

SAM – INFORMATION SECURITY
(Office of Information Security)

IDENTITY AND ACCESS MANAGEMENT
(Revised 6/14)

5360

Policy: Each state entity shall safeguard access to information assets by managing the identities of users and devices and controlling access to resources and data bases on a need to know basis throughout the identity lifecycle. Each state entity shall establish processes and procedures to ensure:

1. Maintenance of user identities, including both provisioning and de-provisioning;
2. Enforcement of password policies or more advanced multifactor mechanisms to authenticate users and devices;
3. Management of access control rules, limiting access to the minimum necessary to complete defined responsibilities;
4. Separation of duties to avoid functional conflicts;
5. Periodic recertification of access control rules to identify those that are no longer needed or provide overly broad clearance;
6. Use of privileged accounts that can bypass security are restricted and audited;
7. Systems to administer access based on roles are defined and installed; and
8. Encryption keys and system security certificates are effectively generated, exchanged, stored and safeguarded.

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