



# State of Nevada

## Information Technology Security Committee

### Standard

Control No.	Rev.	Title	Effective Date	Page
4.64	A	Hacking	05/09/02	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 IT Security Policy, Section 2.0 Scope.

#### 3.0 EFFECTIVE DATES

The requirements of this standard are effective 90 days after sign-off by the Governor or his designee.

#### 4.0 RESPONSIBILITIES

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

#### 5.0 RELATED DOCUMENTS

State IT Security Policy 4.02  
State Information Security Officer (ISO) Roles and Responsibility, 4.03

#### 6.0 STANDARD

- 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.



# State of Nevada

## Information Technology Security Committee

### Standard

Control No.	Rev.	Title	Effective Date	Page
4.64	A	Hacking	05/09/02	2 of 2

- 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

Request for exception to the requirements of this IT Security Standard must be documented, provided to and approved by the State IT Security Committee and Chief Information Officer (CIO).

<i>Approved By</i>		
Title	Signature	Date
<b>State IT Security Committee Chair</b>	Signature on File	10/31/2001
<b>NV IT Operations Committee Chair</b>	Signature on File	05/09/2002
<b>Governor/Governor's Representative</b>	Signature on File	06/17/2003

<i>Document History</i>		
Revision	Date	Change
(-)		Initial release.