



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

**DoIT, DBM, MEMA, and Executive Office of the Governor (EOG) Firewall Policy**

**1.0 Introduction**

Firewalls are an essential component of DoIT, DBM, and EOG's security infrastructure. They are defined as security systems that control and restrict both network connectivity and services. Firewalls serve as a perimeter defense mechanism separating trusted and un-trusted networks.

**2.0 Scope**

This policy shall apply to all firewalls owned, rented, leased, or otherwise managed by DoIT personnel.

**3.0 Policy**

Departures from this policy will be permitted only if approved by the Chief Information Security Officer and/or the Director, Enterprise Information Services.

**3.1 Firewall Platform**

All DoIT managed firewalls must run on secured, dedicated devices and may not serve other purposes, for instance; act as web servers.

**3.2 Physical Security**

All DoIT managed firewalls must be located in secured rooms accessible only to those who have management's permission to enter such area.

**3.3 Configuration**

All default administrator credentials shall be changed including SNMP strings (disable SNMP if not used). Firewall management access shall be restricted to approved personnel utilizing secure protocols. Telnet must be disabled. All unused firewall services must be disabled. All traffic passing through the firewall must be strictly defined by pre-approved access-lists, all other traffic must be denied. Current firewall configurations must be backed up and stored on a separate platform. Firewall code must be upgraded and patched in a timely manner when vendor security flaws have been identified and deemed relevant to the current operational environment.

**3.4 External Connections**

All external Internet traffic destined to DoIT, DBM, and/or EOG must pass through a firewall and be directed to a secured de-militarized zone (DMZ). Internal network services must only be accepted from defined DMZ's. No direct connections originating from the Internet may be permitted to the internal local area network.

### 3.5 Change Control

All firewall configuration changes shall be pre-approved by the Chief Information Security Officer and/or the Director, Enterprise Information Services and must be documented. Firewall rules will be reviewed on a regular basis and any rule not used for 90 days will be de-activated or removed.

### 3.6 Logging

All firewalls shall have full event logging enabled and logs must be stored for a minimum of 30 days. A process must be implemented to analyze stored logs in an effort to identify suspicious activity and/or hardware/configuration errors on a daily basis.

### 4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

### 5.0 Definitions

De-militarized zone (DMZ)	Also known as a Data Management Zone or demarcation zone, is a physical or logical subnetwork that contains and exposes an organization's external services to a larger, untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's Local Area Network (LAN); an external attacker only has access to equipment in the DMZ, rather than the whole of the network.
SNMP	Simple Network Management Protocol is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention.