Standard Title: UA NetID Password Standard
Standard Number: IS-S703U
Responsible Office: Information Security Office

UA NetID credentials (username and password) are used to access a multitude of *university* services, *resources* and *data* -- everything from email to benefits enrollment and higher-risk applications requiring increased levels of assurance. In an effort to protect campus assets and *personal information*, to meet or exceed auditing requirements, and to conform with standards set by identity federations, *UITS* established a NetID password standard that:

- Responds to a defined threat model
- Provides a means of gauging password strength deterministically, using quantifiable *data*
- Defines password lifetime as a function of password strength

An emerging trend in password security, and one to which *UITS* management subscribes, is that complexity does not necessarily equal strength and that introducing human behavior, or unpredictability, into password creation yields better protection against security threats. *UITS* has greatly mitigated the risk of *compromise* by utilizing the NIST algorithm to quantitatively define the probability of a successful attack, and then designing password creation protocols that exceed these established levels of *authentication.*

UA NetID password strength guidelines were formulated using NIST's recommendations for Password Entropy Calculation (from NIST SP800-63). This calculation considers the character length of the password, the number of character classes (described below), and dictionary/complexity checks to quantitatively determine password strength.

The current NetID password requirements:

1. Minimum password strength: at least ten characters and three character classes are required.
    - Character Classes
    - - Lowercase characters (a-z)
    - - Uppercase characters (A-Z)
    - - Numeric digits (0-9)
    - - Symbols (all other printable characters, not including blank space) !@#$%^&*()_+{}|:"<>?,./'[]\=-`~
2. All passwords are subjected to a strength check.
3. Password reuse: reuse of the previous seven passwords is prohibited and a minimum password age of 24 hours prevents *users* from cycling through old passwords
4. NetID lockout: a 15-minute lockout occurs after seven consecutive invalid *authentication* attempts

A password's lifespan is contingent on its strength. Users are able to determine the strength of any proposed password (and thus its expiration) in real-time using a "strength-o-meter" on the NetID self-service website (netid.arizona.edu). The table below shows the length and complexity requirements as they relate to password expiration periods.

PASSWORD LENGTH	3 CHARACTER CLASSES	4 CHARACTER CLASSES
10 characters	90 days	360 days
11 characters	180 days	360 days
12 or more characters	360 days	360 days

Advanced warnings of password expiration are issued to *users* via the WebAuth login page and email messages. Should a *user* be locked out of his/her account, he/she can attempt another logon in 15 minutes. The user may also use the "unlock my account" utility on the NetID website.

Related Guidance
Information Security Policy (IS-100)
Information Security Terms Guideline (IS-G100)
Data Classification Standard (IS-S302)
Minimum Security for Networked Devices Standard (IS-S602)
Password Construction and Maintenance Guideline (IS-G703)
ISO Compliance Checklist

Reference
NIST's recommendations for Password Entropy Calculation (from NIST SP800-63)

All *italicized* terms used in this standard are defined in the Information Security Terms Guideline (IS-G100).

Revision History

Initial Draft	08/03/10
UA-ISAC Review of Initial Draft	08/16/10
Sent to UA-ISAC for review after revision	08/23/10
Effective Date	08/23/10

For any questions or additional information, please contact the Information Security Office at infosec@email.arizona.edu or (520) 621-8476 (UISO).