BRINDLE OAK FREIGHT • ENTERPRISE POLICY FRAMEWORK

Access and Data Governance Policy

Information Security & Compliance | Commercial Trucking & Logistics Operations

■ Internal Controlled Document

Policy Number	
Policy Title	Access and Data Governance Policy
Version	2.0
Effective Date	July 16, 2026
Review Cycle	Annual (next review: July 2027)
Policy Owner	Chief Information Officer / Director of IT and Compliance
Approved By	Chief Operating Officer (COO)
Classification	**Internal Controlled Document**
Supersedes	BOF-POL-008 v1.x (all prior versions)
Distribution	All employees, contractors, owner-operators, and authorized third-party vendors

⚠️ Controlled Document Notice

This is a controlled internal document. Printed copies are uncontrolled. Always reference the current version maintained in the company document management system. Unauthorized distribution is prohibited.

■ Table of Contents

---

1. Purpose and Scope

1.1 Purpose

This policy establishes enterprise-wide standards for the access, classification, protection, and lifecycle governance of all company data assets and information systems. The primary objectives of this policy are to:

- Establish and enforce standards for controlling access to company systems, data, platforms, and network infrastructure;
- Define a consistent framework for classifying and protecting data assets appropriate to their sensitivity and regulatory exposure;

- Govern the full data lifecycle — from creation and collection through storage, use, transmission, and certified destruction;
- Ensure ongoing compliance with applicable federal and state privacy laws, data security regulations, and industry standards relevant to commercial trucking and logistics operations;
- Minimize the risk of unauthorized access, data breach, regulatory penalty, and operational disruption arising from inadequate information governance.

1.2 Scope

This policy applies universally and without exception to:

- **All employees** of the company, including full-time, part-time, and temporary personnel;
- **Contractors and consultants** engaged to perform services on behalf of the company;
- **Owner-operators** and leased drivers with access to any company system, application, or electronic logging device (ELD) platform;
- **Third-party vendors, suppliers, and service providers** granted access to any company network, system, application, or data asset;
- **All information systems, networks, devices, applications, and data assets** owned, leased, or operated by the company, regardless of physical location or hosting environment (on-premises, cloud, or hybrid).

> ⓘ **Scope Note**
>
> Individuals subject to this policy who fail to comply are subject to disciplinary action as outlined in Section 16. Acceptance of access credentials or system accounts constitutes acknowledgment of and agreement to comply with this policy.

2. Regulatory and Standards References

This policy is designed to satisfy requirements and align with guidance established by the following federal regulations, state laws, and industry frameworks. Compliance with this policy supports the company's posture under each reference below.

Reference	Description and Applicability	Applicability Trigger
49 CFR Part 395.38	FMCSA data security requirements for Electronic Logging Device (ELD) data, including transmission standards, data access controls, and authorized data sharing limitations.	All carrier operations using ELD-equipped vehicles
CCPA / CPRA	California Consumer Privacy Act and California Privacy Rights Act — consumer data rights, opt-out requirements, and data processing disclosures for California residents.	Operations involving California residents' personal data
GDPR	General Data Protection Regulation — strict requirements for collection, processing, and transfer of personal data belonging to EU/EEA residents.	International operations or EU-resident personal data
SOC 2 Type II	AICPA Trust Services Criteria covering Security, Availability, Confidentiality, Processing Integrity, and Privacy. Framework for demonstrating data security controls to customers and partners.	Customer contractual requirements; cyber insurance
NIST CSF 2.0	NIST Cybersecurity Framework — Identify, Protect, Detect, Respond, Recover functions used as the operational cybersecurity reference model for this policy.	Enterprise-wide cybersecurity governance
PCI-DSS v4.0	Payment Card Industry Data Security Standard — requirements for	If the company processes or stores cardholder data

Reference	Description and Applicability	Applicability Trigger
	organizations that process, store, or transmit cardholder data or payment card information.	
HIPAA / HITECH	Health Insurance Portability and Accountability Act — requirements for protected health information (PHI), applicable if employee health data is stored in company systems.	If company stores or processes employee health data
State Breach Notification Laws	All U.S. states maintain data breach notification statutes. Ohio requires notification within 45 days. Timelines vary significantly by jurisdiction. See Appendix D.	Any data breach involving personal information
Cyber Insurance Policy	Company's current cyber liability policy establishes minimum technical and procedural controls as conditions of coverage. Policy requirements are binding. IT Director maintains current policy requirements.	All operations; required for policy coverage

3. Definitions

The following terms carry specific meanings within this policy. All personnel subject to this policy are expected to understand these definitions.

Term	Definition
Data Asset	Any information or data in any format (digital or physical) that has value to the company, including records, files, databases, communications, reports, and system configurations.
Data Classification	The process of categorizing data assets into defined tiers (Public, Internal, Confidential, Restricted) based on sensitivity, regulatory exposure, and required handling controls.

Term	Definition
Access Control	Technical and administrative mechanisms that restrict access to systems and data only to authorized individuals based on verified identity and assigned permissions.
Role-Based Access Control (RBAC)	An access management model in which permissions are assigned to job roles rather than individuals. Users receive access by virtue of their assigned role within the organization.
Principle of Least Privilege	The requirement that users, systems, and applications be granted only the minimum level of access rights necessary to perform their defined job functions — nothing more.
Multi-Factor Authentication (MFA)	An authentication method requiring verification using two or more independent factors: something the user knows (password), something the user has (authenticator app or hardware token), or something the user is (biometric).
Single Sign-On (SSO)	An authentication framework allowing a user to log in once with a single set of credentials and gain access to multiple enterprise applications without re-authenticating for each.
Data Custodian	An individual or team (typically IT) responsible for the technical storage, maintenance, backup, security controls, and availability of data assets on behalf of the Data Owner.
Data Owner	The department head or senior manager accountable for a specific data asset or category of data, including decisions about classification, access, and retention.
Privileged Access	Elevated system rights beyond standard user permissions, including administrative access to servers, network devices, databases, and security systems. Subject to heightened controls under this policy.
Third-Party Access	System or data access granted to individuals not employed directly by the company, including vendors, contractors, consultants, auditors, or partner organizations.
Data Breach	Any unauthorized acquisition, access, use, disclosure, alteration, or destruction of protected data, whether intentional or accidental, that compromises its confidentiality, integrity, or availability.
Incident Response	The structured process for detecting,

Term	Definition
	containing, investigating, remediating, and reporting a security incident or data breach in accordance with established procedures.
Data Subject Rights	Legal rights afforded to individuals under applicable privacy law (e.g., CCPA, GDPR) regarding their personal data, including rights to access, correction, deletion, and opt-out.
Retention and Disposal	The management of data across its lifecycle including defined retention periods and certified destruction methods. Governed by BOF-POL-007 (Data Retention and Disposal Policy), which is incorporated by reference.
Shadow IT	Any hardware, software, application, service, or system used within the company without explicit IT department approval, oversight, or knowledge. Shadow IT is prohibited for systems that access or store Confidential or Restricted data.

