Identity and Access Management Policy

Policy 905

1 Introduction

The security, privacy, and integrity of Institutional Data is an operational priority for Appalachian State University (“Appalachian”). The purpose of this policy is to outline responsibilities and authorities for the effective management of Appalachian’s User Identity and Access Control Program.

2 Scope

This policy applies to all Appalachian State University employees, students, visitors and vendors.

3 Definitions

3.1 User Identity

An electronic identity Data Element that represents a known individual or group affiliated with the University.

3.2 Access

The ability and means to: (a) communicate with or otherwise interact with Institutional Resources; (b) use Information Technology to Access Institutional Data; (c) gain knowledge of Institutional Data contained in Information Technology; or (d) control Information Technology components and functions.

3.3 [Other Terms]

Other capitalized terms have the same meaning as defined inAppalachian Policy 901 – IT Governance Policy and Appalachian Policy 902 - Data Governance Policy

4 Policy and Procedure Statements

4.1 Roles and Responsibilities

The Chancellor has delegated authority and oversight for the administration and implementation of Appalachian's User Identity and Access control functions to the Chief Information Officer. The Chief Information Officer is responsible for developing and overseeing a User Identity and Access Control Program (the “Program”) that includes:

a. the implementation and maintenance of User Identity confirmation and Access control techniques, including the User Identity and Access of students, faculty, and staff, and other individuals with Access to the University’s Information Resources and Institutional Data;
b. the development and implementation of IT Standards to establish the University’s Identity and Access Management practices in accordance with UNC System policies and standards;
c. ensuring that Appalachian’s User Identity and Access Control Program incorporates measures to sufficiently control Access to Institutional Data consistent with federal and state laws, and UNC System policies; and
d. seeking and receiving recommendations from the IT Governance Groups and Data Governance Groups on risk-informed techniques to confirm User Identity and Access control to University Information Resources and Institutional Data.

4.2 Confidentiality of Institutional Data

The standards and practices developed and maintained in accordance with this policy shall be confidential and not considered a public record to the extent permitted by North Carolina law.

5 Additional References

Appalachian Policy 901 - Information Technology Governance Policy
Appalachian Policy 902 - Data Governance Policy
Appalachian Policy 903 - Information Security Policy

Appalachian Policy 906 - Acceptable Use of Computing and Electronic Resources Policy

6 Authority

UNC Policy 1400.3 User Identity and Access Control
IT Policy, Standards and Guidelines Website
Identity and Access Management Standard
Data Management Standard

7 Contact Information

Office of the Chief Information Officer (828-262-6278)

8 Original Effective Date

December 7, 2020

9 Revision Dates