Vendor Risk Assessment Framework

NMFTA™ National Motor Freight Traffic Association, Inc. | CYBER

VENDOR RISK ASSESSMENT CHECKLIST

Section	Question	Vendor Response	Compliance Level	Follow-Up Action Req	Reviewer Notes
Pre-Contract	Is there an individual responsible for cybersecurity within your organization?				
Pre-Contract	Do you have a CISO or equivalent leadership role?				
Pre-Contract	Have you experienced a major cybersecurity incident? If so, how was it handled?				
Pre-Contract	Do you use any subcontractors or fourth-party service providers (MSP or MSSP, Others)?				
Pre-Contract	When was your last external cybersecurity assessment or penetration test?				
Contractual Safeguards	Do your service agreements include breach notification terms, access limitations, and audit rights?				
Contractual Safeguards	What controls are in place to secure, or out-of-band communications (email, portals, other)?				
Contractual Safeguards	Are service termination or liability clauses included for cybersecurity non-compliance?				

Section	Question	Vendor Response	Compliance Level	Follow-Up Action Req	Reviewer Notes
Contractual Safeguards	Do you maintain a removable media policy?				
Contractual Safeguards	Are your contractual terms reviewed by legal and security jointly?				
Vendor Categorization	What systems or data will your services interact with?				
Vendor Categorization	Would an outage in your systems impact our operations?				
Vendor Categorization	How do you classify sensitive data, and what protections are in place?				
Vendor Categorization	What critical infrastructure or cloud dependencies do you rely on (AWS, Azure, GCP)?				
Vendor Categorization	Are your systems integrated into our network or isolated?				
Onboarding & Integration	What access will your personnel or tools require?				
Onboarding & Integration	How do you implement least privilege access?				
Onboarding & Integration	Do you use secure credential vaulting, MFA, or SSO integration?				
Onboarding & Integration	Who will serve as our technical point of contact?				
Onboarding & Integration	Do you inventory and document third-party access by role?				

Section	Question	Vendor Response	Compliance Level	Follow-Up Action Req	Reviewer Notes
Monitoring & Ongoing Review	How do you monitor for suspicious behavior across endpoints or networks?				
Monitoring & Ongoing Review	Do you conduct regular internal/external vulnerability scans or red team exercises?				
Monitoring & Ongoing Review	How will you notify us of a breach affecting our data?				
Monitoring & Ongoing Review	Do you have an external security monitoring service (CyHy or other)?				
Monitoring & Ongoing Review	Can we schedule annual or event-driven reviews of your cybersecurity program?				

NOTES