Siena College Password Management Policy

I. Purpose:

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of changing these passwords.

II. Scope:

The scope of this policy includes all personnel (students, faculty, staff, administrators, guests, volunteers, vendors, contractors, temporary workers, alumni, etc.) who have been granted or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Siena College facility or has access to the Siena College network.

This policy applies, but not limited to, the following areas:

- E-Mail/Network/Active Directory
- Banner/Oracle
- Banner's Pin
- Central ITS Administered Services

III. Policy Statement:

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Siena College's entire college network. As such, all Siena College faculty, staff, administrators and students (including contractors, guests, volunteers and vendors with access to Siena College systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. It is important to set a strong password and change them regularly. As a general rule of thumb, changing your password every 90 days is recommended.

A strong password consists of:

- A minimum of ten characters
- A mix of upper and lower case letters
- At least one numeric, and
- At least one special character
- See Password Policy Chart below for further details

A password helpful hint: A suggestion is to create a strong password phrase and then develop your password for it. This might be easier than trying to remember a random combination of characters. Remember, however, to use special characters as well.

Password Best Practices:

- Do not reveal a password over the phone to anyone.

**Note: 7/23/12 Moran Group recommendation; increased from5 times.*

- Do not reveal a password in an email message without encryption.
- Do not reveal a password to your boss or administrative assistant.
- Do not talk about a password in front of others.
- Do not hint at the format of a password.
- Do not use passwords that could be easily identifiable or easy for someone to guess such as your name or school name.
- Do not use dictionary words in any language.
- Do not reuse old passwords.
- Do not reveal a password on questionnaires or security forms.
- Do not share a password to co-workers while on vacation.
- Do not write down a password and store it in an easily accessible location, i.e. under your keyboard.
- Do report to the ITS Help Desk immediately if you suspect that your user account or password has been compromised.

Password Policy Chart:

	Network/E-Mail (Active Directory)	**Banner System INB**	**Banner Self Service PIN**
Password Expiration (days)	365	90	120
Minimum length (characters)	10	10	10
Account Locking / Failed Logins	12 times*	5 times	5 times
Password Grace Period (days)	None	14	None
Account Inactivity Locking	After one year	After six months	None
Minimum password complexity	Password must contain from three of the following four categories: -Upper Alpha (A-Z) -Lower Alpha (a-z) -Numeric (123) -Special character (ex: !, ^, *, %, +, ?, -) Note that not all symbols are allowed	Password is case sensitive and should be a combination of letters, numbers, and one special character. It must be different from the previously used password for at least three characters.	PIN must contain at least one alpha and one numeric character; in addition, the user will need to setup two security questions.
Password History	12 passwords	None – password cannot be reused for one year	None – password cannot be reused for one year

Policy Related to Central IT Systems Administered by ITS (Servers)

**Note: 7/23/12 Moran Group recommendation; increased from5 times.*

ITS' policy is to create the strongest passwords possible to protect the College's central IT infrastructure, i.e. servers, network storage, etc. Thus, the following policies are in place:

- All system level passwords (e.g. root, enable, Windows Administrator, application administration accounts, etc.) are changed every 90 days.
- Default passwords are not used.
- Where SNMP is used, the community string must be defined as something other than the standard defaults of "public", "private", and "system" and must be different from the passwords used to log in interactively.
- Passwords are at least ten characters in length.
- Passwords have the following characteristics:
    - Contain at least three of the five following character classes:
        - Lower case characters
        - Upper case characters
        - Numbers
        - Punctuation
        - Special characters (e.g. @#$%^&, etc.)

Right to Modify Policy

The college reserves the right to modify or change this policy in its absolute discretion.

IV. Governance:

This policy will be updated by the Department of ITS. It will be approved by the CIO and President's Cabinet.

V. Exceptions:

Exceptions can be granted in limited circumstances by the CIO based upon the needs of the College and upon the requestor's written justification, which has been reviewed and approved by the College's Risk Officer.

VI. Revision History:

Date	Revision #	Modification	Approved Date
6/27/12		Original Draft for Cabinet Review	
7/23/12		Modified Draft based upon Moran Group Recommendation	
12/11/13	2	Modified Network from none to annually and Banner Self Service Expiration from 90 days to 120 days, Account Inactivity locking after 365 days of inactivity	1/22/14
4/9/14		GIT Approved	4/9/14
		Cabinet Reviewed	4/28/15
8/6/15	3	Update language about which special characters can be used	9/7/15

**Note: 7/23/12 Moran Group recommendation; increased from5 times.*