4. Data Classification Framework

All company data must be classified into one of four tiers based on its sensitivity, regulatory exposure, and the potential impact of unauthorized disclosure. Data Owners are responsible for classifying data within their domain. When in doubt, data must be classified at the higher tier until reviewed. The classification framework is structured as follows:

> ⚠️ **Classification Responsibility**
>
> Data Owners (department heads) are accountable for classifying all data assets generated or held within their functional area. Unclassified data must be treated as **Internal** until formally classified. Misclassification that results in a breach is subject to review under Section 16.

Tier 1 — PUBLIC

Attribute	Details
Definition	Information intentionally made available to the general public, or whose unrestricted disclosure poses no risk to the company, its personnel, or its customers.
Examples	Marketing materials, public website content, press releases, public rate sheets, job postings, approved promotional content, company contact information.
Handling Requirements	No restrictions on sharing or distribution. May be posted publicly or shared with any party without approval. No encryption required for transit or storage.
Storage Standards	Standard company file systems or public-facing platforms. No special security controls required beyond basic integrity protections.
Labeling	No mandatory labeling required, though documents may optionally be marked "Public."

Tier 2 — INTERNAL

Attribute	Details
Definition	Information intended for use within the company only, whose unauthorized disclosure to external parties could cause reputational damage, competitive harm, or operational disruption, but would not constitute a regulatory violation or result in severe harm.
Examples	Internal operating procedures, company policies, employee directory, internal operational reports, meeting minutes, non-sensitive project documentation, training materials, general company announcements.
Handling Requirements	Internal distribution only. External sharing requires manager or department head approval. Must not be posted publicly or shared via personal email without documented authorization.
Storage Standards	Company-approved file systems and document management platforms. Access should be limited to relevant personnel but does not require individual-level permissions. Standard backup and access controls apply.

Attribute	Details
Labeling	Documents should be marked "Internal" in the header, footer, or watermark.

Tier 3 — CONFIDENTIAL

Attribute	Details
Definition	Sensitive information whose unauthorized disclosure could result in financial loss, regulatory penalty, significant reputational harm, legal liability, or harm to individuals. Includes personally identifiable information (PII) and commercially sensitive data.
Examples	Driver PII (name, address, date of birth, license number), financial records and statements, customer contracts, shipper rate agreements, ELD and telematics data, HR personnel files and performance records, safety investigation records, background check results (non-drug), insurance claim details.
Handling Requirements	Access granted on a strict need-to-know basis only. Encryption required both at rest (AES-256) and in transit (TLS 1.2 minimum). Must not be stored on personal devices without company-approved MDM enrollment. Prohibited from unapproved cloud storage platforms. Cannot be transmitted via unencrypted email. External sharing requires written approval and a data sharing agreement.
Storage Standards	Encrypted company servers, approved cloud platforms with DLP controls, or encrypted local device storage (company-issued and MDM-managed). Physical documents stored in locked cabinets when not in use.
Labeling	All documents, files, and emails must be marked "CONFIDENTIAL" prominently in the header or subject line.

Tier 4 — RESTRICTED

Attribute	Details
Definition	The highest sensitivity classification. Information whose unauthorized disclosure

Attribute	Details
	would cause severe harm to individuals, result in significant legal liability or regulatory action, or expose the company to criminal liability. Access is strictly limited to named, individually authorized personnel.
Examples	Drug and alcohol test results, Social Security numbers (SSN), banking and ACH payment data, cardholder data, attorney-client privileged communications and legal strategy documents, proprietary pricing algorithms, trade secrets, passwords and cryptographic keys, law enforcement-related records.
Handling Requirements	Maximum controls required. Access only by individually named and approved personnel — no group access. MFA required for every access event. Physical originals stored in locked, limited-access filing or secured encrypted digital storage only. Must never be transmitted via standard email. Destruction only by certified method (NIST 800-88 or physical destruction for media; cross-cut shredding minimum for paper). Any access event must be logged.
Storage Standards	Dedicated, access-controlled encrypted systems or physically secured locked storage. Separate from general company file systems. Cloud storage permitted only on approved platforms with dedicated encryption and individual-level access logging.
Labeling	All materials must be marked "RESTRICTED — AUTHORIZED PERSONNEL ONLY" in bold at the top of every page and in email subject lines.

5. Access Control Standards

5.1 Principle of Least Privilege

All users — employees, contractors, owner-operators, and vendors — shall be granted only the minimum level of system and data access necessary to perform their defined job function. Excess permissions are prohibited regardless of convenience or historical precedent. Access must be:

- Requested by the user's direct manager and approved by IT prior to provisioning;
- Reviewed and adjusted immediately upon any change in the user's role, position, or employment status;
- Revoked entirely upon offboarding, contract completion, or whenever the business need ceases;
- Regularly recertified as part of the quarterly and annual access review cadence (see Section 12.4).

5.2 Role-Based Access Control (RBAC)

Access to all enterprise systems is managed through a Role-Based Access Control model. IT maintains a current access matrix defining the standard permissions associated with each role in each system. Role provisioning requires documented manager approval submitted to IT via the company's IT service request system.

