UNG
UNIVERSITY of NORTH GEORGIA™

University of North Georgia

2013

User Account Password Policy (DRAFT)

Division of Information Technology

Version 1.0

Unrestricted

Revision & Sign-off Sheet

Change Record

Date	Author	Version	Change Reference

Reviewers

Name	Version Approved	Position	Date
Jenna Colvin	1.0	Legal Representative	
IT Leadership	1.0	Governance Review	
Jill Holman	1.0	Internal Audit	

Distribution

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

Document Properties

Item	Details
Document Title	User Account Password Policy (DRAFT)
Document Type	Policy – External
Author	Alfred Barker and Brandon Haag
Document Manager	Alfred Barker
Creation Date	02/19/2013
Last Updated	04/09/2013
Document Classification	Unrestricted

1.0 Executive Summary

The account credential consists of two parts: the username, which is a unique identifier of easy to remember characters and the password, which is a secret combination of key strokes that when combined with the username authenticates the user to the computer or the network. This form of authentication is referred to as "what you know." For this to work, the user's credentials MUST remain secret!

User accounts are the entry point to the Division of Information Technology's resources (hereinafter "IT resources"). Protecting access to these resources is pivotal in ensuring that the systems remain secure. IT must be diligent in guarding access to IT's resources and protecting them from threats from both inside and outside the University of North Georgia (the "University"). This policy acts as an extension of IT's *System Security Plan*.

2.0 Governance/Compliance/Authority

The President and the Cabinet of the University fully support this policy. This policy is to be used in conjunction with, and is an extension of, the *Information Security Program Policy* and the *Information Security's Appropriate Usage Policy*. IT is responsible for managing and administering this policy, which has been written to support USG's *IT Handbook, Section 5.8 Password Security* standard.

3.0 Continuance

This policy may be reasonably modified at any time by the Chief Information Officer / Chief Information Security Officer ("CIO/CISO") of IT or the President and/or the Cabinet of the University. This document replaces the *Password Policy, Rev 2.1* (NGCSU-Revised 2010) and the *User Password Credentials Policy* (GSC-Revised 2012).

4.0 Scope

This policy outlines the standards for account handling, composition and support of the University's IT resources. 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

IT's objective is to enable the users to perform their tasks with technology, while appropriately addressing the University's mission to support educational discourse and keeping information secure within and exchanged between IT resources.

5.1 Account Handling

In accordance with *Section 5.8.3 Password Security and Composition Standard*, credentials should adhere to the following best practices:

- Passwords should not be the user's name, address, date of birth, nickname, and /or any term that could be easily guessed by someone familiar with the user.
- Use *Pass Phrases* to assist in remembering long and complex passwords.
- In the event a user's account MUST remain active after an employee departs, the password of that account MUST be changed.

- All passwords shall be treated as sensitive, confidential information and shall not be shared with anyone including, but not limited to, administrative assistants, system administrators and helpdesk personnel.
- Users shall not write passwords down or store them anywhere in their office or publically in clear text. They shall not store passwords in a file on any computer system, including smart devices, without encryption.
- Passwords shall not be inserted into email messages or other forms of electronic communication unless encrypted.
- Temporary or "first use" passwords (e.g., new accounts or guests) must be changed the first time the authorized user accesses the system, and have a limited life of inactivity before being disabled.

5.2 Account Composition

IT assigned ***Faculty, Staff, and Affiliate*** accounts have systematically enforced requirements as stated:

- Usernames are composed of the first letter of the first name (include middle initial if two usernames are the same) and the last name. If a collision exists, append a second letter of the first name and so on until the collision is broken.
- E-mail accounts are composed of the first name followed by a dot and last name (i.e. first.last@ung.edu). If a collision exists, append the first letter of the middle name and so on to the first name until the collision is broken.
- Passwords should follow USG's *IT Handbook Section 5.8 Password Security* standard.
- All user-level passwords shall be changed every one hundred and eighty (180) days.

IT assigned ***Student*** accounts have systematically enforced requirements as stated:

- The 900 ID number is generated in Banner. To obtain a 900 ID number and Student ID, open the Student ID Number Retrieval System on the web.
    - Enter your SS# and date of birth. The Student ID and 900 ID number will be displayed.
- All students will sign into the Banner system using their Student ID's (ex. JPSMIT1234 = John Paul Smith, 900991234). Student ID's are composed of the first letter of the first name, the first letter of the middle name and the first four letters of the last name followed by the last four numbers of the 900 ID. If a collision exists, append a second letter of the first name and so on until the collision is broken.
- *Initial Password* – Banner generated password format: Last four digits of Social Security Number plus two-digit day of your birthday. Enter a 0 as the first digit of your day of birth if you were born on a day between the first and the ninth. Enter four zeroes if you did not provide your SSN to the university.
- Passwords should follow USG's *IT Handbook Section 5.8 Password Security* standard.
- All user-level passwords shall be changed every one hundred and eighty (180) days.

IT assigned ***Administrative Accounts*** are subject to stringent composition using complexity best practices and pass-phrasing, frequent change, and limited access. This includes passwords for

routers, switches, WAN links, firewalls, servers, Internet connections, BIOS settings, administrative-level network operating system accounts, and any other IT resource.

- All system-level administrative passwords shall be changed every ninety (90) days.
- User accounts that have system-level privileges granted through group memberships or programs shall have a unique password from other accounts held by that user.
- Access to all University information systems and applications used to process, store, or transfer data with a security categorization of MODERATE or higher shall require the use of strong passwords or other strong authentication mechanisms.

5.3 Account Support

University users are to contact the IT staff for support of the password policy. Students are encouraged to seek assistance via the Help Desk personnel, which can assist students with resetting, changing and entering challenge questions into the password management system. IT welcomes any questions and suggestions and strives to keep the campus resources secure.

5.3.1 Changing Passwords

A network accessible tool has been provided to allow users to change his or her user password. Users shall immediately change their password and notify the IT Help Desk if they suspect any unauthorized access or compromise of any password used to access IT resources.

5.3.2 Forgotten Passwords

Faculty, Staff and Affiliates – contact the IT Helpdesk for assistance.

Students – contact the IT Helpdesk for assistance.

5.4 Exceptions

Policy exceptions must be approved by the Chief Information Officer, which in turn must seek approval from USG's CISO in accordance with USG's *IT Handbook Section 5.8.2.6 Exceptions, Password Security* standard.

6.0 Enforcement

Users shall not attempt to access, recover, crack, or guess the passwords of others. Failure to comply with this policy may result in revocation of privileges and/or actions as specified in the University's HR *Progressive Disciplinary Policy* and/or Student Handbook. Faculty violations will be directed to Academic Affairs; staff or affiliate violations will be directed to Human Resources; and student violations will be directed to the Dean of Students. Any information related to illegal or suspicious activity will be direct to Public Safety and IT Information Security.

7.0 Responsibilities

Information Technology documentation and its upkeep are the responsibility of IT and are stored within IT's fire-rated safe(s), online within the University's secure portal, and in working form with the CISO. Any changes to this document are to be reported to the Document Manager for inclusion or exclusion. It is recommended that the content of this policy be audited at a minimum annually by the CISO.