OFFICE OF THE
STATE AUDITOR

Privacy Provisions for Vendor Contracts

The following are basic privacy clauses to consider including in third-party contracts when sharing personal, sensitive, confidential, or proprietary data. Review with your legal counsel before use and adjust as needed. This document is for educational purposes only and does not constitute legal advice.

Legal Compliance: The Vendor shall comply with federal and state data protection laws and regulations in relation to the services provided under this contract.

Data Protection and Security: The Vendor shall implement and comply with federal and state technical, physical, and administrative regulations to ensure the security and confidentiality of the [contracting party's] data. The Vendor shall employ industry-standard security measures and best practices to safeguard the data. Such measures may include, but are not limited to, encryption, access controls, firewalls, intrusion detection systems, regular security assessments, and employee training on data protection and security.

Confidentiality: The Vendor shall maintain the strict confidentiality of the [contracting party's] data and shall not disclose it to any third party without obtaining the [contracting party's] prior written consent. The Vendor shall ensure that its personnel involved in the processing of data are subject to confidentiality obligations and are aware of the importance of maintaining the security of the data.

Use of Data: The Vendor shall use the [contracting party's] data solely for the purposes explicitly specified in the contract and may not use the data for any other purpose without obtaining the [contracting party's] prior written consent.

Subcontracting: In the event that the Vendor intends to subcontract any services under this contract, they shall ensure that subcontractors comply with the privacy clauses required by the Vendor and obtain the [contracting party's] approval of the subcontractors engaged.

Breach[1] Notification: The Vendor shall promptly notify the [contracting party] within 24 hours of any verified or suspected breach of data security, unauthorized disclosure, or misuse of the [contracting party's] data, as defined by federal and state law. Further, if it is unclear whether an event may be considered a breach, unauthorized disclosure, or misuse of data as defined in the contract, the Vendor shall err on the side of caution and disclose the event to the [contracting party]. The Vendor shall fully cooperate with the [contracting party] during the

[1] Breach is typically defined as: the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: a person other than an authorized user accesses or potentially accesses regulated data such as personally identifiable information, personal information or personal data, or an authorized user accesses such data for another than authorized purpose.

investigation and mitigation of the breach and shall provide the [contracting party] with all relevant details regarding the breach, including the nature of the breach, the data affected, the potential consequences, and any remedial actions taken or proposed to address the breach. Vendor is obligated to get a [contracting party's] approval before circulating a notice of breach to the impacted individuals or regulatory bodies. <<Define breach>>

Data Deletion: Upon termination of the contract, the Vendor shall securely delete or return all of the [contracting party's] data as specified in the contract, ensuring that the data is securely and irreversibly deleted to prevent unauthorized access or recovery and providing a Certificate of Destruction within 14 days from contract termination.

Liability and Insurance: The Vendor shall assume full liability for any damage or loss arising from a confirmed or suspected breach of data security or privacy, or its investigation, and shall maintain adequate insurance coverage that specifically includes data privacy protection throughout the term of the contract as well as throughout the term the vendor holds or in any way uses the [contracting party's] data. The Vendor shall provide to the [contracting party] a certificate of insurance satisfactory to the [contracting party] before services provided.

The Vendor acknowledges that its liability for any damage or loss arising from or connected to a data security breach or privacy violation shall not be limited solely to the extent of insurance coverage, and the Vendor remains fully responsible for any liabilities beyond the insurance coverage limits.

Audit Clause: The [contracting party] has the right to conduct audits, on-site or virtually, to verify the Vendor's compliance with the contract. The [contracting party] may choose to conduct the audit themselves or engage a third-party auditor, and the Vendor shall fully cooperate with the audit process.