System / Platform	Defined Roles	Access Scope
TMS (Transportation Management System)	Dispatcher, Operations Manager, Driver (limited), Accounting Read-Only, TMS Admin	Load management, route data, carrier records, billing integration
ELD Platform	Driver (own records only), Safety Manager, Compliance Officer, ELD Admin	HOS logs, DVIR records, vehicle tracking, inspection data
Accounting / ERP	AP/AR Clerk, Controller, Payroll Admin, Auditor Read-Only, Finance Admin	Invoices, payments, payroll, financial statements
HRIS / HR System	Employee (self-service), HR Coordinator, HR Manager, Payroll Admin, HRIS Admin	Personnel files, benefits, performance records, DQF data
Document Management	General User, Department Contributor, Department Manager, DMS Admin	Policy documents, contracts, compliance records, SOP library

The full access matrix (by role and system) is maintained in Appendix B and updated by IT whenever roles are added, modified, or deprecated.

5.3 User Account Lifecycle

Lifecycle Stage	Trigger	Required Action	Deadline
Onboarding — New Hire	HR submits new hire notification to IT	IT provisions accounts and access based on approved role profile. User receives credentials on or before first day.	Within 24 hours of confirmed start date
Role Change / Transfer	HR submits role change notification to IT	Prior role access revoked; new role access provisioned. No access carryover without documented approval.	Within 48 hours of HR notification
Offboarding — Voluntary Separation	HR notifies IT of resignation/last day	All system accounts disabled; all credentials revoked; company device retrieval initiated; VPN and SSO tokens invalidated.	Within 4 hours of last working hour
Offboarding — Involuntary Termination	HR or COO notifies IT at time of termination meeting	All access revoked simultaneously with or before employee notification of termination. Remote wipe of company mobile devices authorized.	Immediately — within 1 hour of notification
Leave of Absence	HR notifies IT of leave commencement	Accounts suspended (not deleted) during leave. Reactivated upon confirmed return date.	On leave start date

5.4 Privileged Access Management

- Administrators requiring elevated system access must use a **separate, dedicated privileged account** (e.g., *admin.jsmith*) distinct from their standard user account. Standard accounts must not hold administrative rights.
- All privileged account sessions must be logged and retained for a minimum of 1 year. SIEM integration is required for real-time alerting on privileged activity anomalies.

- Privileged access is subject to **quarterly review** by the IT Director. Any privileged account not associated with a current, active administrative need must be immediately suspended.
- Just-in-time (JIT) privileged access controls are encouraged wherever technically feasible to reduce standing administrative privileges.

5.5 Third-Party and Vendor Access

- All third-party access requests must be submitted using the Vendor Access Request Form (Appendix C) and approved by the IT Director prior to access being granted.
- Vendor access must be scoped to the minimum permissions necessary to perform the contracted service.
- All third-party credentials are time-limited and must be set to expire upon contract end date. Standing vendor accounts are prohibited.
- A signed **Vendor Access Agreement** (referencing this policy and the company's information security requirements) is mandatory before credentials are issued.
- Vendor access is reviewed quarterly and revoked immediately upon contract completion, termination, or any violation of policy terms.

6. Authentication and Identity Standards

6.1 Password Policy

Requirement	Standard Account	Privileged Account
Minimum Length	12 characters	16 characters
Complexity	Must include uppercase, lowercase, number, and special character	Must include uppercase, lowercase, number, and special character
Expiration	90 days	60 days
History / Reuse	Last 12 passwords may not be reused	Last 24 passwords may not be reused

Requirement	Standard Account	Privileged Account
Failed Attempt Lockout	Account locked after 5 consecutive failed attempts	Account locked after 3 consecutive failed attempts; IT alert generated
Password Manager	Company-approved password manager recommended	Company-approved password manager required
Prohibited Patterns	Dictionary words, usernames, company name, sequential characters, keyboard patterns, or any previously breached password as identified by IT	

6.2 Multi-Factor Authentication (MFA)

MFA is mandatory under the following conditions without exception:

- All remote access to company systems from any external network (VPN, cloud portals, web applications);
- All access to systems containing Confidential (Tier 3) or Restricted (Tier 4) data;
- All privileged account logons, regardless of access location;
- All access to the company's email platform, HR system, accounting/ERP system, and document management platform.

MFA Method	Status	Applicable Use Case
Authenticator App (TOTP)	**Preferred**	All standard user and privileged remote access
SMS One-Time Code	Permitted (fallback only)	When authenticator app is unavailable; not permitted for Restricted-tier systems
Hardware Security Token (FIDO2/YubiKey)	Required for highest-privilege accounts	IT administrators, CIO, system root-level access
Email-Based OTP	Not permitted	Prohibited — email compromise would defeat the MFA purpose

6.3 Single Sign-On (SSO)

SSO must be implemented for all enterprise applications where the technology supports it. SSO simplifies access management, improves audit logging, and reduces password fatigue-related vulnerabilities. Applications that do not support

SSO integration must be documented as exceptions and reviewed annually. All SSO implementations must integrate with the company's identity provider (IdP) and must enforce MFA at the IdP level.

6.4 Shared and Generic Accounts

Shared or generic accounts (e.g., *dispatcher@company.com* used by multiple individuals) are **strictly prohibited** on any system containing Confidential or Restricted data. All individuals must authenticate with uniquely assigned credentials traceable to a single identity. Exceptions require:

- Documented and specific business justification;
- Written approval from the IT Director;
- Compensating controls (e.g., shared account activity logging at session level); and
- A defined expiration date for the exception.

7. System and Network Access Governance

7.1 Network Segmentation

The company's network infrastructure must be logically segmented to prevent unauthorized lateral movement between environments. The following network segments must be maintained as isolated zones:

- **Corporate Network:** Administrative workstations, servers, and enterprise applications. Highest protection tier.
- **Driver/ELD Network:** Dedicated segment for ELD devices and in-cab telematics. Isolated from corporate network. Internet access restricted to ELD platform hosts.
- **Guest Network:** Internet access only. No access to any internal resource or corporate system. Isolated from all other segments.
- **Production vs. Development:** Production and development/test environments must be logically isolated. Test environments must not contain

live Confidential or Restricted data without specific IT Director approval and compensating controls.

