Password Standard
St. Bonaventure University

1.0 Purpose

This policy describes the University's requirements for acceptable password selection and maintenance to maximize security of the password and minimize its misuse or theft.

Passwords are the most frequently utilized form of authentication for accessing a computing resource. Due to the use of weak passwords, the proliferation of automated password-cracking programs, and the activity of malicious hackers and spammers, they are very often also the weakest link in securing data. Password use must therefore adhere to the policy statement found below.

2.0 Scope

This policy applies to anyone accessing or utilizing St. Bonaventure University's network or data. This use may include, but is not limited to, the following: personal computers, laptops, St. Bonaventure-issued cell phones, and hand-held factor computing devices (e.g., PDAs, USB memory keys, electronic organizers), as well as St. Bonaventure electronic services, systems and servers. This policy covers departmental resources as well as resources managed centrally.

3.1 Policy

All passwords (e.g., email, web, desktop computer, etc.) should be strong passwords and follow the standards listed below. In general, a password's strength will increase with length, complexity and frequency of changes.

Greater risks require a heightened level of protection. Stronger passwords augmented with alternate security measures such as multi-factor authentication, should be used in such situations. High risk systems include but are not limited to: systems that provide access to critical or sensitive information, controlled access to shared data, a system or application with weaker security, and administrator accounts that maintain the access of other accounts or provide access to a security infrastructure.

Central and departmental account managers, data trustees, and security and/or system administrators are expected to set a good example through a consistent practice of sound security procedures.

All passwords must meet the following minimum standards, except where technically infeasible:
•be at least ten characters in length

•contain at least one lowercase character
•contain at least one number
•contain at least one special character
•contain at least one uppercase character
•cannot contain your first name, last name, or username
•cannot match your last three passwords.

To help prevent identity theft, personal or fiscally useful information such as Social Security or credit card numbers must never be used as a user ID or a password.

All passwords are to be treated as sensitive information and should therefore never be written down or stored on-line unless adequately secured.

Passwords should not be inserted into email messages or other forms of electronic communication.

It is recommended that passwords be changed at least every six months.

Individual passwords should not be shared with anyone, including administrative assistants or IT administrators.

If a password is suspected to have been compromised, it should be changed immediately and the incident reported to St. Bonaventure Technical Services.

3.2 Shared Accounts

In addition to the general password standards listed above, the following apply to server administrator passwords, except where technically and/or administratively infeasible:

Passwords for servers must be changed as personnel changes occur.
If an account or password is suspected to have been compromised, the incident must be reported to St. Bonaventure Technical Services and potentially affected passwords must be changed immediately.