

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

**ENCRYPTION**  
(Revised 12/13)

**5350.1**

**Policy:** End-to-end encryption or approved compensating security control(s) shall be used to protect confidential, sensitive, or personal information that is transmitted or accessed outside the secure internal network (e.g., email, remote access, file transfer, Internet/website communication tools) of the state entity, or stored on portable electronic storage media (e.g., USB flash drives, tapes, CDs, DVDs, disks, SD cards, portable hard drives), mobile computing devices (e.g., laptops, netbooks, tablets, and smartphones), and other mobile electronic devices. In rare instances where encryption cannot be implemented, compensating control(s) or alternatives to encryption must be in place. Compensating controls and alternatives to encryption must be reviewed on a case-by-case basis and approved in writing by the state entity ISO, after a thorough risk analysis.

**Implementation Controls:** FIPS 140-2, FIPS 197, NIST SP 800-53: [Access Control \(AC\)](#), and [System and Communications Protection Controls \(SC\)](#)