INFORMATION SECURITY PROGRAM 5305

(Revised 6/14)

Policy: Each state entity is responsible for establishing an information security program. The program shall include planning, oversight, and coordination of its information security program activities to effectively manage risk, provide for the protection of information assets, and prevent illegal activity, fraud, waste, and abuse in the use of information assets.

Each state entity shall:

1. Align the information security program, its activities, and staff with the requirements of this Chapter;
2. Establish a governance body to direct the development of state entity specific information security plans, policies, standards, and other authoritative documents;
3. Oversee the creation, maintenance, and enforcement of established information security policies, standards, procedures, and guidelines;
4. Ensure the state entity's security policies and procedures are fully documented and state entity staff is aware of, has agreed to comply with, and understands the consequences of failure to comply with policies and procedures;
5. Identify and integrate or align information security goals and objectives to the state entity's strategic and tactical plans;
6. Develop and track information security and privacy risk key performance indicators;
7. Develop and disseminate security and privacy metrics and risk information to state entity executives and other managers for decision making purposes; and
8. Coordinate state entity security efforts with local government entities and other branches of government as applicable.

Implementation Controls: NIST SP 800-53: Planning (PL); Program Management (PM)