Vital Components to Consider When Engaging with a Third-Party Vendor as Part of a Supply Chain Contract

REMINDER: The information contained here is not intended to be used in lieu of an actual attorney's review of a contract but rather as an awareness tool for suggested items to consider when reviewing contracts with a cybersecurity component when engaging with a third-party vendor as part of a supply chain.

IMPORTANT: Have a signed nondisclosure agreement with parties to protect the precontract negotiations as well as confidential and/or proprietary information that may be shared as part of that process.

Minimum Standard 1	**Audit Rights**
Due Diligence	Ask to review any third-party security assessments and/or SOC2 reports.
	RED FLAG: any vendor unwilling or unable to provide third-party security assessments.
Contracting	Require right to audit controls directly or by a third party.
	Define recourse when not met.
Monitoring and Performance	Evaluate capability of client to perform audit and understand output.
	Frequency of monitoring?
	Output Examples: Assessment questionnaire, Updated SOC2 reports

Minimum Standard 2	**Data Ownership, Usage, Encryption, and Disposal**
Due Diligence	Review and understand all key terms and exceptions within the contract.
	Procedures around collecting personal Information as required by law must be defined and restrictions on disclosing that information must be documented.
	If contract permits data to be stored outside of the United States, other laws, rules and regulations will apply.
	If accessing client data or contacting customers of client, vendor must have defined and enforced operational procedures that ensure the confidentiality, integrity and availability of Personally Identifiable Information or other Confidential Information.
Contracting	The client shall own all right, title and interest in and to the data that is related to the vendor services.
	Identify data disposition that will occur in an agreed upon time frame at contract termination: Vendor shall possess the means to recover and return client data within thirty (30) days of termination of the contract in a file format reasonably requested by client.
	Promptly following return of client data to client, vendor shall destroy all copies of client data in its possession or in the possession of its contractors in such a way that Client data cannot reasonably be recovered and shall certify completion of such destruction to client.
	Client must have access to data at all times.
	Vendor will permit its personnel and subcontractors to access data remotely only as required to provide technical or call center support.
	Encryption of non-public data in transit and at rest.
	Vendor shall cooperate with client in obtaining consent from users to collect personal Information, giving users the ability to access, correct, opt-out, delete, restrict, make portable, or object to the processing of personal information. (Opt-out provisions are not currently applicable in every state. Understand the jurisdictions covered by the contract before agreeing not to offer opt-out options.)

Monitoring and Performance	Privacy – Monitor and audit Vendor controls to ensure appropriate processing and protection of Personally Identifiable Information. National identification numbers must not be utilized as User IDs for logon to applications.
Minimum Standard 3	**Representations and Warranties**
Due Diligence	Determine who bears the risk for a breach.
	Understand exceptions within contract definitions.
	Understand the services being provided and your own responsibilities as identified within the contract.
Contracting	Ensure vendor provides warranties for product quality, functionality, sustainability and security and privacy controls and a warranty against introducing harmful code or viruses.
	Ensure vendor provides warranty that services will be performed in a professional and workmanlike manner and in accordance with generally accepted industry standards, using personnel with the requisite skill, experience and qualifications.
	Ensure vendor provides warranty that any Deliverables do not violate, infringe or misappropriate any intellectual property right of any third party.
Monitoring and Performance	Use security rating service sites such as https://www.bitsight.com/ to monitor vendor security controls based on third-party sources.
	Require that vendor provide an annual certification of security services.

Minimum Standard 4	**Security**
Due Diligence	Confirm vendor has a documented information security program.
	When vendor's security program lacks maturity or when unsure about vendor information security program, consider requiring the vendor to hold cyber security insurance to mitigate any security control gaps. Client should be named as additional insured on insurance policy.
Contracting	The vendor shall develop, implement, maintain, monitor and comply with a written information security program that contains administrative, technical and physical safeguards appropriate to the nature and scope of its activities to protect against anticipated threats to the security, confidentiality, integrity of or unauthorized access to or loss of Confidential or Personally Identifiable Information.
	Vendor shall ensure that any subcontractors leveraged in providing the contracted product or service comply with all terms of the contract and that vendor remains responsible for performance by subcontractors.
Monitoring and Performance	Verify presence of appropriate threat and vulnerability protection.
	Ensure access to test results demonstrating the effectiveness of vendor's security program.
	Ensure vendor's employees are provided data security training.

