Policy Title: Data Stewardship, Security and Protection

Impact: Employees, Students, Affiliates

Responsibility: Chief Information Officer

Effective Date: 3/28/2018

Revised Date:

Reviewed Date:

Relates to Procedure(s): 3.08.03

Legal Citation(s):

I. Policy

It is the policy of North Idaho College (NIC) to protect its institutional data and allow the use, access, and disclosure of such information in accordance with NIC interests and applicable laws and regulations. NIC owns all institutional data and throughout its lifecycle, the data shall be classified and protected in a reasonable and appropriate manner based on its level of sensitivity, value, and criticality to NIC. All NIC faculty, staff, students, and affiliates who provide services or work with NIC institutional data are responsible for protecting it from unauthorized access, modification, destruction, or disclosure.

Authorization for access and the maintenance of security of all institutional data, particularly highly sensitive data, is delegated to specific individuals within their defined roles (data steward, data custodian, data user, or system administrator) and in relation to the data being used. Data security measures are commensurate with the value, sensitivity, and risk involved with particular data.

II. Compliance

A. NIC prohibits the disclosure of restricted and sensitive data in any medium except as approved by the appropriate data steward or data custodian. The use of any data for one's own personal gain or profit, for the personal gain or profit of others, or to satisfy personal curiosity is strictly prohibited.

B. NIC prohibits the storage of restricted data on any storage device or media not approved for use by the NIC IT department. If an individual is required to store data on such media, that individual must obtain written approval from both the data steward and CIO.

C. All individuals accessing NIC institutional data are required to comply with federal and state laws and NIC policies and procedures regarding data security. Any NIC employee, student, or affiliate with access to NIC data who engages in unauthorized use, disclosure, alteration, or destruction of data is in violation of this policy and will be subject to appropriate disciplinary action.

III. Data Classification

To implement security at the appropriate level, to establish guidelines for legal/regulatory compliance, and to reduce or eliminate conflicting standards and controls, data is classified by the appropriate data steward or data custodian into one of the following categories:

A. Restricted: Any NIC institutional data that, if disclosed to unauthorized persons, would be a violation of federal or state laws, NIC policy, or NIC contractual obligations. Any file or data that contains personally identifiable information may also qualify as restricted data. The highest level of security is applied to this data classification.

B. Sensitive: Any NIC institutional data that must be guarded due to proprietary, ethical, or privacy considerations and must be protected from unauthorized access, use, modification, transmission, or storage. A reasonable level of security is applied to this data classification.

C. Public: Any NIC institutional data to which the public is granted access, in accordance with NIC policy or standards. A level of control is applied to this data classification to ensure appropriate use.

VI. Data Stewardship Roles

A. Data steward refers to executive level NIC officials responsible for managing a major area of NIC institutional data, and who oversee the lifecycle of one or more sets of institutional data.

B. Data custodian refers to NIC officials and their staff who have operational-level responsibility for the capture, maintenance, and dissemination of data for specific areas.

C. Data user refers to individuals that have been granted access to institutional data in order to conduct NIC business.

D. System administrator refers to individuals with administrative access to an information system at NIC.

VII. Definitions

A. *"Affiliate"* refers to any authorized individual, business, or organization that acts on behalf of NIC, or is authorized to conduct work for NIC.

B. *"Institutional data"* refers to any type of information that is processed, created, collected, transferred, recorded, or stored by NIC to conduct NIC business.

C. *"Information Technology (IT) resources"* refers to any resources related to the access and use of digitized information, including but not limited to hardware, software, devices, appliances, and network bandwidth.

D. *"Security controls"* are safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets.