State of Nevada

Information Security Committee

Standard

Control No.	Rev.	Title	Effective Date	Page
135	B	Hacking	08/20/2014	1 of 2

1.0 PURPOSE

This standard establishes the minimum for protection against Information Technology (IT) Hacking.

All systems and networks must be adequately protected from malicious activity. In order to ensure this protection employees and contractors must understand that hacking will not be tolerated.

2.0 SCOPE

This standard applies to all state agencies meeting the requirements identified in the State Information Security Consolidated Policy, Section 1.1, Scope and Applicability.

3.0 EFFECTIVE DATES

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

4.0 RESPONSIBILITIES

The agency head and appointed agency Information Security Officer (ISO) have the responsibility to ensure the implementation of and compliance with this standard.

5.0 RELATED DOCUMENTS

State Information Security Consolidated Policy, 100
State Information Security Officer (ISO) Roles and Responsibilities, 102

6.0 STANDARDS

A. Suspected violations shall be formally reported to the appropriate authorities for their evaluation and action.

B. System administrators shall implement security practices to protect their systems from attack.

C. All violators and/or responsible parties will lose access rights to state computers connected to any other computer or network device. In addition, violators and/or responsible parties are subject to disciplinary actions.

D. Violators and/or responsible parties who are contractors or consultants may have contracts terminated and may be subject to legal action.

E. Violators and/or responsible parties suspected of breaking Federal or State laws shall be reported to the proper authorities.

F. All phone calls to and from any dial-up devices must be logged, reviewed as required for suspicious activity and archived for at least three (3) months. All E-mail systems must be scanned for viruses; current virus protection will be maintained on either the E-mail server or at the E-mail gateway (firewall, proxy server).

G. Documented activity of suspicious occurrences shall be retained for at least one (1) year.

7.0 DEFINITIONS

Hacking: The intentional unauthorized access, removal, duplication, and/or modification, interference or denial of access to of one or more State of Nevada systems (including, but not limited to, computer hardware, computer software, operating systems, networks, phone systems and data) which results in damage, lost use, degraded use, injury, violation of any applicable laws and/or invasion of privacy. See NRS 205.4765, 205.47, 205.481, 205.492, 205.498.

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).

Approved By		
Title	**Signature**	**Date**
State Information Security Committee	Approved by Committee	1/30/2014
State Chief Information Security Officer (CISO)	Signature on File	8/20/2014
State Chief Information Officer (CIO)	Signature on File	8/20/2014

Document History		
Revision	**Date**	**Change**
A	10/31/01	Initial release.
B	08/20/14	Office of Information Security biennial review, replaces standard 4.64