7.2 Remote Access

- VPN is required for all access to internal company systems from any external network. Direct internet-facing access to internal systems is prohibited without IT-approved security controls (e.g., zero-trust network access).
- Split-tunneling configurations must be reviewed and approved by IT. All Confidential and Restricted data traffic must route through the company VPN regardless of split-tunnel configuration.
- Endpoint compliance must be verified before VPN connection is granted. Non-compliant endpoints (outdated OS, missing EDR agent, failed disk encryption check) must be denied access until remediated.
- VPN credentials are subject to all password and MFA requirements in Section 6.

7.3 Mobile Device Management (MDM)

All devices — company-issued or personal (BYOD) — that access company email, applications, or data must be enrolled in the company's MDM platform before access is granted. MDM enrollment is a non-negotiable condition of access. MDM policies applied to all enrolled devices include:

- Device screen lock enforcement (maximum 5-minute inactivity timeout);
- Full device encryption required;
- Approved application list enforced;
- Remote wipe capability enabled and authorized upon device loss, theft, or separation from the company;
- OS patch compliance enforcement (maximum 30-day lag for critical patches).

7.4 Wireless Network Standards

- All company wireless networks must use WPA3 encryption as a minimum standard. WPA2 networks must be remediated to WPA3 or decommissioned.

- Guest wireless networks must be physically or logically isolated from corporate infrastructure with no route to internal resources.
- SSID broadcast controls must be configured; default manufacturer SSIDs are prohibited.
- Rogue access point detection must be enabled on corporate wireless infrastructure. IT must investigate all detected rogue APs within 4 hours.

7.5 ELD and Telematics Systems

- Access to ELD data and telematics platforms is restricted to authorized Safety, Compliance, and Operations personnel as defined in the System Access Matrix (Appendix B).
- ELD data transmission must meet all encryption requirements specified under 49 CFR 395.38, including secure data transfer to roadside inspectors via approved ELD output methods only.
- Driver personal conveyance time, off-duty status, and rest period data must be treated as Confidential (Tier 3) and access restricted to Safety and Compliance personnel on a need-to-know basis.
- ELD platform vendor access to company ELD data must be governed by a current Data Processing Agreement (see Section 10.2).

8. Data Handling Procedures

8.1 Data in Transit

- TLS 1.2 is the minimum required encryption protocol for all data transmission over any network. TLS 1.3 is preferred. SSL and TLS 1.0/1.1 are prohibited and must be disabled on all company-controlled endpoints and servers.
- Unencrypted email (standard SMTP) must not be used to transmit any Confidential or Restricted data. Secure email, encrypted file transfer, or the company's approved file-sharing platform must be used instead.

- Bulk data transfers to external parties must use a company-approved secure file transfer protocol (SFTP or equivalent) with authentication logging.

8.2 Data at Rest

- AES-256 encryption is required for all Confidential and Restricted data stored on servers, databases, network-attached storage, backup media, and portable devices.
- All company-issued laptops must have full-disk encryption enabled (e.g., BitLocker or equivalent) as a condition of deployment. Unencrypted company laptops may not access Confidential or Restricted data.
- Database encryption must be implemented for all databases containing Confidential or Restricted data. Encryption keys must be stored separately from the encrypted data.

8.3 Removable Media

- USB drives and other removable media are prohibited on workstations and servers containing Confidential or Restricted data unless IT has issued an encrypted, company-controlled drive specifically for the purpose.
- All removable media usage on company systems must be logged by endpoint management tools. Unauthorized removable media events generate an IT alert.
- Removable media containing Confidential or Restricted data must be stored securely when not in use and destroyed using certified methods when no longer needed.

8.4 Cloud Storage

Storage Platform	Status	Conditions
Company-approved enterprise cloud (e.g., Microsoft 365 OneDrive/SharePoint)	**Approved**	Subject to company access controls, DLP policies, and audit logging. MFA required.
Company-approved TMS cloud storage	**Approved**	Per platform access matrix; DPA required with vendor.

Storage Platform	Status	Conditions
Personal Google Drive, Dropbox, iCloud, or equivalent	**Prohibited**	Personal cloud storage must not be used for any company data, regardless of classification. Violation subject to enforcement under Section 16.
Unapproved third-party cloud platforms	**Prohibited (Shadow IT)**	Any cloud platform not on the IT-approved list is prohibited. Requests for new platforms must be submitted to IT for review and approval prior to use.

8.5 Printing and Physical Documents

- Confidential and Restricted documents must be retrieved from the printer immediately upon printing. Unattended sensitive documents in printer output trays constitute a policy violation.
- Secure shredding bins must be available at all office locations. Documents classified as Confidential or Restricted must not be placed in standard recycling or trash receptacles.
- Clean desk policy applies to all workstations: Confidential and Restricted materials must be secured in locked storage when the employee is away from their desk or at end of day.
- Physical copies of Restricted documents (e.g., drug test results, SSN records) must be stored in locked, limited-access filing with an access log.

9. Driver and Field Personnel Data Governance

9.1 ELD Data Rights and Privacy

Drivers have the right to review their own ELD records, including Hours of Service (HOS) logs and Driver Vehicle Inspection Reports (DVIRs). The company must provide drivers with access to their own data upon reasonable request. The following controls govern ELD data disclosure:

- ELD data may be shared with authorized FMCSA roadside inspectors during roadside inspections using the approved transfer methods (telematics output or display) as required by 49 CFR 395.38;
- ELD data must **not** be shared with unauthorized third parties, brokers, or carriers without the driver's written consent and a specific business and legal justification;
- Blanket third-party sharing of ELD data is prohibited under any circumstances;
- All ELD data access by internal personnel must be role-restricted and logged.

9.2 Driver PII Protection

- Driver Qualification File (DQF) data — including employment applications, MVRs, background check results, medical certificates, and training records — is classified as **Confidential (Tier 3)** and access is restricted to Safety and HR personnel with a documented need.
- Driver Social Security Numbers and Driver's License numbers must **never** be transmitted via standard email. Secure messaging or encrypted file transfer must be used.
- Driver SSNs stored in company systems must be masked in display and encrypted at rest. Access to unmasked SSN data requires Restricted-tier controls.
- Driver PII must not be used for any purpose other than employment, compliance, and safety administration without explicit consent.

