance

The commitment supports evidence-based deployment and improvement of appropriate crash-avoidance systems.

- Automatic emergency braking where applicable.
- Collision warning/mitigation.
- Stability systems.
- Visibility and lane-related assistance as appropriate.

G4. Crash Mitigation

The OEM should evaluate feasible crash-mitigation measures consistent with law, engineering evidence and vehicle use.

- Rear impact protection.
- Side impact/underride mitigation where applicable.
- Cab/occupant protection.
- Trailer conspicuity/visibility.

G5. Maintenance Information

Safety-critical systems require clear inspection, maintenance and repair information.

- Service procedures.
- Diagnostic information appropriate to qualified repair.
- Recall and campaign communication.

G6. Defects and Recalls

The manufacturer shall maintain lawful safety-defect and recall processes and shall not use recognition claims to minimize an unresolved recall obligation.

- Timely communication.
- Repair support.
- Tracking/closure where applicable.

G7. Cybersecurity

Connected commercial vehicles and systems should be managed under a documented cybersecurity process.

- Access control.
- Vulnerability response.
- Software/update integrity.
- Incident response.

G8. Theft and Identity

The OEM should support reasonable vehicle identity integrity and theft-deterrence capabilities.

- VIN/identifier integrity.
- Connected-system security.
- Owner/operator guidance.

G9. Safety Data

Where vehicle data can responsibly support crash investigation or maintenance, access frameworks should balance safety utility, privacy, security, proprietary rights and law.

- Do not overstate what data proves.

G10. Claims

Marketing of safety technology must not materially overstate validated capability.

- Driver-assistance systems are described accurately.
- Known operational limitations are not intentionally concealed.

G11. Technical Review

OEM participation may require periodic technical review by qualified subject-matter experts with conflict controls.

- Evidence-based criteria.
- Protection of legitimate confidential information.

G12. Agreement

The OEM commitment defines scope, reporting, technical review, registry/mark rules and enforcement applicable to the commitment.

- No implication of government approval.

G. Commercial Vehicle OEM Dalilah Standard Safety Pledge and Commitment

An OEM participating under Appendix G shall execute this safety pledge and commitment.

- We will support evidence-based continuous improvement in crash avoidance, crash mitigation, visibility, stability, braking, underride protection, and other safety-critical technologies appropriate to our products.
- We will maintain responsible processes for safety defects, recalls, repair and maintenance information, cybersecurity, vehicle-identification integrity, and theft deterrence.
- We will not represent experimental or unvalidated safety technology as proven and will cooperate with appropriate evidence-based safety review within the scope of this voluntary commitment.
- We accept the recognition, monitoring, mark-use, Registry, complaint, investigation, enforcement, and appeal rules applicable to this commitment.

Program Administrator: The Dalilah Standard Council

By signing below, I attest that I am authorized to bind the organization identified below, that the representations made for this recognition are truthful and materially complete, and that the organization voluntarily accepts the Dalilah Standard requirements applicable to this role, including monitoring, self-reporting, investigation, corrective action, suspension, revocation, permanent disqualification where authorized, Registry publication, and cessation of mark use when required.

Organization / Participant Legal Name: ____

DBA (if applicable): ____

USDOT / MC / Other Identifier (if applicable): ________________________________

Authorized Representative: ____

Title: ____

Signature: ____ Date: ____________________

APPENDIX H

Recognition, Audit, Monitoring and Revalidation Procedures

Appendix H turns the Standard into an operating recognition program. It defines the lifecycle, evidence review, independence, sampling, monitoring, material-change reporting and renewal.

H1. Application

Every applicant identifies legal entity, requested role, requested scope, related entities relevant to scope, principal contacts and required declarations.

- Incomplete applications are not recognized.
- Material misrepresentation can trigger denial/enforcement.

H2. Conflict Screening

Before assignment, recognition personnel disclose conflicts with the applicant.

- Reassign when impartiality is reasonably compromised.

