ADMINISTRATIVE POLICY

Data Security Policy

POLICY STATEMENT

It is the responsibility of Nevada State College employees to protect sensitive data from unauthorized change, destruction, or disclosure according to college, campus, or local guidelines as well as any other regulations or laws which may apply. This policy governs all administrative systems that provide access to confidential data and defines the responsibilities of employees who maintain or use those systems.

REASON FOR POLICY

The purpose of this policy is to ensure the security of sensitive data which is viewed, processed, stored, maintained, or transmitted at Nevada State College and to protect the confidentiality of that data. This policy is designed to protect this data from unauthorized change, destruction, or disclosure, whether intentional or accidental.

PROCEDURES

Termination of Access

When an employee no longer works for the college, it is the responsibility of his/her manager or supervisor to request from Information & Technology Services (ITS) that the associated administrative account(s) be disabled or deleted, at the latest, by the date of termination or transfer.

Safeguarding Accounts and Passwords

Access to computers and accounts that contain sensitive data must be protected, at minimum, by a user ID and password. It is the responsibility of the user to safeguard his/her user ID and password. User IDs and passwords are not to be divulged to others for the use of accessing sensitive data. Users accessing administrative systems must do so using only ITS approved software that utilize a secure network protocol and/or data encryption for transmitting sensitive data across a public network. Computers and devices containing or having access to sensitive data should be restricted when the user is away by locking the workstation and/or physically securing the device.

Data Storage

Data owners must be aware of where sensitive data is stored both physically and electronically. It is the responsibility of the data owner to provide adequate security and to provide yearly audits on these areas to ensure their protection. Sensitive data should not be stored on personal desktop or laptop computers since these computers tend to reside in less secure locations that have a greater chance of unauthorized access or theft. If data must be stored on

a personal device, drive/device encryption must be enabled. All servers containing sensitive data must be housed in a secure location and operated on only by authorized personnel.

Eradication of Data
All sensitive data is to be properly disposed of when it has exceeded its required retention period or is no longer needed for the operation of the college. This includes output such as paper reports, CDs, DVDs, magnetic tapes, etc. Sensitive data contained on workstations is to be removed from all storage devices within the unit prior to repurposing or disposal using a minimum of a single pass overwrite process.

Security Breaches
If data is released and/or obtained inappropriately, the incident must be reported immediately to the Information & Technology Services. ITS will then determine how the breach occurred, make every effort to protect the exposed data, and report the incident to the data owner. It is then up to the data owner to disclose the breach of security to any person whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person per NRS 603A.220.

Application Security Lead
Each application system shall have an Application Security Lead designated by the data owner. This individual is responsible for authorizing access privileges to the application, for ensuring that employees who receive user IDs have proper authorization, and for monitoring data access violations. All such authorizations and approvals must be documented.

Security Coordinator
The Security Coordinator is responsible for creating user IDs with the associated access privileges granted by the appropriate Application Security Lead, for maintaining an appropriate level of overall system security, and for monitoring the system for security violations. This individual shall also maintain records for all accounts including appropriate approvals and associated access privileges granted. Such records shall be maintained for two years after account termination.

Individual Responsibilities
Individual employees are responsible for maintaining the security and confidentiality of data in their possession, such as hardcopy reports or data downloaded to their workstations. Individuals must report to the Office of Information & Technology Services any known breach of application or system security. It is the responsibility of all employees to safeguard any and all confidential information and ensure that it is used appropriately. Employees shall not use any confidential information except in work for the college or copy, publish, disclose, or provide access to any confidential information except as necessary to such permitted use. Under no circumstances will employees remove, or permit the removal of, any materials containing confidential information from the college premises except in permitted activities. All Nevada State College employees shall comply with the Family Education Rights and Privacy Act (FERPA) as well as any overarching information security policy from the Nevada System of Higher Education.

CONTACTS

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

DEFINITIONS

Custodian of the data – The entity or office that is delegated by the data owner the responsibility of performing management functions for the data.

Data owner – The entity or office that is authorized to collect and manage the data as official record.

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

Family Educational Rights and Privacy Act (FERPA)
https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

HISTORY

Revised 2/22/18