



S T A T E O F M A R Y L A N D
DEPARTMENT OF INFORMATION TECHNOLOGY

Publicly Accessible Systems Policy

1.0 Purpose

The purpose of this policy is to define standards to be met by all publicly accessible systems owned and/or operated by the Department of Information Technology (DoIT). These standards are designed to minimize the potential exposure to DoIT from the loss of data confidentiality, integrity and availability.

2.0 Scope

All publicly accessible systems or devices deployed owned and/or operated by DoIT and/or registered in any Domain Name System (DNS) domain owned by DoIT must follow this policy. This policy also applies to widely accessible systems that may not be exposed to Internet traffic but are accessible to outside (untrusted) entities. This policy also covers any systems outsourced or hosted at external/third-party service providers, if that equipment resides in the "[DBM/DoIT/GOV].state.md.us" domain or appears to be owned by DoIT.

3.0 Policy

All publicly or widely accessible systems shall be separated from internal networks by a firewall. Additionally, all hardware, operating systems, services and applications must be approved by DoIT as part of the planning phase. Communications between systems shall only be introduced according to business requirements and must be documented and approved by DoIT. Publicly accessible systems shall not store confidential information.

All vendor recommended patches, hot-fixes or service packs must be installed prior to deployment and processes must be in place to keep system hardware, operating system and applications current based on vendor support recommendations (including patches, hot-fixes, and service packs).

System inventory must be documented and maintained. At a minimum, the following information is required:

- Business owner contact name
- Hardware and operating system/version.
- Primary system purpose
- Applications installed
- Protocols required for public and management access

Password groups must be maintained in accordance with agency password management procedures. Access to application services shall be restricted to DoIT approved mechanisms and protocols. System management access shall be limited to authorized personnel and system management access shall utilize approved secure communication methods.

Antivirus solutions shall be implemented and updated using vendor specified recommendations. Services not required by the primary system/business purpose must be disabled. Additionally, default administrative account names and passwords shall be changed or disabled.

Insecure services or protocols (as determined by DoIT) must be replaced with more secure equivalents whenever such exist.

Security-related events must be logged and audit trails saved for a minimum of seven days. Access to system logs must be granted to DoIT management upon request. Security-related events include (but are not limited to) the following:

- Login failures
- Failure to obtain privileged access
- Access policy violations

3.1 Change Management Procedures

DoIT must review and approve all configuration change requests and perform system/application audits prior to the deployment of new services.

3.2 Equipment Outsourced to External Service Providers

If the DoIT publicly accessible system is outsourced, it is the responsibility of the business owner to ensure that the contractor is aware of the compliance requirements associated with this policy.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. External service providers found to have violated this policy may be subject to financial penalties, up to and including termination of contract.

5.0 Definitions

Confidential Information	Non-Public information that is deemed private, privileged or sensitive.
Private Information	Personally identifiable information (PII) that, if exposed, may cause harm to an individual. Harm, in this context, meaning any adverse effects that would be experienced by an individual whose PII was the subject of a loss of confidentiality,
Privileged Information	Records protected from disclosure by the doctrine of executive privilege which may include but not limited to records: <ul style="list-style-type: none"> • Relating to budgetary and fiscal analyses, policy papers, and recommendations made by the Department or by any person working for the Department; • Provided by any other agency to the Department in the course of the Department's exercise of its responsibility to prepare and monitor the execution of the annual budget; • Relating to a State procurement when a final contract award has not been made or when disclosure of the record would adversely affect future procurement activity; • Of confidential advisory and deliberative communications relating to the preparation of management analysis projects conducted by the Department pursuant to State Finance and Procurement Article, §7-103, Annotated Code of Maryland.
Sensitive Information	Information that, if divulged, could compromise or endanger the citizens or assets of the State.