

**SAM – INFORMATION SECURITY**  
**(Office of Information Security)**

**INFORMATION SYSTEM BACKUPS**

5325.6

(Revised 12/13)

**Policy:** Each state entity shall perform regularly scheduled backups of system and user-level information. Backups shall be:

1. Conducted at the operating system, application, and user level;
2. Conducted of information system documentation including security-related documentation;
3. Stored in a protected locations; and
4. Securely destroyed upon expiration of retention period.

System-level information includes system-state information, operating system and application software, and software licenses. User-level information includes any information other than system-level information. Mechanisms to protect the integrity of information system backups shall include digital signatures and cryptographic hashes. Information system backups shall reflect the requirements in contingency plans as well as other state entity requirements for backing up information.

**Implementation Controls:** NIST SP 800-53: [Contingency Planning \(CP\)](#)