

SAM – INFORMATION SECURITY
(Office of Information Security)

ENDPOINT DEFENSE

5355

(Revised 01/19)

Policy: Each state entity shall be responsible for protecting information on computers that routinely interact with untrusted devices on the internet or may be prone to loss or theft.

Each state entity shall develop and implement capabilities, methods and techniques to manage processes and tools to:

1. Detect malicious software;
2. Permit only trusted software to run on a device, commonly referred to as white listing;
3. Prevent certain software from running on a device, commonly referred to as blacklisting;
4. Identify unauthorized changes to secure configurations;
5. Encrypt confidential and sensitive data; and
6. Comply with the Endpoint Protection Standard (SIMM 5355-A)

Implementation Controls: Endpoint Protection Standard (SIMM 5355-A); NIST SP 800-53: [System and Information Integrity \(SI\)](#)