BAKER DONELSON

THIRD-PARTY VENDOR CYBERSECURITY DUE DILIGENCE CHECKLIST

Given the proliferation of third-party cyber incidents, businesses should conduct the appropriate level of due diligence on third-party vendors and suppliers that access, create, or transfer data on the business' behalf to ensure adequate security controls. Third-party vendor contracts should also be carefully reviewed to ensure acceptable protection to the business in the event that the third-party vendor experiences a cyber incident that impacts the business.

The following is a template **cybersecurity due diligence checklist** for evaluating vendors and suppliers. This template should be tailored to the specific industry, regulatory requirements, and unique risk profile of the business to ensure relevance and effectiveness.

CYBERSECURITY DUE DILIGENCE CHECKLIST FOR VENDORS AND SUPPLIERS

GENERAL INFORMATION

- ☐ Company name, location, and contact details.
- ☐ Description of services/products provided.
- ☐ Points of contact for security and compliance.

SECURITY GOVERNANCE

- ☐ Is there a Chief Information Security Officer (CISO) or equivalent?
- ☐ Does the vendor have a dedicated security team?
- ☐ Are there documented security policies and procedures?
- ☐ Are employees trained regularly on cybersecurity awareness?

COMPLIANCE AND CERTIFICATIONS

- ☐ SOC 2 Type II, ISO/IEC 27001, NIST, or other relevant certifications.
- ☐ GDPR, HIPAA, CCPA, or other applicable regulatory compliance.
- ☐ Results of recent third-party audits or assessments.

DATA PROTECTION AND PRIVACY

- ☐ Is data encrypted at rest and in transit?
- ☐ Are data retention and disposal policies in place?
- ☐ Is there a data classification and handling policy?

ACCESS CONTROLS

- ☐ Are role-based access controls implemented?
- ☐ Is multi-factor authentication (MFA) required for access?
- ☐ Are regular access reviews and audits conducted?

NETWORK AND INFRASTRUCTURE SECURITY

- ☐ Are firewalls and intrusion detection/prevention systems (IDS/IPS) in place?
- ☐ Is there regular vulnerability scanning and patch management?
- ☐ Are regular code reviews and penetration testing performed?

BAKER DONELSON

INCIDENT RESPONSE AND BREACH NOTIFICATION

- ☐ Is there a documented incident response plan?
- ☐ Is there a history of past security incidents or breaches?
- ☐ Are breach notification timelines and procedures defined?

BUSINESS CONTINUITY AND DISASTER RECOVERY

- ☐ Are business continuity and disaster recovery plans in place?
- ☐ What is the frequency of testing these plans?
- ☐ Are there backup procedures and data recovery capabilities?

THIRD-PARTY RISK MANAGEMENT

- ☐ Does the vendor assess its own vendors (fourth parties)?
- ☐ Are subcontractors held to the same security standards?
- ☐ Are there flow-down clauses in contracts?

CONTRACTUAL AND LEGAL PROTECTIONS

- ☐ Are there security and privacy clauses in the contract?
- ☐ Is there a right to audit or assess the vendor's security posture?
- ☐ Are there indemnification and liability clauses for data breaches?

NetDiligence AUTHORIZED BreachCoach

Baker Donelson has a toll-free incident response hotline that is available 24/7 if an incident occurs: 877.215.6115

www.bakerdonelson.com/data-incident-response