H3. Evidence Request

The program provides a role-specific evidence list and may request supplemental evidence when red flags arise.

- Avoid unnecessary sensitive data.
- Use secure transfer/storage.

H4. Verification

Reviewers verify material evidence rather than relying entirely on self-attestation.

- Public/government sources.
- Independent third-party sources.
- Applicant records.
- Direct confirmation when warranted.

H5. Nonconformity Classification

Findings are classified consistently.

- Observation - improvement opportunity, no violation.
- Minor/Corrective - correctable issue not creating immediate serious risk.
- Major - material failure requiring correction and possible suspension.
- Critical/Non-negotiable - disqualifying or emergency issue under the Standard.

H6. Recognition Decision

The final initial-recognition decision is made by an authorized person or panel sufficiently independent from the substantive evaluation.

- Approve.
- Approve with defined correction/condition if permitted.
- Additional screening.

- Unable to validate/deny.

H7. Certificate and Registry

Approved recognition identifies entity, role, scope, effective date, expiration/revalidation date and recognition identifier.

- Certificate wording matches Registry.

H8. Routine Monitoring

Monitoring focuses on changes that can materially affect recognition.

- Authority/registration.
- Insurance.
- Ownership/control/contact changes.
- Driver qualification events for carriers.
- Dispatch location/control.
- Fraud/cargo-theft indicators.
- Mark misuse.

H9. Material Change Reporting

Participants must report material changes within published timeframes.

- The official version should contain a role-specific reporting matrix.
- Serious immediate risks receive accelerated reporting.

H10. Surveillance Review

Between full revalidations, the program may perform targeted surveillance.

- Automated monitoring.
- Document refresh.
- Transaction sampling.
- Attestation plus independent verification.

H11. Random Audit

Random audits reduce the risk that only known problems receive scrutiny.

- Selection methodology should avoid favoritism.
- Random selection can be risk-weighted if methodology is documented.

H12. For-Cause Audit

Credible material information can trigger a focused audit.

- Scope may expand if evidence shows related control failures.

H13. Sampling

Sampling must be documented and defensible.

- Define population.
- Select sample method.
- Include risk-based items where appropriate.

- Record exceptions and expansion logic.

H14. Revalidation

Recognition is revalidated on the schedule adopted for the role, with annual full revalidation as a strong default for launch unless the Council adopts another evidence-based cycle.

- Refresh core identity/authority/insurance/ownership evidence.
- Review material changes.
- Review prior corrective actions.
- Sample operating records.

H15. Failure to Revalidate

If required revalidation is not completed, recognition expires or is suspended according to published rules.

- No silent indefinite extension.

H16. Auditor Competence

Reviewers and auditors must be competent for assigned work.

- Training.
- Role knowledge.
- Evidence handling.
- Conflict/ethics.
- Periodic calibration.

H17. Calibration and Quality Review

The program should periodically compare reviewer decisions to improve consistency.

- Blind or second review of sample cases.
- Document recurring ambiguity and amend guidance.

H18. Audit Trail

Every recognition event produces a traceable record.

- Who.
- What.
- When.
- Evidence.
- Finding.
- Decision.
- Next action.

Pledge, Recognition Marks, Claims and Brand-Use Rules

Appendix I separates a voluntary pledge from verified recognition and protects the public from misleading recognition claims.

I1. Pledge Signatory

Signing the pledge is a public commitment to the principles but is not proof that the organization passed recognition.

- Pledge Signatory mark, if used, must be visually distinct from Recognized mark.

I2. Applicant

An applicant may truthfully state that an application is pending only if allowed by policy.

- Applicant may not use Recognized mark.

I3. Recognized

Only active recognized participants may use the approved Recognized designation for the approved role/scope.

- Role/scope must not be obscured when material.

I4. Affiliate Claims

Recognition does not automatically extend to parent, subsidiary, affiliate, separate authority, facility or product line.

- Claims must avoid group-wide implication when scope is narrower.