Minimum Standard 5	**Threat/Breach Detection and Notification**
Due Diligence	Ensure vendor has a documented protocol for prompt client notification when it is impacted by an incident that compromises the security, confidentiality or integrity of client data (a "Security Breach").

Contracting	Include language in the contract related to who receives notification of incidents and breaches, by what means, and within what timeframe. Notification should be made directly to contracted client and not the client's customers.
	Include language that specifies if contract can be terminated if a Security Breach occurs and includes details related to a termination/transition to new vendor. Note: Some contract provisions may continue to exist after the termination of the contract.
	Vendor should be obligated, at its own cost, to provide reasonable assistance and cooperation to Client in investigating any Security Breach and should pay all costs and losses of Client in responding to a Security Breach.
Monitoring and Performance	Incident Response Plans, Response Procedure Playbook, Security Operations Center Procedures; and how/how often these plans are tested.

Minimum Standard 6	**Vendor Business Continuity / Resiliency / Governance**
Due Diligence	If a critical vendor, are there documented Incident Response/Business Continuity/Disaster Recovery plans to ensure service resiliency and does it conduct regularly scheduled functional exercises of these plans?
	Determine if vendor uses a third party to host its product. If the third-party host's service is down, the vendor's service could be down as well. Identify remedies and expectations if that were to occur.
Contracting	Define the priority the vendor will give the client in a contingency situation that impairs the vendor's performance.
Monitoring and Performance	Verify Business Continuity/Resiliency Exercise Plans and confirm that these plans are tested.

Term	**Definition**
Client	An entity that contracts for services from a vendor as part of a supply chain. The highest-risk services from a cybersecurity perspective involve vendors that require access to client networks or data or that store client data or host client services on their own platforms (also known as "cloud providers").
Vendor	A contracted provider services to a client. The vendor may, in turn, use subcontractors in connection with providing services, which creates so-called "fourth-party risk." Clients should be aware of any subcontractors used by vendors and evaluate how that impacts the risk profile.
Confidential Information	Consists of documents, data, recordings, statements (verbal or written), renderings, plans, schematics, etc., considered private or proprietary based upon designation of such in an Agreement, or established legal or industry standards.
National Identity Number	In the U.S., this is the Social Security Number (SSN), but over 100 countries have national identity systems that include a registration number legally linked to an individual.
Personally Identifiable Information	Any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor. This definition differs by state and country and triggers obligations for reporting a Security Breach.

References	Link
State of Delaware Cloud Terms and Conditions	https://webfiles.dti.delaware.gov/pdfs/pp/Delaware%20Cloud%20Services%20Terms%20and%20Conditions%20Agreement.pdf
State of Delaware Data Usage Terms and Conditions	https://webfiles.dti.delaware.gov/pdfs/pp/Delaware%20Data%20Usage%20Terms%20and%20Conditions%20Agreement.pdf
ABA Cybersecurity Legal Task Force Vendor Contracting Project	https://www.potteranderson.com/media/publication/941_Vendor%20Contracting%20Project%20-%20Cybersecurity%20Checklist.pdf
JP Morgan Chase Supplier Minimum Control Requirements	https://www.jpmorganchase.com/content/dam/jpmc/jpmorganchase-and-co/documents/supplier-minimum-control-requirements.pdf
JP Morgan Chase New FSI Suppliers	https://www.jpmorganchase.com/content/dam/jpmc/jpmorgan-chase-and-co/documents/suppliers-documents/guidance-new-fsi-suppliers.pdf
JP Morgan Chase Supplier Incident Response Procedure Best Practice Recommendations	https://www.jpmorganchase.com/content/dam/jpmc/jpmorgan-chase-and-co/documents/Supplier%20Incident%20Response%20Procedure%20-%20Best%20Practice%20Recommendations.pdf