

SAM – INFORMATION SECURITY
(Office of Information Security)

PROVISIONS FOR AGREEMENTS WITH STATE AND NON-STATE ENTITIES
(Revised 12/13)

5305.8

Introduction: State entities are required to enter into written agreements with state and non-state entities when they engage such entities in the development, use, or maintenance of information systems, products, solutions, or services.

Policy: Each state entity shall ensure agreements with state and non-state entities include provisions which protect and minimize risk to the state. Agreements shall include, at a minimum, provisions which cover the following:

1. Appropriate levels of security (confidentiality, integrity and availability) for the data based on data categorization and classification and [FIPS Publication 199](#) protection levels.
2. Standards for transmission and storage of the data, including encryption and destruction, if applicable.
3. Agreements to comply with statewide policies and laws regarding the use and protection of information resources and data, including those set forth in this Chapter.
4. Signed confidentiality statements.
5. Agreements to apply security patches and upgrades, and keep virus software up-to-date on all systems on which data may be used.
6. Agreements to notify the state data owners promptly if a security incident involving the information system or data occurs.
7. Agreements that the data owner shall have the right to participate in the investigation of a security incident involving its data or conduct its own independent investigation, and that data custodian shall cooperate fully in such investigations.
8. Agreements that the data custodian shall be responsible for all costs incurred by the data owner due to security incident resulting from the data custodian's failure to perform or negligent acts of its personnel, and resulting in an unauthorized disclosure, release, access, review, or destruction; or loss, theft or misuse of an information asset. If the contractor experiences a loss or breach of data, the contractor shall immediately report the loss or breach to the data owner. If the data owner determines that notice to the individuals whose data has been lost or breached is appropriate, the contractor will bear any and all costs associated with the notice or any mitigation selected by the data owner. These costs include, but are not limited to, staff time, material costs, postage, media announcements, and other identifiable costs associated with the breach or loss of data.
9. Agreements that the data custodian shall immediately notify and work cooperatively with the data owner to respond timely and correctly to public records act requests.
10. Agreements between the data custodian and data owner to address the appropriate disposition of records held by the data custodian during the term of its agreement with the data owner.

Implementation Controls: NIST SP 800-53, [System and Services Acquisition \(SA\)](#)