I5. Digital Mark

Digital marks may link to the Registry record to enable verification.

- Do not alter embedded verification features.

I6. Suspension

During suspension, current-recognition claims and mark use cease.

- Historical factual references must clearly state status/date and not imply current recognition.

I7. Revocation/Expiration/Withdrawal

Recognition claims cease when status is no longer active.

- Remove marks from websites, proposals, email signatures and new marketing within the ordered timeframe.

I8. Counterfeit/Misuse

Unauthorized use can trigger demand, registry notice where appropriate, contractual/trademark remedies and referral.

- Misuse by a nonparticipant is not treated as a recognition sanction but may be addressed through lawful brand protection.

I9. No Government Implication

Marks shall not imply DOT/FMCSA/state/government approval unless an actual government statement independently exists and is accurately described.

I10. Pledge Text

The official pledge should preserve the original commitment to compliance before capacity, verification, zero tolerance for known serious noncompliance, accountability, support for legitimate drivers/carriers, opposition to fraud, continuous improvement, shared responsibility, public safety and validation accountability.

- Final pledge maintained as controlled program document.

I11. Role-Specific Pledges Are Part of the Applicable Appendix

The pledge and recognition acknowledgment contained in each applicable role appendix is incorporated into that appendix and must be executed as part of initial recognition and as otherwise required for revalidation. A participant recognized in more than one role must execute each applicable role-specific pledge. Signing a pledge alone does not establish recognition; recognition requires satisfaction of the applicable verification and approval requirements.

Public Registry, Status Definitions and Publication Rules

Appendix J defines what the public can verify and limits publication to accurate, necessary recognition information.

J1. Purpose

The Registry is the authoritative public source for current Dalilah Standard recognition status.

- A logo or certificate should be verifiable against the Registry.

J2. Core Fields

Registry records should include enough information to distinguish the recognized entity and scope.

- Legal name/approved DBA.
- Recognition ID.
- Relevant USDOT/MC or public identifier where applicable.
- Role/scope.
- Effective and revalidation/expiration dates.
- Current status.

J3. Adverse Status

Suspension, revocation, expiration and permanent disqualification may be displayed according to policy.

- Effective date.
- Concise reason code.
- Final vs interim status.

J4. Complaint Confidentiality

A complaint alone is not published as an established violation.

- Interim suspension may be identified as interim.

J5. Reason Codes

Use factual standardized codes where possible.

- Authority/insurance.
- Identity/ownership.
- Driver qualification.
- Dispatch location/control.
- Fraud/evidence integrity.
- Mark misuse.
- Failure to cooperate/revalidate.

J6. Narrative Limits

Public narratives should be concise, factual and limited to what is necessary to explain recognition status.

- Avoid inflammatory adjectives.
- Distinguish allegation, interim action and final finding.

J7. Corrections

Participants may request correction of demonstrable factual Registry errors.

- Correction request does not suspend a valid sanction automatically.
- Maintain change history.

J8. Historical Status

The Council should adopt a policy for how long historical adverse status remains publicly searchable.

- Balance public verification, fairness, legal requirements and data minimization.
- Counsel review required.

J9. API/Data Use

If Registry data is offered through an API, terms should prohibit deceptive alteration of status and should preserve update timestamps.

- Third parties should not present stale status as current.

Complaints, Whistleblower Protection and Non-Retaliation Procedures

Appendix K provides accessible reporting while protecting due process and discouraging retaliation or malicious reporting.

K1. Reporting Channels

The program should accept reports through secure web, email/phone or other documented channels appropriate to scale.

- Emergency threats should be directed to appropriate emergency/law-enforcement channels as well as program reporting when relevant.

K2. Who May Report

Employees, drivers, contractors, customers, insurers, law enforcement, families, competitors, members of the public and other sources may submit information.

- Source identity affects reliability analysis but does not automatically prove or disprove a report.

K3. Anonymous Reports

Anonymous reports may be accepted.

