

SAM – INFORMATION SECURITY
(Office of Information Security)

OPERATIONAL SECURITY
(Revised 6/14)

5350

Introduction: In order to mitigate against successful attacks, each state entity is responsible for separating and controlling access to various systems and networks with different threat levels and sets of users which may operate or interface within their technology environment.

Policy: Each state entity shall develop, implement, and document, disseminate, and maintain operational security practices which include, but are not limited to:

1. A network security architecture that:
 - a. includes distinct zones to separate internal, external, and DMZ traffic; and
 - b. segments internal networks to limit damage, should a security incident occur.
2. Firewall, router, and other perimeter security tools which enforce network security architecture decisions.
3. Periodic review of perimeter security access control rules to identify those that are no longer needed or provide overly broad access.

Each state entity's security architecture shall align with the following security controls and best practices:

1. Application partitioning;
2. Denial of service protection;
3. Boundary protection;
4. Confidentiality of transmitted information or appropriate compensating security controls if protection assurances cannot be guaranteed; and
5. Cryptographic protections using modules that comply with FIPS-validated cryptography.

Implementation Controls: NIST SP 800-53: [System and Information Integrity \(SI\)](#); [System and Communications Protection \(SC\)](#)