1.0 PURPOSE
This establishes minimum information security requirements for the protection of State systems regarding email, and for accessing personal email using State systems.

2.0 SCOPE
This standard applies to all state agencies meeting the criteria identified in the State Information Security Program Policy, Section 1.2, 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 Information Security Officer (ISO) have the responsibility to ensure the implementation of and compliance with this standard.

5.0 RELATED DOCUMENTS
State Information Security Program Policy, 100

6.0 STANDARD
State-provided email should be used for legitimate state business. However, brief and occasional email messages of a personal nature may be sent and received. All content on State email applications are property of the State of Nevada.

6.1 Use of State-Provided Email Applications
A. Employees have no right to privacy with regard to email usage on state systems. Management has the right to view employees’ usage patterns and take action to assure that agency email resources are devoted to maintaining the highest level of productivity.

B. Creating, forwarding, or propagating any racist, sexist, threatening, or obscene material via State-provided email applications is prohibited.

C. Employees shall not use email to intentionally disable, impair, or overload performance of any computer system or network, or to circumvent any system intended to protect the privacy or security of the systems or another user.

D. All user interactions with State-provided or enterprise email applications must adhere to their agency’s acceptable use agreements.

E. Employees shall not use State-provided email applications to subscribe to mailing lists or services strictly for personal use.

F. User photographs in the enterprise email system must be of the user of the account. All photographs should be professional and appropriate for business use. Avatars and other images are not allowed. Any prohibited content discovered in violation of this
standard will be removed without notice by EITS, and may be reported to the agency head and/or Information Security Officer (ISO) as appropriate.

G. Personal use of State-provided email applications is a privilege. As such, the privilege may be revoked at any time. Any prohibited content discovered in violation of this standard may be reported to the agency head and/or Information Security Officer (ISO) as appropriate.

H. When employees send email of a personal nature on a state system, there is always the possibility of the employees’ words being interpreted as official agency correspondence. When an employee sends a personal email from State-provided email, especially if the content of the email could be interpreted as an official agency statement, the employee should use the following disclaimer at the end of the message: “This email contains the thoughts and opinions of (employee name) and does not represent official (agency name) policy.”

6.2 Use of Personal Email

A. Personal email use on State systems is a privilege. As such, the privilege may be revoked at any time at the discretion of the agency. Abuse of the privilege may result in appropriate disciplinary action.

B. Personal email use shall not impede the conduct of state business; only incidental amounts of employee time shall be used to attend to personal matters.

C. Creating, forwarding, or propagating any racist, sexist, threatening, or obscene material via State systems is prohibited.

D. Personal email shall not be used for any monetary interests or gain while on State systems.

E. All personal email sent on state systems or across state networks can be archived.

7.0 DEFINITIONS

Email: A system for sending and receiving messages electronically.

Enterprise email applications: The standardized application(s) for email connectivity provided by Enterprise IT Services for all using agencies.

Personal email: The application(s) for email connectivity which are not provided by an employer for work-related activities.

State-provided email applications: The application(s) for email connectivity provided by any State of Nevada agency.

8.0 RESOURCES

NSLA Bulletin No. 1 FINAL 2011 Guidelines for Developing an Agency Email Policy
9.0 EXCEPTIONS

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

<table>
<thead>
<tr>
<th>Title</th>
<th>Signature</th>
<th>Approval Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>State Information Security Committee</td>
<td>Approved by Committee</td>
<td>11/19/2020</td>
</tr>
<tr>
<td>State Chief Information Security Officer (CISO)</td>
<td>Signature on File</td>
<td>11/24/2020</td>
</tr>
<tr>
<td>State Chief Information Officer (CIO)</td>
<td>Signature on File</td>
<td>11/30/2020</td>
</tr>
</tbody>
</table>

Document History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Effective Date</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>4/11/2002</td>
<td>Initial release</td>
</tr>
<tr>
<td>B</td>
<td>12/01/2016</td>
<td>Re-write to incorporate State-provided email standards</td>
</tr>
<tr>
<td>C</td>
<td>12/26/2018</td>
<td>Renumbering (116 to S.3.04.02) and compliance to ADA standards</td>
</tr>
<tr>
<td>D</td>
<td>12/31/2020</td>
<td>Biennial review for alignment with CIS Controls v7.1, Implementation Group 1 (IG1)</td>
</tr>
</tbody>
</table>