Procedure Title: Security Awareness Training

Impact: Employees, Affiliates

Responsibility: Chief Information Officer

Effective Date: 04/16/2018

Revised Date:

Reviewed Date:

Relates to Policy(s): 3.08.08

Legal Citation(s):

The North Idaho College (NIC) Information Technology (IT) Department is responsible for developing, implementing, and maintaining a security awareness training program. All employees and affiliates are responsible for participating in the program, for being knowledgeable about information security policies, and for complying with the procedures and best practices provided in the training.

I. Responsibilities

All NIC employees and affiliates are required to complete a security awareness training program annually. Some users will require additional training based on their responsibilities at NIC.

II. Security Awareness Training Program

The NIC IT Department will maintain a security awareness training program that instructs employees and affiliates on security awareness and best practices.

Security awareness training will have the following objectives:

- Improve users' awareness of the need to protect information resources.
- Ensure that users clearly understand their responsibilities for protecting information.
- Ensure that users are knowledgeable about information security issues and best practices.
- Maintain skills and knowledge so users can perform their jobs securely.

III. Targeted Audience Training

Certain users at NIC may require advanced or specialized training in order to best support the security goals of NIC. Additional education for IT professionals, managers, administrators, and jobs requiring expertise in security will be provided as needed.

IV. Training Notification

Notification of training will be done by the NIC IT department on a semi-annual basis at a minimum. Any changes to the security training program will be communicated to the entire campus community. NIC IT department will provide all instructions of how to access, use, and complete required training.

V. Enforcement

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.

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

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

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

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

A. 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.
B. Warning: alerting a user to the violation, with the understanding that any additional violation will result in a greater penalty.
C. 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.
D. Penalties: if applicable, the violator may be subject to criminal or civil penalties.

VI. Appeal

For employees, appeal of actions taken which result in an unresolved dispute will be handled via the Grievance Policy and Procedure. For students, all provisions of the Student Code of Conduct shall apply.

VII. Maintenance

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

VIII. 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.