Password Expiration Regulation

RUL08.05.03 Current Version

Authority: Vice Chancellor for Administration and Finance

History: Regulation Number 7.400 Supersedes Policy Dated: June 23, 2003 Effective Date: September 25, 2003 Review Date: September 9, 2011 Placed in University Policy Manual after EXPEDITED REVIEW, transitioned without substantive change from prior version, March 25, 2013.

Related Policies: N/A

Additional Resources: N/A

Contact Information: Margaret Umphrey, Director, IT Security, (252) 328 - 9187

1. Introduction

1.1 Purpose of Regulation

This regulation defines the procedures for the expiration of passwords for ITCS enterprise systems. This regulation affects the use of ITCS maintained systems and enterprise servers. This regulation has been designed to meet N.C. State audit requirements, governing access to sensitive data

1.2 Person(s) with Primary Responsibility

The Chief Technology Officer is the primary person charged with administering the ITCS Password Expiration Regulation. The systems administrators for the ITCS enterprise systems will be responsible for the notification and expiration of passwords.

2. Regulation

Passwords on ITCS enterprise systems will expire on a regular basis, currently no longer than ninety (90) days, with notification to users via e-mail or system messaging at least 3 times in the two weeks prior to expiration. The only exceptions to this regulation are those systems that do not have the capability to force password changes