9.3 Field Device Security

- All company-issued tablets, phones, and in-cab devices are subject to MDM enrollment and policies described in Section 7.3.
- Drivers and field personnel must report lost or stolen devices **within 1 hour of discovery** to their dispatcher and to the IT department using the emergency device report procedure.

- Remote wipe of a lost or stolen company-issued device may be authorized by the IT Director or on-call IT administrator without further approval delay.
- Personal devices used for company communications must be MDM-enrolled before any company email or application access is granted.

10. Third-Party and Vendor Data Governance

10.1 Vendor Risk Assessment

Before any vendor, supplier, or service provider is granted access to Confidential or Restricted company data or systems, a formal security risk assessment must be completed and approved by the IT Director. Assessment requirements include:

- Completion of the company's Vendor Security Questionnaire (included in Appendix C);
- Review of the vendor's most recent SOC 2 Type II report (or equivalent attestation) if available;
- Evaluation of the vendor's incident response and breach notification capabilities;
- Confirmation of the vendor's data encryption and access control practices;
- Annual reassessment required for all vendors with ongoing Confidential or Restricted data access.

10.2 Data Processing Agreements (DPA)

A signed Data Processing Agreement is mandatory before any vendor may process personal data on behalf of the company. The DPA must include, at minimum:

- Clear description of the data processed, purpose, and lawful basis;
- Data security obligations aligned with this policy's standards;
- Breach notification obligation (vendor must notify the company within 24 hours of discovery);
- Data deletion or return obligations upon contract termination;

- Restrictions on vendor use of company data for any purpose other than the contracted service;
- Company's right to audit the vendor's data security practices.

Legal/Compliance is responsible for reviewing and executing all DPAs. No DPA may be signed by operational or IT personnel without Legal approval.

10.3 Data Sharing Agreements

Any sharing of Confidential company data with brokers, freight partners, customers, or other external parties must be governed by a formal written data sharing agreement, using company-approved templates maintained by Legal/Compliance. Ad hoc or verbal data sharing authorizations for Confidential data are prohibited.

10.4 Subprocessor Management

- All vendors processing company data must disclose their subprocessors (third parties they engage to assist in service delivery).
- Company approval is required before a vendor may engage a subprocessor that will have access to Restricted data.
- Vendor contracts must include a requirement to notify the company before adding or replacing subprocessors and to impose equivalent data protection obligations on subprocessors.

11. Data Breach and Incident Response

> ⚠️ **Critical — Mandatory Response Timelines Apply**
>
> All personnel who suspect or discover a data breach or security incident must report it immediately to the IT department or their manager. Delayed reporting may result in regulatory penalties and is subject to disciplinary action under Section 16.

11.1 Breach Detection Sources

- SIEM real-time alerts and anomaly detection;

- Employee and driver reports of suspicious activity;
- Third-party security researchers or partner notifications;
- Regulatory authority notification (e.g., law enforcement, FTC, state AG);
- Vendor or subprocessor breach notification.

11.2 Incident Response Procedure

Phase	Action Required	Responsible Party	Deadline
1 — Contain	Isolate affected systems, revoke compromised credentials, block malicious activity at network level.	IT / System Administrators	**Within 1 hour of detection**
2 — Assess	Determine scope: systems affected, data categories exposed, individuals impacted, likely source.	IT Director + Legal	**Within 4 hours of detection**
3 — Notify (Internal)	Notify Director of IT and COO. Brief on scope, containment status, and preliminary risk.	IT Director	**Within 2 hours of detection**
4 — Notify (Legal)	Engage Legal/Compliance for regulatory notification obligations and attorney-client privilege preservation.	CIO / IT Director	**Within 4 hours of detection**
5 — Remediate	Patch, restore, verify integrity of systems. Implement additional controls to prevent recurrence.	IT / System Administrators	Per remediation plan; no unnecessary delay
6 — Report	File required regulatory notifications per state law and federal requirements. Notify cyber insurer.	Legal / CIO	Per jurisdiction (see Appendix D); typically 72 hours–30 days

Phase	Action Required	Responsible Party	Deadline
7 — Post-Incident Review	Root cause analysis completed. Lessons learned report circulated. Policy and control updates implemented.	IT Director + All stakeholders	**Within 5 business days of incident closure**

11.3 Regulatory and Insurance Notification

- State attorney general and affected residents must be notified according to applicable state breach notification law timelines (see Appendix D). Legal is responsible for identifying the correct jurisdiction and timeline;
- If ELD data is compromised, FMCSA must be notified as required under 49 CFR Part 395;
- The company's cyber liability insurance carrier must be notified per the terms of the current policy. IT Director maintains the carrier's breach notification contact information and policy requirements.

11.4 Driver and Employee Notification

Affected individuals (drivers, employees, customers) must be notified of a breach involving their personal data within the timeframes mandated by applicable state law. Notification letters must be reviewed by Legal before distribution and must include:

- Description of what data was involved;
- Date of the breach (or estimated date range);
- Steps the company is taking to remediate;
- Steps individuals can take to protect themselves;
- Offer of credit monitoring services (minimum 12 months) for any breach involving SSNs, financial account numbers, or other high-risk identifiers.

12. Audit Logging and Monitoring

12.1 Required Audit Logs

The following events must be captured in audit logs across all applicable systems. IT is responsible for configuring and maintaining log collection infrastructure.

