University of North Georgia

2013

User Account Management Policy

Division of Information Technology

Version 1.0

Sensitive

Revision & Sign-off Sheet

Change Record

Date	Author	Version	Change Reference

Reviewers

Name	Version Approved	Position	Date

Distribution

Name	Location
Computer Center	Dunlap Mathis Building, Rm. 132 (Fire-rated Safe)
Alfred Barker	Dunlap Mathis Building, Rm. 129 (CISO’s Office)
Online	https://my.ung.edu/departments/InfoSec/ (Secure Portal)

Document Properties

Item	Details
Document Title	User Account Management Policy
Document Type	Policy - Internal
Author	Alfred Barker and Haley Carter
Document Manager	Alfred Barker
Creation Date	02-20-2013
Last Updated	04-08-2013
Document Classification	Sensitive

1.0 Executive Summary

The University of North Georgia (hereinafter the “University”) requires secure, reliable, available access to University networks and systems to carry out its mission. The Division of Information Technology (hereinafter “IT”) facilitates Identity and Access Management support in concert with other offices, including but not limited to Human Resources, Student Affairs, and the Card Office in order to enable campus users to appropriately access University resources.

The University provides an environment that encourages the free exchange of ideas and sharing of information. Access to this environment and the University’s information systems is critical to the success of the institution. IT facilitates access provisioning, maintenance, and de-provisioning to support the University’s business practices and needs.

2.0 Governance/Compliance/Authority

USG’s *IT Handbook*, Board of Regents’ *Records Retention Schedule*, and the University’s *Appropriate Usage Policy*, *Password Policy* and *Document Development and Approval Standard* govern this policy. The President and the Cabinet of the University fully support this policy. IT is responsible for managing and administering this policy, which is currently in effect for all University employees, students, affiliates and computer & network systems.

3.0 Continuance

This policy may be reasonably modified at any time by the Chief Information Officer/Chief Information Security Officer with the approval of the President and/or the Cabinet of the University. This document replaces the *Network Account Policy v2.5* (NGCSU-Revised 2011) and the *Administrative Procedures for User Accounts in Academic Computing v2.1* (GSC-Revised 2006).

4.0 Scope

This policy outlines the standards for creation, maintenance, and deletion of user accounts that enable use of University IT resources, which include, but are not limited to, equipment, software, networks, data, and telephones whether owned, leased, or otherwise provided by the University. In addition, this policy is binding and applies to all University employees, students, or affiliates located on but not limited to the facilities at Cumming, Dahlonega, Gainesville, and Oconee (hereinafter “Users”).

5.0 Policy

Users are expected to access only those IT resources for which they have authorization, protect the access and integrity of IT resources, and abide by applicable local, state, federal laws and University policies. If a user believes he or she may have access to resources that are not required for fulfillment of his or her job duties or role, the user shall inform a supervisor, HR or IT representative. The Chief Information Officer is a trusted authority for resolving access questions or concerns, and may be contacted at any time with questions regarding appropriate access and identity management.

5.1 Account Creation

Account creation is governed in accordance with USG’s *IT Handbook*, Section 3.1 *Information System User Account Management.*