- Anonymous status can limit follow-up.
- Evidence still must be evaluated.

K4. Confidentiality

Reporter identity is protected to the extent reasonably possible and permitted by law/policy.

- Do not promise absolute confidentiality that cannot legally be guaranteed.

K5. Non-Retaliation

Retaliation against a good-faith reporter or witness is prohibited.

- Termination, threat, harassment, blacklisting or commercial punishment can be examined when causally related to protected reporting.

K6. Malicious Reports

Knowingly false or fabricated reports may violate program rules.

- A good-faith report is not malicious merely because it cannot be substantiated.

K7. Triage

Reports are triaged under Appendix B.

- Immediate safety/fraud risks prioritized.

K8. Feedback

Where appropriate and lawful, the program may acknowledge receipt and provide limited closure/status information to the reporter.

- Protected case details are not disclosed merely because someone filed a complaint.

Master Participation and Recognition Agreement

Appendix L provides the substantive framework for the contract every recognized participant signs. Counsel should convert this working language into final enforceable agreement terms for the chosen legal entity and jurisdictions.

L1. Parties

The agreement identifies The Dalilah Standard Council/authorized Administrator and the exact legal Participant.

- Legal name.
- Entity type/jurisdiction.
- Address.
- Authorized signer.
- Recognition identifiers.

L2. Incorporated Documents

The Participant agrees that the current adopted Standard, applicable role appendix, recognition procedures, mark rules and enforcement/appeal rules are incorporated as stated in the agreement.

- Version/effective date must be identifiable.

L3. Voluntary Participation

The Participant acknowledges that it voluntarily chose to apply and that recognition is private.

- No government status is conferred.

L4. Mandatory Compliance After Acceptance

While recognized, the Participant agrees to comply with all applicable requirements.

- Voluntary participation does not mean voluntary compliance after recognition.

L5. Representations

The Participant represents that application information is materially truthful and complete to the required scope.

- Continuing duty to correct material errors.

L6. Monitoring Consent

The Participant consents to program monitoring using lawful sources and methods described in policy.

- No consent beyond what law permits.

L7. Audit and Records

The Participant agrees to provide reasonably requested recognition records subject to law, privilege, confidentiality and data-minimization rules.

- Failure to cooperate can affect recognition.

L8. Material Changes

The Participant agrees to report material changes under the applicable reporting matrix.

- Role-specific triggers incorporated.

L9. Self-Reporting

The Participant agrees to report known material recognition violations affecting its status.

- Good-faith self-reporting may mitigate but does not erase the condition.

L10. Confidentiality

The program protects nonpublic Participant information under adopted policy and applicable law.

- Exceptions for Registry, legal process, required reporting and authorized investigations.

L11. Registry Consent

The Participant consents to publication of defined recognition status information.

- Public fields limited by Appendix J.

L12. Mark License

Active recognition includes a limited, nonexclusive, nontransferable, revocable license to approved marks.

- No sublicensing.
- Ends on suspension/revocation/expiration/withdrawal as provided.

L13. Enforcement

The Participant accepts Appendix B procedures as a condition of recognition.

- Emergency interim action.
- Notice/response.
- Sanctions.
- Appeal.

L14. No Warranty

Recognition is not a warranty or guarantee of safety, performance, creditworthiness, legality of every future act, or suitability for a particular shipment.

- Third parties retain their own duties.

L15. Fees

Fees, billing, refunds and nonpayment consequences are governed by the executed schedule.

- Payment does not purchase outcome.

L16. Withdrawal

The Participant may withdraw prospectively under the agreement.

- Mark use ends.
- Registry updated.
- Prior conduct/pending matters and surviving duties handled under policy.

L17. Amendments

The Council may amend the Standard through the adopted governance process.

- Material changes include effective date/transition.
- No case-specific retroactive manipulation.

L18. Data Security

Program and Participant shall use reasonable safeguards for recognition information under their control.

