Procedure 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 Policy(s): 3.08.03

Legal Citation(s):

This procedure defines data stewardship and the security requirements for protecting institutional data based on its data classification at North Idaho College (NIC).

I. Data Stewardship

A. Individuals who create, collect, handle, manage, or use institutional data are responsible for complying with the responsibilities of their identified role. Responsibilities are defined by guidelines that accompany this procedure, and are created and maintained by the Information Technology department (IT) in conjunction with the IT Planning and Policy Council (ITPPC).

B. All data stewards and data custodians must have a thorough understanding of security risks impacting institutional data. Security risks will be documented and reviewed by a data steward or data custodian so that they can determine whether greater resources need to be devoted to mitigating these risks.

C. The IT department will not provide access to institutional data without approval from a data steward or data custodian. The IT department will identify security risks as well as provide and remove user access.

D. The IT department shall provide guidelines for restricted data types based on state/federal regulatory requirements and contractual obligations.

II. Classifying and Reclassifying Data

A. Classifying Data. Data stewards and data custodians assign a single classification to a collection of data that is common in purpose or function. When classifying a collection of data, the most restrictive classification of any of the individual data elements will be used.

If the appropriate classification is not obvious, the data steward or data custodian will default to classifying data based on the Federal Information Processing Standards ("FIPS") publication 199 published by the National Institute of Standards and Technology (NIST).

If an appropriate classification is still unclear after using FIPS, the data steward or data custodian will contact the Chief Information Officer (CIO).

B. Reclassifying Data. Periodically, the classification of institutional data will be reviewed by a data steward or data custodian to ensure the classification is still appropriate based on changes to legal and contractual obligations as well as changes in the use of data or its value to NIC.

III. Security and Controls

The NIC IT department will work with personnel to ensure that the correct security controls are in place for data based on its classification. The NIC IT department and the ITPPC will establish security guidelines in accordance with industry best practices, standards, and federal and state laws.

IV. Enforcement

A. Regarding employees and other affiliates, the consequences of policy violation will be commensurate with the severity and frequency of the offense and may include termination of employment or contract.

B. Regarding students, the consequences of policy violations will be commensurate with the severity and frequency of the offense and may include suspension or expulsion.

C. Violations of this policy will be addressed in accordance with appropriate NIC policies and procedures, as issued and enforced by the appropriate authorities.

D. Violations of any local, state, or federal law will be reported to law enforcement.

E. Consequences of policy violation may include, but are not limited to, the following:

1. Notification: alerting a user to what appears to be an inadvertent violation of this policy in order to educate the user to avoid subsequent violations.
2. Warning: alerting a user to the violation with the understanding that any additional violation will result in a greater penalty.
3. Loss of computer and/or network privileges: limitation or removal of computer and/or network privileges, either permanently or for a specified period of time.
4. Penalties: if applicable, the violator may be subject to criminal or civil penalties.

V. Appeal

For employees, an appeal of unresolved disputes of enforcement actions will be handled via the Grievance Policy and Procedure. For students, all provisions of the Student Code of Conduct shall apply.

VI. Maintenance

This procedure will be reviewed by NIC's Chief Information Officer (CIO), IT Department, and the ITPPC every three years or as deemed appropriate based on changes in technology or regulatory requirements.

VII. Exceptions

Exceptions to this procedure must be approved by the NIC IT Department and formally documented under the guidance of the CIO, and President's Cabinet.