ADMINISTRATIVE POLICY

Information Security Plan

POLICY STATEMENT

This Information Security Plan describes Nevada State University's safeguards to protect sensitive information in compliance with institutional, state, and federal guidelines. 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 sensitive 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.

The purpose of this plan is to:

- Identify the risks that may threaten sensitive information maintained by Nevada State University;
- 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

I. Identification of Risk to Sensitive Information

Nevada State University recognizes that it faces both internal and external risks regarding sensitive information. 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 sensitive information during transmission;
- Loss of data integrity;
- Physical loss of sensitive information in a disaster;
- Corruption of data or systems;
- Unauthorized access of sensitive information by employees;
- Unauthorized access of sensitive information through hardcopy files or reports;
- Unauthorized transfer of sensitive information through a third party.

II. 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 policy.

III. Safeguards Program

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

B. *Physical Security*: Nevada State University 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.

C. *Information Systems*: Information systems housing sensitive information shall be secured behind network firewalls, physically accessible only to key personnel, electronically accessible only via controlled access, kept up-to-date with security patches, backed up on a routine basis, and shall transmit sensitive information in a secured manner such as via encrypted channels.

D. *System Monitoring & Testing*: Nevada State University will maintain systems to monitor, prevent, detect, and respond to attacks or intrusions. This includes anti-virus protection, a network intrusion detection/alert system, and tools to secure systems in the event of a breach. Additionally, routine penetration and vulnerability scanning shall be conducted to ensure that security mechanisms are correctly configured and systems are patched for any vulnerabilities.

E. *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 such data. Contracts with service providers should also include the following provisions:

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

F. *Risk Assessment*: Nevada State University shall perform routine risk assessments based on the National Institute of Standards and Technology (NIST) standards and guidelines to evaluate and remediate vulnerabilities in security controls.

IV. Incident Response Plan

Nevada State University 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.

V. 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 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@nevadastate.edu

DEFINITIONS

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

Sensitive Information: Any information or data associated with an individual that is considered personal or confidential, including but not limited to social security numbers, individually-identifiable health information, education records, non-public information, and data that is protected by Board policy, state, or federal law.

Third Party: Any individual or entity contracted by Nevada State University.

RELATED INFORMATION

HISTORY

Revised 8/5/24