- Incident notification obligations finalized by counsel/policy.

L19. Legal Boilerplate Reserved for Counsel

Final agreement requires jurisdiction-specific legal terms.

- Governing law.
- Venue/arbitration if used.
- Limitation of liability.
- Indemnification.
- Severability.
- Assignment.
- Force majeure if appropriate.
- Notices.
- Electronic signatures.
- Entire agreement.

L20. Role-Specific Addenda

Each recognized role signs/incorporates its role appendix.

- Carrier - Appendix C.
- Broker - Appendix D.
- Forwarder - Appendix E.
- Shipper/BCO - Appendix F.
- Third Party Vetting Platform - Appendix O.
- OEM - Appendix G.

Definitions, Records, Evidence and Documentation Framework

Appendix M standardizes terminology and evidence handling so the same words and records mean the same thing across recognition, audits and enforcement.

M1. Defined Terms

Administrator. The entity or staff authorized to perform administrative, verification, technology, registry or other delegated functions.

Applicant. An organization seeking recognition but not yet holding active recognition.

Recognized Participant. An organization holding active recognition for a defined legal entity, role and scope.

Council. The fourteen-member Dalilah Standard Governing Council unless context clearly refers to the organization.

Organization. The Dalilah Standard Council as the private organization responsible for the program.

Material. Information or conduct significant enough that a reasonable recognition decision-maker would consider it important to recognition, safety, identity, authority, insurance, qualification, fraud or transaction integrity.

Dispatch. Operational functions that assign, direct, coordinate or communicate with drivers/equipment concerning loads, pickup, delivery, routing or related carrier operations, as further defined by adopted policy.

Red Flag. Information that reasonably requires additional review but is not necessarily a violation by itself.

Scope. The legal entity, role, authority, facility, business unit, product line or activity covered by recognition.

Known. Actual knowledge; where a provision uses “known or should have been known,” the final legal drafting should define the objective diligence standard.

Independent Verification. Confirmation through a source or channel not controlled solely by the incoming representation being verified.

Material Change. A change reasonably capable of affecting recognition status, scope, verification or risk.

Interim Suspension. Temporary protective inactive status pending final review; not a final merits finding.

Revocation. Final withdrawal of recognition after applicable process.

Permanent Disqualification. Highest private recognition sanction, subject to the heightened process adopted by the Council.

M2. Evidence Reliability

- Prefer original/authenticated and independent records when reasonably available.

- Evaluate source, date, completeness, chain of custody, corroboration and motive/bias where relevant.
- A government database may contain lag or error; conflicting evidence should be investigated.
- A participant's own record is evidence but may require independent corroboration for high-risk issues.
- Screenshots should preserve source and date/context where possible.
- Do not rely on AI-generated summaries as the sole evidence of a material violation.

M3. Evidence Inventory

Material investigations and audits should maintain an evidence inventory identifying item, source, date received/collected, custodian/location, relevance and any authenticity concern.

M4. Record Retention

Before launch, the Council shall adopt a retention schedule by record category after legal/privacy review. The schedule should distinguish application records, audit records, enforcement files, appeals, governance records, conflict disclosures, Registry history, financial records and sensitive personal information.

M5. Legal Hold / Preservation

When litigation, government inquiry or a material recognition investigation reasonably requires preservation, ordinary deletion should be suspended for relevant records to the extent required by law/policy.

M6. Privacy and Data Minimization

- Collect only information reasonably necessary for recognition, enforcement, security or legal compliance.
- Use role-based access.
- Avoid publishing sensitive personal information in the Registry.
- Define deletion/disposal methods.
- Document authorized sharing with vendors/contractors.

M7. Confidential and Privileged Material

The program should not require waiver of attorney-client privilege as a routine condition of recognition. Procedures should permit privilege logs or alternative evidence when appropriate. Trade secrets and security-sensitive information should receive appropriate handling.

Implementation, Transition, Change Control and Future Standards

Appendix N provides a controlled path from working draft to a credible operational program.

