

SAM – INFORMATION SECURITY
(Office of Information Security)

SYSTEM DEVELOPMENT LIFECYCLE

5315.2

(Revised 11/2019)

Policy: Each state entity shall manage its information assets using a documented SDLC methodology that:

1. Incorporates information security (data confidentiality, integrity and availability) including business impact assessment requirements and considerations;
2. Incorporates information privacy protection requirements and considerations;
3. Incorporates technology recovery requirements and considerations, per SAM Sections 5325-5325.6 and SIMM Section 5325-A and SIMM Section 5325-B;
4. Defines and documents operational information security roles and responsibilities throughout the information asset lifecycle including, but not limited to adoption of secure coding practices and security and vulnerability testing during test phases;
5. Defines and documents operational information privacy roles and responsibilities throughout the information asset lifecycle;
6. Identifies individuals having information security roles and responsibilities;
7. Identifies individuals having information privacy roles and responsibilities;
8. Identifies individuals and entities having technology recovery roles and responsibilities;
9. Integrates the organizational information security risk management process into the development lifecycle activities;
10. Integrates the Privacy Threshold Assessment (PTA) for all information system projects and proposals, and the Privacy Impact Assessment (PIA) into the system development lifecycle activities when personal information or a privacy risk is involved. PTA and PIA shall be through the use of SIMM 5310-C; and
11. Integrates the organizational technology recovery solution that meets the business recovery requirements and the recovery plan within the security risk management process into the development lifecycle activities.

Implementation Controls: NIST SP 800-53:

- [System and Services Acquisition \(SA\) and Accountability, Audit, and Risk Management \(AR\); Appendix J – Privacy Control Catalog, FIPS 199](#)
- [SIMM 5310-C](#)