Password Complexity Policy

Purpose

To protect confidential information vital to University business. Password complexity will help prevent individual user accounts and the information contained therein from being compromised by others

Policy Statement

User accounts in the BSU domain and other systems that house confidential data will require complex passwords before the information in those accounts can be accessed.

Applies to

All user accounts in the BSU domain and other systems that contain confidential data (exceptions are not possible).

Responsibilities

All passwords must be at least eight characters in length.

Passwords must not have been used in four previous passwords.

Passwords must not contain the individual's name or account name.

Passwords must contain at least three of the following four character groups:

- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Numerals (0 through 9)
- Non-alphabetic characters (such as !, $, #, %)

Complete training on creating complex passwords is available in Element K and in video format. The Element K course that covers password security is *Security Awareness (Part 1): Accessing a Computer, a Network and the Internet in a Secure Manner*.

Title:	Password Complexity Policy
Approved By:	Pat Cronin, Chief Information Officer
Approval Date:	January 29, 2008
Date of Last Revision:	February 23, 2011
Policy Category:	Information Technology Division