N1. Formation

Establish the legal entity, ownership of intellectual property, governance authority and administrator relationship.

- Counsel review.
- Insurance/risk review.
- Banking/accounting controls.

N2. Initial Council

Appoint the initial fourteen seats through a documented transition process.

- Disclosures.
- Background/qualification review.
- Ethics/competition training.

N3. Controlled Documents

Create controlled final versions of the Standard, appendices, applications, audit checklists, agreements, mark guide, Registry policy and enforcement forms.

- Version number.
- Effective date.
- Document owner.
- Change history.

N4. Technology

Implement secure systems for applications, evidence, monitoring, case management, Registry and audit trail.

- Access control.
- Logging.
- Backup/recovery.
- Vendor security.

N5. Pilot

Pilot with a limited, diverse group before broad launch.

- Carrier sizes.
- Broker/shipper/forwarder participants.
- Test audit burden.
- Test false positives.
- Test appeal and Registry workflows.

N6. Pilot Review

Use pilot findings to correct ambiguity and impractical requirements.

- Do not weaken non-negotiables merely for convenience.
- Distinguish real risk from administrative friction.

N7. Official Adoption

The Governing Council adopts the first official version only after legal, operational and stakeholder review.

- Record vote.
- Publish effective date.
- Publish transition period.

N8. Existing Participants

If pledge signatories or pilot participants predate official recognition, clearly distinguish historical pledge/pilot status from final recognition.

- No automatic grandfathering unless approved criteria are satisfied.

N9. Change Control

Proposed material changes should be documented with rationale and impact.

- Technical review.
- Conflict review.
- Legal review where appropriate.
- Council vote threshold.
- Transition period.

N10. Emergency Amendments

An emergency amendment may be used for a newly discovered serious risk but should receive prompt full review.

- Do not use emergency changes to manipulate a pending individual case.

N11. Future Role Standards

The Council may add standards for dispatch services, factoring/finance, insurance, driver training, other technology/data providers, warehouses/facilities, maintenance providers and other roles. Third Party Vetting Platforms are addressed in Appendix O.

- New standards follow the same governance and adoption safeguards.

N12. Annual Program Audit

The program should conduct an annual internal or independent program-level audit.

- Governance.
- Conflicts.
- Recognition consistency.
- Enforcement timeliness.

- Appeals.
- Registry accuracy.
- Data security.
- Financial independence.

N13. Public Annual Report

Publish aggregate program performance without exposing protected case data.

- Applications/recognitions.
- Status changes.
- Complaints/enforcement.
- Appeals.
- Major amendments.
- Program improvements.

Third Party Vetting Platform Recognition Standard

Appendix O applies to a third party that supplies identity, registration, authority, insurance, safety, fraud, compliance, or counterparty risk information to support transportation decisions. It covers the legal entity and the specific products, data feeds, reports, scores, APIs, and services submitted for recognition. A platform that also acts as a broker, carrier, forwarder, shipper, or OEM must satisfy each applicable role appendix. Recognition of a platform does not validate every entity it reports on or substitute for a customer's own decision.

O1. Scope and Legal Identity

The platform SHALL identify its legal entity, ownership and control, relevant affiliates, customer-facing brands, principal business location, and products within the requested recognition scope.

It SHALL accurately describe which checks are performed by the platform, which are supplied by third parties, and which require customer action. It SHALL not imply that private recognition is an FMCSA determination, safety rating, government endorsement, or guarantee against fraud or loss.

O2. Source Provenance and Data Currency

For each material data element, the platform SHALL document its source, collection or last verification time, update cadence, known latency, and any transformation applied. It SHALL distinguish official records from commercial, user-provided, inferred, or unverified data.

The platform SHALL display or make available the as-of time for material findings and establish a controlled process for stale, unavailable, inconsistent, or interrupted feeds. It SHALL not present an old or missing check as a current clear result.