Log Category	Events Captured	Systems Covered
Authentication Events	Successful login, logout, failed login attempts (with source IP), account lockouts, MFA success/failure, password changes	All company systems, VPN, email, SSO IdP
Privileged Account Activity	All actions performed under privileged credentials, including configuration changes, account management, and data exports	All systems; admin consoles; server access
Data Access — Restricted Tier	Every access, read, modify, copy, or export of Restricted-classified data	HRIS, drug test database, payment systems, legal document repository
File Access — Confidential/Restricted	File open, download, copy, share, delete, rename events on Confidential and Restricted files	Document management system, cloud storage, file servers
System Configuration Changes	Firewall rule changes, group policy changes, user provisioning/deprovisioning, permission changes, system settings modifications	Network infrastructure, identity provider, all enterprise platforms
VPN and Remote Access	VPN connection events, source IP, session duration, endpoint compliance status at connection	VPN gateway, remote access platform
Removable Media	USB and removable media insertion/removal events on managed endpoints	All company-managed workstations and servers

12.2 Log Retention

- Audit logs must be retained for a **minimum of 1 year in an immediately accessible (online) state**;
- Logs must be retained for a **minimum of 2 years in archived storage** (secure, retrievable);
- Logs for systems subject to PCI-DSS must be retained for a minimum of 12 months with immediate availability for the last 3 months;

- Logs subject to litigation hold must be retained for the duration of the legal matter plus 1 year.

12.3 Log Integrity and SIEM

- All audit logs must be written to tamper-evident, write-once storage. Administrators with access to monitored systems must not have the ability to delete or modify logs from those same systems.
- All critical log sources must be integrated with the company's Security Information and Event Management (SIEM) platform for real-time correlation and alerting.
- SIEM alert rules must be maintained and reviewed quarterly by IT to ensure effectiveness and relevance.

12.4 Access Review Cadence

Review Type	Frequency	Responsible Party	Scope
Automated Access Report Review	Quarterly	IT / System Administrators	All active accounts across enterprise systems; flag dormant, excess-privilege, and orphaned accounts
Full Access Recertification	Annual	Department Heads	Each department head certifies that all access held by their team members is current, necessary, and appropriate
Privileged Account Review	Quarterly	IT Director	All accounts with administrative or elevated permissions reviewed and individually justified
Triggered Review	Immediate (upon trigger)	IT Director + affected Department Head	Triggered by: security incident, breach event, role change, or regulatory finding

13. Roles and Responsibilities

Role	Key Responsibilities	Accountability
All Employees, Contractors, and Owner-Operators	Comply with all requirements of this policy Protect credentials and report suspected compromise immediately Report suspected security incidents or policy violations Complete all required security awareness training on time Adhere to data classification and handling requirements	Accountable to their direct manager and the CIO. Non-compliance subject to Section 16 enforcement.
Data Owners / Department Heads	Classify all data assets within their functional domain Approve or deny access requests for their department's systems and data Conduct annual access recertification for all team members Escalate data handling violations within their department	Accountable to the CIO for classification accuracy and access recertification completion.
IT / System Administrators	Implement and maintain all technical security controls Manage the full user account lifecycle (provisioning, changes, deprovisioning) Maintain audit log infrastructure and SIEM platform Lead incident response containment and remediation Perform quarterly access reviews and privileged account reviews Maintain and enforce MDM and endpoint compliance standards	Accountable to the IT Director for technical control effectiveness and response timelines.
CIO / Director of IT and Compliance	Own this policy and ensure annual review and maintenance Oversee	Accountable to the COO for enterprise information security posture and policy

Role	Key Responsibilities	Accountability
	vendor risk management and assessment program Lead breach notification decisions in coordination with Legal Drive security investment and control prioritization decisions Report cybersecurity posture to COO and executive leadership Approve exceptions and maintain the exception register	compliance.
Legal / Compliance	Ensure policy alignment with applicable regulations and laws Review and execute all Data Processing Agreements and data sharing agreements Manage regulatory breach notification obligations and timelines Advise on data subject rights requests and responses Oversee litigation hold compliance for data and logs	Accountable to the COO and company counsel for regulatory compliance and legal risk management.
Human Resources	Trigger timely IT provisioning and deprovisioning notifications Enforce policy violations through the disciplinary process Maintain access restrictions for sensitive HR and personnel data Track and report security awareness training completion Coordinate device retrieval upon employee offboarding	Accountable to the COO for timely provisioning/deprovisioning and policy enforcement support.

14. Security Awareness Training

A comprehensive security awareness training program is essential to maintaining a security-conscious organizational culture. Human error is among the most significant sources of data breach risk, and training is a primary control to mitigate that risk.

Training Component	Audience	Frequency / Deadline	Tracking
Annual Security Awareness Training	All employees, contractors, and owner-operators	Annually; completion required within 30 days of assignment	LMS or HR system; IT generates completion report monthly
New-Hire Onboarding Security Training	All new employees and contractors	Must be completed within 15 calendar days of start date	HR system; completion is condition of continued system access
Phishing Simulation Program	All employees with email access	Minimum quarterly simulations; individuals who click must complete remedial training within 5 days	Phishing platform; results reported to IT Director and HR quarterly
Specialized IT Administrator Training	IT staff, system administrators, security personnel	Annual; includes advanced threat response, privileged access management, incident response	IT Director verifies completion and maintains certifications log
Data Custodian / Data Owner Training	Department heads and designated data custodians	Annual; includes classification framework, DPA responsibilities, access recertification process	IT Director; completion required before annual access recertification is performed
Driver-Specific ELD and Device Security Training	All company drivers and owner-operators	At onboarding; annual refresher; upon significant ELD platform changes	Safety/HR department; included in driver qualification file

Consequences for Non-Completion: Failure to complete mandatory security awareness training by the required deadline may result in suspension of system access until training is completed, a formal written warning, and escalation to HR for inclusion in the employee's performance record. Repeated non-compliance is subject to disciplinary action under Section 16.

15. Policy Exceptions

Compliance with all provisions of this policy is mandatory. Exceptions to policy requirements may be granted in limited circumstances where a documented, specific business need exists and compensating controls adequately mitigate the associated risk.

15.1 Exception Request Process

1. The requesting manager submits a written exception request to the IT Director, including: (a) the specific policy provision for which an exception is requested; (b) the business justification; (c) the proposed duration of the exception; and (d) proposed compensating controls.
2. The IT Director reviews the request and assesses the risk of the exception, consulting Legal/Compliance where regulatory implications exist.
3. The IT Director approves or denies the request in writing. Exceptions for Restricted-tier data or systems require co-approval from the COO.
4. Approved exceptions are documented in the Policy Exception Register maintained by IT, including the approval date, expiration date, and compensating controls.
5. All active exceptions are reviewed quarterly. Exceptions may be revoked if business need has lapsed or compensating controls prove insufficient.

