Procedure Title: User Authentication

Impact: Employees, Students, Affiliates

Responsibility: Chief Information Officer

Effective Date: 3/28/2018

Revised Date:

Reviewed Date:

Relates to Policy(s): 3.08.05

Legal Citation(s):

To access North Idaho College (NIC) accounts, associated data, computing and network resources, NIC requires users to authenticate using the combination of a username and secure password that meets or exceeds the minimum requirements defined by NIC.

This procedure applies to all faculty, staff, students, and third-party agents of NIC as well as any other NIC affiliate authorized to access NIC Information Technology (IT) resources using a user credential.

I. Responsibilities of all users

A. NIC accounts, access, and passwords are the responsibility of the individual to whom the account is assigned.

B. Users are responsible for the maintenance and confidentiality of their passwords.

C. If a user suspects that their account or password has been compromised, they must report this issue to the NIC IT helpdesk immediately.

II. User account creation

NIC users who have a legitimate need to acquire access to non-public resources are issued a unique user account for authentication.

A. Account creation will be determined by the NIC IT department. All enrolled students, employees, or other approved affiliates will be issued an account.

B. NIC contractual obligations or software licensing terms may limit the ability to allow access to specific resources.

III. Secure Passwords/Passphrase Requirement

All users should create a strong password or passphrase for their user account. NIC IT department will maintain guidelines and standards for creating passwords and make them available to all users.

IV. Account deletion and disabling of access

Access to an account shall be disabled or removed when a user no longer meets the criteria for access. The NIC IT department will maintain guidelines related to the deletion and disabling of accounts at NIC.

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 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, an 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.