O3. Identity and Affiliation Controls

The platform SHALL use documented methods to resolve legal identity and relevant identifiers, including USDOT and MC numbers when applicable, and investigate material mismatches in legal name, authority, contact details, ownership, or business location.

It SHALL assess material affiliation and impersonation indicators within its stated scope, and document the limitations of checks that cannot establish beneficial ownership or operational control. Shared addresses, phone numbers, or identifiers are leads for review, not conclusive evidence of misconduct.

O4. Authority, Insurance and Safety Representations

When the platform reports authority, registration, insurance, or safety information, it SHALL identify the source and date of each check, the status actually observed, and material limitations. A pending, inactive, revoked, missing, or conflicting record SHALL not be represented as verified current authority or coverage.

The platform SHALL distinguish an FMCSA safety rating from its own evaluation and distinguish no rating or insufficient data from an affirmative finding of safety. A score, flag, or risk tier SHALL have documented meaning and SHALL not conceal a known disqualifying fact.

O5. Decision Logic and Human Review

The platform SHALL maintain documented, version-controlled criteria for material alerts, scores, recommendation categories, overrides, and changes to decision logic. It SHALL test material changes before release and maintain a rollback process.

Material adverse outputs SHALL permit qualified human review of the underlying evidence and context. An automated or AI-generated summary SHALL not be the sole basis for a material violation finding or irreversible adverse action under this Standard. Unknown, unverified, and confirmed adverse conditions SHALL be distinguished.

O6. Customer Disclosures and Audit Trail

The platform SHALL communicate material limitations, data age, unresolved discrepancies, scope of service, and actions the customer must take before reliance. Marketing and interface claims SHALL be consistent with actual checks.

For material reports and decisions, the platform SHALL preserve a time-stamped record of source data or defensible source references, rule or model version, findings, reviewer actions, overrides, and customer-visible output under an approved retention schedule. Records SHALL support reconstruction of what was known when a decision was made.

O7. Error Correction and Disputes

The platform SHALL provide a reachable process for a reported entity or customer to challenge material identity or status errors, submit evidence, and receive a documented disposition. It SHALL triage urgent errors that could cause substantial harm promptly.

Corrections SHALL be propagated to affected products and customers where reasonably practicable, with an audit trail. Disputed data SHALL not be silently deleted to conceal a true adverse fact, and allegations SHALL not be presented as established findings.

O8. Conflicts, Independence and Commercial Influence

The platform SHALL disclose to the Council material ownership, referral, sponsorship, data-provider, or customer relationships that could affect review or presentation of findings and shall maintain controls for those conflicts.

Payment, advertising, preferred-provider status, or a customer relationship SHALL not buy a favorable verification outcome or suppress a material warning. Any paid placement or commercial preference SHALL be clearly separate from the factual vetting result.

O9. Security, Privacy and Service Providers

The platform SHALL apply role-based access, authentication, encryption appropriate to risk, logging, incident response, vendor oversight, and secure retention and disposal to sensitive records. It SHALL collect and expose only information reasonably necessary for the stated purpose.

A subcontractor or data vendor does not relieve the platform of responsibility for the accuracy of its own claims, access controls, and documented response to known feed failures. It SHALL protect confidential and personal data in accordance with applicable law and Appendix M.

O10. Monitoring, Incidents and Material Changes

The platform SHALL monitor source-feed health, material data quality, unauthorized access, significant false positives and false negatives, overrides, complaints, and mark misuse within its recognized scope. It SHALL investigate patterns and document corrective action.

It SHALL notify the Council without undue delay of a material breach, compromised verification process, systemic data error, or loss of a critical source that could undermine recognition. It SHALL report material ownership, product-scope, control, or methodology changes under Appendix H and its recognition agreement.

O11. Evidence and Independent Audit

The platform SHALL provide the Council a product and data-flow inventory; source and update-cadence matrix; sample time-stamped reports; documented rules, score meanings and change controls; dispute and incident procedures; security and access-control evidence; and a conflict disclosure. Sensitive details may be reviewed under controlled access.