> ⚠️ **Exception Limitations**
>
> No exception may be granted that would place the company out of compliance with a federal regulation (including 49 CFR 395.38 or FMCSA requirements) or state law. Exceptions that would violate regulatory requirements are automatically denied and referred to Legal for guidance.

16. Non-Compliance and Enforcement

Violations of this policy are taken seriously and subject to a tiered enforcement framework based on severity, intent, and impact. All violations are investigated by IT and HR before disciplinary action is taken. The company reserves the right to apply any appropriate measure given the specific circumstances of a violation.

Violation Tier	Examples	Consequences
Minor Violation (First Offense / Inadvertent)	Missing training deadline, password shared with colleague, sensitive document left unattended, personal cloud storage used for non-critical data	Mandatory remedial security training Formal documented written warning placed in personnel file Manager notification Follow-up review within 30 days
Significant Violation (Reckless or Repeated)	Unauthorized access to another employee's data, sharing Confidential data with unauthorized external parties, disabling security controls, repeated minor violations, failure to report a known breach	Formal HR investigation Suspension of system access during investigation Disciplinary action up to and including termination of employment Regulatory notification if required by applicable law Civil liability referral if damages are incurred
Malicious Violation (Intentional / Criminal)	Intentional data theft, deliberate data destruction, selling company data, sabotaging systems, unauthorized access for personal gain, intentional breach enabling	Immediate termination of employment or contract Referral to local, state, and/or federal law enforcement Civil litigation for damages, including loss of revenue and breach remediation costs Criminal prosecution pursued to the fullest extent of the law Notification to regulatory authorities as required

This policy applies equally to all personnel regardless of position, seniority, or tenure. Executives and managers are held to the same standards and subject to the same enforcement framework as all other personnel.

17. Policy Review and Amendment

- This policy is subject to a **formal annual review** by the CIO/IT Director and Legal/Compliance, scheduled no later than 12 months from the effective date or the date of the prior review, whichever comes first.
- In addition to the scheduled annual review, a **triggered review** must be initiated within 30 days of any of the following events: a confirmed data breach or significant security incident; a material change in applicable federal or state law or regulation; a significant change to company information systems, technology platforms, or operations; or a finding from an external audit or cyber insurance assessment.
- All amendments must be approved by the COO prior to publication. Minor editorial corrections that do not alter the substance of any requirement may be made by the IT Director and noted in the version log.
- Version control is maintained by IT. All superseded versions are archived in the document management system and remain accessible for historical reference. Personnel are bound by the current version as of its effective date.

Version	Date	Change Summary	Approved By
1.0	January 15, 2024	Initial policy release	COO
1.1	August 3, 2024	Added ELD data rights provisions (Section 9.1); updated MFA requirements	CIO
1.2	February 10, 2025	Updated breach notification timelines; added MDM standards	CIO
2.0	July 16, 2026	Full policy revision: expanded classification framework; added vendor DPA requirements; updated password standards to 12-	COO

Version	Date	Change Summary	Approved By
		character minimum; added phishing simulation program; updated regulatory references to NIST CSF 2.0 and PCI-DSS v4.0; restructured enforcement tiers	

Policy Approval and Authorization

By signature below, the undersigned authorize the publication and enforcement of this policy effective July 16, 2026.

Chief Information Officer / Director of IT and Compliance Policy Owner — BOF-POL-008 v2.0
Date: _____

Chief Operating Officer
Approving Authority — BOF-POL-008 v2.0 Date: _____

Appendices

APPENDIX A

Data Classification Quick Reference Card

This reference card provides a condensed summary of the Data Classification Framework (Section 4) for day-to-day operational use. Post at workstations and include in onboarding materials.

Tier	Label	Common Examples	Key Rule
TIER 1	**PUBLIC**	Marketing materials, public rate sheets, job postings, press releases	No restrictions. Share freely.
TIER 2	**INTERNAL**	Internal procedures, employee directory, operational reports, company policies	Internal only. No external sharing without manager approval.
TIER 3	**CONFIDENTIAL**	Driver PII, financial records, customer contracts, shipper rates, ELD data, HR records	Need-to-know only. Encrypt always. No personal devices. No unapproved cloud. Mark all documents.
TIER 4	**RESTRICTED**	Drug test results, SSNs, banking/payment data, attorney-client docs, trade secrets	Named individuals only. MFA every time. Encrypted storage only. Certified destruction. Log all access.

ⓘ **When In Doubt — Classify Up**

If you are unsure what tier applies to a piece of data, treat it as one tier higher until your manager or IT clarifies. It is always safer to over-protect than to under-protect.

APPENDIX B

System Access Matrix by Role

This matrix defines standard access levels by job role across core enterprise systems. IT maintains the authoritative version in the IT service management system. This appendix is informational. Legend: RW = Read/Write, RO = Read Only, ADM = Administrator, NONE = No Access, LTD = Limited Self-Service Only.

Role	TMS	ELD Platform	Accounting / ERP	HRIS	Document Mgmt
Driver / Owner-Operator	LTD (own loads)	LTD (own records)	NONE	LTD (self-service)	RO (policies only)
Dispatcher	RW	RO	NONE	NONE	RW (operations folder)
Operations Manager	RW	RO	RO	NONE	RW
Safety / Compliance Officer	RO	RW	NONE	RO (DQF only)	RW (safety folder)
HR Coordinator	NONE	NONE	RO (payroll summary)	RW	RW (HR folder)
HR Manager	NONE	NONE	RO	RW (full)	RW (HR + policy)
AP/AR Clerk	RO	NONE	RW (assigned modules)	NONE	RW (finance folder)
Controller / Finance Manager	RO	NONE	RW (full)	RO (payroll)	RW
IT Administrator	ADM	ADM	ADM	ADM	ADM
CIO / IT Director	ADM	ADM	RO	RO	ADM
COO	RO	RO	RO	RO	RO
Third-Party Vendor	LTD (per agreement)	LTD (per agreement)	NONE	NONE	LTD (per agreement)

Any access beyond the above standard matrix requires documented manager approval and IT Director authorization. Access matrix is reviewed and updated by IT quarterly and upon any organizational change.

