Tier 1 Control Standards (State-Wide)

**Internet Filtering**

**Standard ID**
IOT-CS-SEC-112

**Published Date**
6/1/2006

**Effective Date**
6/1/2006

**Last Updated**
5/19/2017

**Next Review Date**
5/19/2018

**Policy**
06.0 Access Control (PR.AC)
06.4 PR.AC-4
06.4.1 Identity Access Management

**Purpose**
Computing resources are only to be used for State government business except as permitted by the agency's de minimis policy. This Internet Blocking Standard is describes the enforcement of that policy as it relates to the computing resources used for internet access.

**Scope**
All Devices that Connect to the State Network

**Statement**
There are three categories of Internet sites that potentially violate State use policy. The first category covers those sites that can reasonably be determined to be morally offensive or illegal. The second category includes web activities that have operational implications (e.g. – excessive bandwidth usage). The third category is those sites that typically have no business use and whose extensive use may suggest abuse of time.

The State policy is to deny access to sites within the parameters described below rather than to police Internet activity. Agencies may police usage as a general routine or upon identification of an acute concern. Internet activities from logs may also be researched by law enforcement agencies and the State Personnel Department. Logs are only monitored by IOT to review the effectiveness of blocking schemes and to determine drivers of Internet bandwidth usage. The activity log is rolling and overwrites itself when space demands. Data from these requests will be the property of the requesting agency.

The State employs the use of hardware and software filters provided by a vendor whose business it is to develop and maintain up-to-date listings of web sites and categories of those web sites. The devices are placed at a single point of access to the Internet so that most State users are affected equally. The filters are configured to prevent access to sites that are in the categories covered by this policy. The State receives and implements updates to this software daily so that the site lists remain as current as possible. If someone using the State Internet resources attempts to access a non-permitted site, they will receive a message that indicates such site is in violation of State policy and access is denied. The following Internet traffic categories, as maintained by the filter vendor, are blocked:

- Internet Radio / TV
- Streaming Media
- Gambling
- Gambling Related
- Games
- Chat
- Instant Messaging
Roles
All Personnel

Responsibilities
All personnel are responsible for understanding the requirements of this Standard, and are not to attempt to circumvent requirements without explicit approval.

Management Commitment
Management is responsible for ensuring their agency is meeting the requirements written within this standard.
Coordination Among Organizational Entities
Agencies shall coordinate with IOT where necessary to apply the appropriate internet filter settings.

Compliance
Agencies shall periodically review and audit their internet filter exception list and work with IOT to maintain least privilege.

Exceptions
Exceptions will be handled on a case by case basis through the State CISO.