State of Nevada

Information Security Committee

Standard

Control No.	Rev.	Title	Effective Date	Page
144	A	Suspension of Services	05/31/2017	1 of 3

1.0 PURPOSE

This standard establishes the criteria to use when determining whether to deny access to State IT resources.

2.0 SCOPE

This standard applies to any entity, regardless of physical location, that operates, manages, or uses State IT services or equipment.

3.0 EFFECTIVE DATES

This standard becomes effective at the time of approval of the State Chief Information Officer (CIO).

4.0 RESPONSIBILITIES

Agency heads and agency IT heads have the responsibility to ensure that their agency complies with the requirements of this Security Standard.

5.0 RELATED DOCUMENTS

State Information Security Consolidated Policy 100, Section 4.8, Security Incident Management
State Information Security Consolidated Policy 100, Section 5.4, Network Security
NIST 800-53, Rev. 4, Security and Privacy Controls, IR Incident Response Control Family
NIST 800-53, Rev. 4, Security and Privacy Controls, SC System and Communications Control Family
NIST 800-53, Rev. 4, Security and Privacy Controls, SI System and Information Integrity Control Family

6.0 STANDARD

A. The following conditions shall be used to determine if a suspension of services is justified:

1) A recognizable pattern of malicious activity.

2) Any activity from an entity that constitutes an emergency (see definitions). This can be permanent or temporary, depending on the particular activity.

3) Any entity identified as a cyber security threat by law enforcement or the Department of Homeland Security or other IT security oversight applicable to the Department or Division.

4) Any entity that violates applicable Nevada Revised Statutes (NRS), Federal or international law, State or agency security policies, standards, and procedures (PSPs).

5) Entities with service providers that do not respond to reports of abuse against State IT resources that emanate from their customers.

B. Service may be suspended without review by automated systems based on rules acceptable to the agency head or their designee.

C. With the exception of emergencies, all incidents must be documented; and documentation provided to the agency head prior to action being taken. In emergencies, first responders may block entities in advance of the agency head or their designee's permission. Requisite documentation for formal permission shall be gathered and forwarded for approval as soon as practical.

D. Law Enforcement entities can request that malicious activity be permitted for evidence gathering purposes, provided it can be controlled and does not create an emergency condition.

7.0 DEFINITIONS/BACKGROUND

Emergency: An event, which, if action is not taken, will result in termination, suspension, or severe degradation of services to a majority of users of a service OR a likely loss of data or system confidentiality, integrity or availability.

First Responder: Entity employees with the responsibility of IT system management capable of denying access to resources.

IT: Information Technology

Malicious: Conduct that violates NRS 205.473 through NRS 205.513 or results in a loss of confidentiality, integrity or availability of systems or data.

Network: Determined by the applicable Internet Registry (e.g., InterNIC, DODNIC, RIPE, APNIC, LACNIC, AFRINIC, ARIN) to the smallest number of nodes (smallest network) that can be identified as a responsible party for the malicious activity.

8.0 EXCEPTIONS/OTHER ISSUES

Requests for exception to the requirements of this Information Security Standard must be documented, provided to the Office of Information Security (OIS), and approved by the State Chief Information Security Officer (CISO).

State of Nevada

Information Security Committee

Standard

Approved By		
Title	**Signature**	**Date**
State Information Security Committee	Approved by Committee	4/27/2017
State Chief Information Security Officer (CISO)	Signature on File	5/25/2017
State Chief Information Officer (CIO)	Signature on File	5/31/2017

Document History		
Revision	**Date**	**Change**
A	04/27/17	Initial Release – Formerly EITS Standard 120