ADMINISTRATIVE POLICY

Information Security Plan

POLICY STATEMENT

This Information Security Plan describes Nevada State College's safeguards to protect sensitive information and data in compliance with institutional, state, and federal guidelines. Sensitive information is defined as any information that is considered personal or confidential such as individually identifiable health information, education records, and non-public information. These safeguards are provided to:

- Protect the security and confidentiality of sensitive information
- Protect against anticipated threats or hazards to the security or integrity of such information
- Protect against unauthorized access to or use of sensitive information that could result in substantial harm or inconvenience to any student, employee, or customer

REASON FOR POLICY

The purpose of this plan is to:

- Identify the risks that may threaten sensitive information maintained by Nevada State College
- Designate individual(s) responsible for coordinating the plan
- Establish and maintain a safeguards program
- Establish and maintain an incident response plan
- Adjust the plan to reflect changes in technology, sensitive information, or threats related to information security

PROCEDURES

Identification of Risk to Sensitive Information
Nevada State College recognizes that it has both internal and external risks. These risks include, but are not limited to:

- Unauthorized access of sensitive information by someone other than the data owner
- Compromised system security which can result in unauthorized access to sensitive information
- Interception of data during transmission
- Loss of data integrity
- Physical loss of data in a disaster
- Corruption of data or systems
- Unauthorized access of sensitive information by employees
- Unauthorized access through hardcopy files or reports

- Unauthorized transfer of sensitive information through third parties

Information Security Plan Coordinator
The appointed Information Security Officer, in cooperation with the Chief Information Security Officer at the Nevada System of Higher Education, is responsible for the implementation and maintenance of this plan.

Safeguards Program

Employee Management and Training
Upon selection for hire, background checks are conducted when deemed appropriate. During onboarding, each new employee that may handle or encounter sensitive information shall receive information security training highlighting the importance of confidentiality and protecting sensitive data.

Physical Security
Nevada State College has addressed physical security of sensitive information by limiting access to only those employees who have a business reason to know such information and requiring acknowledgement of the requirement to keep sensitive information private.

Information Systems
Information systems housing sensitive information shall be secured behind network firewalls, be physically accessible only to key personnel, be electronically accessible only via controlled access, kept up-to-date with security patches, backed up on a routine basis, and transmit sensitive data in a secured manner such as via encrypted channels. Additionally, Nevada State College will maintain systems to prevent, detect, and respond to attacks or intrusions. This includes maintaining anti-virus protection, a network intrusion detection/alert system, and tools to secure systems in the event of a breach.

Selection of Service Providers
In the process of selecting a service provider that will maintain or regularly access sensitive information, the evaluation process shall include the ability of the service provider to safeguard this data. Contracts with service providers should also include the following provisions:

- A stipulation that the sensitive information will be held in strict confidence and accessed only for the explicit business purpose of the contract
- An assurance from the contract partner that the partner will protect any sensitive information it receives

Incident Response Plan
Nevada State College shall maintain an incident response plan. Per the incident reporting and response procedures, all suspected information security incidents must be reported as quickly as possible to Information & Technology Services. This includes, but is not limited to, security breaches, unintended exposure of sensitive information, suspected viruses or malware, or unauthorized requests for login information or sensitive information.

Evaluation and Adjustment
This information security plan will be subject to periodic review and adjustment due to constantly changing technology and evolving risks. The plan coordinator will review standards set forth in this plan recommend updates and revisions as necessary. It may be necessary to adjust the

plan to reflect changes in technology, the definition of sensitive information, or internal/external threats to information security.

CONTACTS

SUBJECT	CONTACT	PHONE	EMAIL
Primary Contact(s)	Brian Chongtai	702-992-2410	brian.chongtai@nsc.edu

DEFINITIONS

Data owner – An individual, entity, or office that is authorized to collect, view, or manage the data.

Sensitive data – Any data associated with an individual, including but not limited to social security number and data that is protected by Board policy, state, or federal law.

Third parties - Any individual or entity contracted by Nevada State College.

RELATED INFORMATION

HISTORY

Revised 2/26/18