APPENDIX C

Vendor Access Request and Security Assessment Form

Complete this form for all third-party vendors, contractors, or service providers requiring access to company systems, networks, or data classified as Internal, Confidential, or Restricted. Submit to IT Director for review and approval prior to granting any access.

Part 1 — Requestor Information

Requesting Manager Name:	
Department:	
Date of Request:	
Vendor Company Name:	
Vendor Primary Contact Name:	
Vendor Contact Email:	
Contract / SOW Reference:	
Contract Start Date:	
Contract End Date (Access Expiration):	

Part 2 — Access Requested

System / Application	Access Level Requested	Business Justification

Data Classification of Data Accessed:	☐ Public ☐ Internal ☐ Confidential ☐ Restricted
Is personal/PII data involved?	☐ Yes ☐ No
Is a Data Processing Agreement required?	☐ Yes — DPA attached ☐ No — Justification:

Part 3 — Vendor Security Assessment (Completed by Vendor)

Security Question	Vendor Response
Does your organization have a documented information security policy?	☐ Yes ☐ No
Do you hold a current SOC 2 Type II report or equivalent attestation?	☐ Yes — provide copy ☐ No
Do you require MFA for access to systems containing client data?	☐ Yes ☐ No
Is data encrypted at rest and in transit?	☐ Yes ☐ No
Do you conduct annual security awareness training for all employees?	☐ Yes ☐ No
Do you have a documented incident response plan?	☐ Yes ☐ No
Will you notify the company within 24 hours of discovering a breach involving company data?	☐ Yes ☐ No
List any subprocessors who will access company data:	

Part 4 — IT Director Approval

Assessment Outcome:	**☐ Approved ☐ Approved with Conditions ☐ Denied**
Conditions / Notes:	
IT Director Signature:	
Date:	

APPENDIX D

Data Breach Notification Checklist and State Timelines

This appendix provides a post-breach action checklist and a reference table of notification deadlines for key states. Legal/Compliance is responsible for confirming current requirements at time of breach. State laws change frequently — this table reflects general guidance as of the effective date of this policy.

Breach Notification Action Checklist

Step	Action	Responsible Party	Completed
1	Isolate affected systems and contain the breach	IT / SysAdmin	☐
2	Preserve evidence — do not destroy logs or forensic data	IT Director	☐
3	Notify CIO/IT Director and COO	First Responder	☐
4	Engage Legal/Compliance; establish attorney-client privilege for investigation	CIO	☐
5	Notify cyber insurance carrier per policy terms	CIO / Legal	☐
6	Determine scope: data categories, individuals affected, jurisdictions involved	IT + Legal	☐
7	Assess notification obligations under applicable state laws (see table below)	Legal	☐
8	Draft individual notification letters (reviewed by Legal before sending)	Legal / HR	☐
9	Notify state attorney general(s) per applicable requirements	Legal	☐
10	If ELD data compromised, notify FMCSA	Legal / Safety	☐
11	Send individual notifications and offer credit monitoring if SSN exposed	HR / Legal	☐
12	Complete root cause analysis and lessons learned report	IT Director	☐

Step	Action	Responsible Party	Completed
	(within 5 business days of closure)		
13	Update policy, procedures, and controls as applicable	CIO	☐

State Breach Notification Timeline Reference

Note: These timelines represent notification to affected individuals unless otherwise noted. Many states also require notification to the state Attorney General. Consult Legal for current requirements at time of breach.

State	Notification Deadline (Individuals)	AG Notification	Key Statute
Ohio	45 days	If 500+ Ohio residents affected	ORC § 1349.19
California	"Expedient time" / no unreasonable delay	If 500+ California residents; sample notice to AG	Cal. Civ. Code § 1798.29
Texas	60 days	AG notification required	Tex. Bus. & Com. Code § 521.053
Florida	30 days	If 500+ Florida residents	Fla. Stat. § 501.171
Illinois	"Expedient time" / no unreasonable delay	AG notification if 500+ affected	815 ILCS 530/10
Pennsylvania	"Expedient time" / no unreasonable delay	AG notification required	73 P.S. § 2303
New York	"Expedient time" — AG recommends 30 days	AG notification required	NY Gen. Bus. Law § 899-aa
Georgia	Expedient time / no more than 60 days	Not expressly required	O.C.G.A. § 10-1-912
Tennessee	60 days	AG notification if 1,000+ affected	Tenn. Code § 47-18-2107
Federal / FMCSA	Notify FMCSA upon confirmation of ELD data breach	N/A	49 CFR 395.38
EU / GDPR	72 hours to supervisory	Lead supervisory authority (EU)	GDPR Art. 33–34

State	Notification Deadline (Individuals)	AG Notification	Key Statute
	authority; individuals "without undue delay"		

APPENDIX E

Security Awareness Training Completion Tracking Template

This template is used by IT and HR to track mandatory security awareness training completion for all personnel. Maintained in the company's HR system or LMS. Generated reports are provided to the IT Director and department heads quarterly.

Employee / Contractor Name	Department	Employee Type	Annual Training Assigned	Annual Training Completed	New Hire Training Due	New Hire Training Completed	Phishing Sim Q1	Phishing Sim Q2	Phishing Sim Q3	Phishing Sim Q4	Status
[Last, First]	[Dept]	☐ FT ☐ PT ☐ Contractor	[Date]	[Date or Pending]	[Date or N/A]	[Date or N/A]	☐ Pass ☐ Fail ☐ N/A	☐ Pass ☐ Fail ☐ N/A	☐ Pass ☐ Fail ☐ N/A	☐ Pass ☐ Fail ☐ N/A	☐ Compliant ☐ Overdue ☐ Remedial Required

Summary Reporting Block (Complete Quarterly)		
Reporting Period:	**Total Personnel in Scope:**	**Overall Compliance Rate:**

Summary Reporting Block (Complete Quarterly)		
Annual Training Completion %:	**New Hire Training On-Time %:**	**Phishing Click Rate This Quarter:**
Overdue / Non-Compliant Individuals:	**Remedial Training Required (Count):**	**Report Prepared By:**