Recognition review SHALL sample records across clear, unresolved, and adverse outcomes and test source traceability, currency, overrides, dispute handling, and correction propagation. Periodic and for-cause reviews follow Appendix H. A platform may protect trade secrets through appropriate confidentiality arrangements without withholding evidence needed to verify compliance.

O12. Agreement and Public Claims

The recognition agreement SHALL identify the approved legal entity, products, data or services, scope, effective period, reporting duties, audit access, mark use, and applicable enforcement and appeal provisions.

A Registry listing and mark SHALL state that recognition applies to the platform's approved vetting practices and scope. The platform SHALL not imply that its customers, listed carriers, brokers, or every data point are themselves Dalilah Standard recognized participants.

O. Third Party Vetting Platform Dalilah Standard Pledge and Recognition Acknowledgment

A third party vetting platform seeking or maintaining Dalilah Standard recognition shall execute this pledge as part of Appendix O.

- We will identify our sources and data age, state the limits of our checks, and distinguish verified facts from inferences and unresolved information.
- We will maintain documented decision logic, human review, audit trails, correction and dispute processes, security controls, and material-incident reporting within our approved scope.
- We will not allow payment or commercial preference to suppress material warnings or represent our private recognition as government approval or as recognition of the entities we assess.
- We accept the recognition, monitoring, mark-use, Registry, complaint, investigation, enforcement, and appeal rules applicable to this role.

Program Administrator: The Dalilah Standard Council

By signing below, I attest that I am authorized to bind the organization identified below, that the representations made for this recognition are truthful and materially complete, and that the organization voluntarily accepts the Dalilah Standard requirements applicable to this role, including monitoring, self-reporting, investigation, corrective action, suspension, revocation, permanent disqualification where authorized, Registry publication, and cessation of mark use when required.

Organization / Participant Legal Name: ____

DBA (if applicable): ____

Products / Services in Scope: ____

Authorized Representative: ____

Title: ____

Signature: ____ Date: ____________________

CONTROLLED FORMS AND IMPLEMENTATION CHECKLISTS

Form 1 - Initial Recognition Decision Record

- Applicant legal name and identifiers
- Role and scope
- Reviewer/evaluator
- Conflict check
- Evidence reviewed
- Red flags and supplemental screening
- Nonconformities
- Corrective actions
- Decision
- Decision-maker
- Effective/expiration dates
- Registry entry
- Next monitoring/revalidation date

Form 2 - Material Change Report

- Participant
- Date discovered
- Date reported
- Affected role/scope
- Description
- Immediate containment
- Supporting evidence
- External reporting if applicable
- Recognition impact assessment
- Reviewer disposition

Form 3 - Complaint Intake

- Case ID
- Date/source
- Confidentiality request
- Participant/entity
- Allegation
- Standard provision potentially implicated
- Evidence received
- Urgency
- Conflict screen
- Triage outcome

Form 4 - Enforcement Decision

- Case ID

- Eligible panel members
- Recusals
- Findings of fact
- Applicable provisions
- Evidence standard
- Vote
- Tie status if any
- Sanction
- Effective date
- Registry wording
- Appeal deadline

Form 5 - Audit Report

- Audit type
- Scope/population
- Sample methodology
- Evidence reviewed
- Findings
- Nonconformity classification
- Corrective action
- Verification of closure
- Auditor
- Independent decision review

Closing Statement

We hold ourselves to the Dalilah Standard because safer highways require more than minimum expectations. They require verification, documentation, accountability and the willingness to act when something does not make sense.

The Standard is not designed to punish legitimate businesses for honest, correctable mistakes. It is designed to make deliberate fraud, known unsafe conduct, concealment, evasion, retaliation and indifference to public safety incompatible with the privilege of displaying the Dalilah Standard designation.

Higher Standards. Safer Roads. Stronger Supply Chains.