Information Security Policy
St. Bonaventure University

St. Bonaventure University ("University") has adopted the following Information Security Policy ("Policy") as a measure to protect the confidentiality, integrity and availability of University Data as well as any Information Systems that store, process or transmit University Data.

Scope

This Policy applies to all faculty, staff and third-party Agents of the University as well as any other University affiliate who is authorized to access University Data.

Maintenance

This Policy will be reviewed by the University's Information Security Council every 3 years or as deemed appropriate based on changes in technology or regulatory requirements.

Enforcement

Violations of this Policy may result in suspension or loss of the violator's use privileges, with respect to University Data and University-owned Information Systems. Additional administrative sanctions may apply according to the appropriate Handbook. Civil, criminal and equitable remedies may apply.

Exceptions

Exceptions to this Policy must be approved and formally documented by the Chief Information Officer, under the guidance of the Information Security Council (ISC). Policy exceptions will be reviewed on a periodic basis for appropriateness.

Definitions

Agent, for the purpose of this Policy, is defined as any third-party that has been contracted by the University to provide a set of services and who stores, processes or transmits Institutional Data as part of those services.

Information Security Council (ISC) is a council appointed by the University President. Members include representatives from Information Technology, Registrar's Office, Student Affairs, Business & Finance, University Advancement and others.

Information System is defined as any electronic system that stores, processes, or transmits data.

University Data is defined as any data that is owned or licensed by the University including, but not limited to, Personally Identifiable Information (PII) stored on University information systems.

Standards & Procedures

The Information Security Policy is comprised of the following standards and procedures, which are summarized below and included as hyperlinks.

1.0 Data Classification Standard

Different types of University Data often require different levels of security. As such, University Data, including Personally Identifiable Information (PII), are assigned sensitivity levels as defined in the Data Classification Standard. Many other Information Security Standards & Procedures refer to the Data Classification Standard.

2.0 Data Breach Response Procedure

A data breach occurs when the confidentiality and/or integrity of University Data, including Personally Identifiable Information, is likely to have been compromised by an outside party. The Data Breach Response Procedure will be used to guide the University's actions, including reporting, in response to a data breach.

In the event of a data breach, a Data Breach Response Form will be completed and filed to document the incident.

3.0 Data Transmission & Storage Standard

University Data is often required to be stored and/or transmitted, sometimes including to external parties and/or by an agent of the University. The Data Transmission & Storage Standard dictates the manner in which University Data is transmitted and stored.

4.0 Endpoint Security Standard

Endpoint devices, including computers and smartphones, constitute a security risk to the extent they are used to store and/or transmit University Data. All employee endpoint devices, including personally owned devices, which store and/or transmit University Data, are subject to the provisions of the Endpoint Device Standard.

5.0 Document Retention Standard

This policy recognizes that University Data often exists in hardcopy. As such, the retention and destruction of hardcopy University Data is subject to the Document Retention Standard.

6.0 Password Standard

Access to University Information Systems is protected by password security. The Password Standard will be used in the creation and maintenance of passwords used to access University Information Systems.

Data Breach Response Procedure
St. Bonaventure University

I. Introduction

St. Bonaventure is committed to compliance with all applicable federal and state laws and regulations relating to the compromise of Sensitive Data. This document establishes measures that must be taken to report and respond to a possible breach or compromise of Sensitive Data, including the determination of the systems affected, whether any sensitive data have in fact been compromised, what specific data were compromised and what actions are required for internal investigation and legal compliance.

II. Overview

A. Reporting

Any suspected or confirmed breach or compromise of sensitive data must be reported immediately to the Chief Information Officer for Information Technology at St. Bonaventure in order to mitigate the risk to information resources and protect the University's operations. In the event that the CIO is unavailable the Director for User Services must be contacted.

B. University Response

Upon receipt of such report, the CIO for Information Technology will review the information with the appropriate parties (this may include, but is not limited to, the Registrar, the Director of HR, the Director of the Wellness Center and the Director of Advancement Operations to determine first if a data breach has taken place and, if so, to determine the composition of the URT (University Response Team). In all cases the URT will be comprised of the affected offices, appropriate communications offices and legal counsel. The CIO for Information Technology will be responsible for service as the lead on any URT.

Other offices likely to be involved, and their responsibilities, are outlined as follows:

Director of the Wellness Center – student and/or employee personal health information
Director of Safety and security – contacts with law enforcement
Human Resources – personnel information and communication with staff
Office of Media Relations – internal and external communications
Registrar – student academic records
Director of Advancement Operations – alumni records
Controller – financial information

C. Procedures

The general steps in a response include the following:

1. University Response Team Composition

The CIO will identify the required offices/personnel to be included in the incident-specific URT.

2. Response and Recovery

The URT may call upon any necessary additional offices and resources required to carry out the investigation, notifications and remediation of any breach. This expanded URT will be responsible for the investigation of the incident and any technical support required. Incident team members will include representatives of affected data owners and any other units responsible for the Information Resources involved. The URT will consult and follow, as applicable to each situation, the protocols described in the Data Security Breach Incident Response Checklist.

3. Lessons Learned

After an incident has been resolved, an incident report will be created and distributed to the Information Security Council. The Council will then convene with the URT to discuss the security controls that failed and establish the steps necessary to prevent or limit the risk of the incident recurring.

D. Contact Information

To report a possible breach of Sensitive Data:

Chief Information Officer for Information Technology:	Dr. Michael Hoffman Email: MHoffman@sbu.edu Telephone: (716) 375 – 2530 (O) (716) 307 – 3667 (C)
Director of User Services:	Mr. Daniel Donner Email: DDonner@sbu.edu Telephone: (716) 375 – 2296 (O) (716) 307 – 0127 (C)

SBU Data Breach Incident Response Form

Date of Incident:

Offices Involved:

Breach Severity:

Status:

Description of Incident:

Action Taken:

Lessons Learned:

Data Transmission & Storage Standard
St. Bonaventure University

Scope: These guidelines apply to all information systems storing or transmitting University data off the University network.

Requirements:

1. Transmission:
    - Critical and highly sensitive data must be transmitted using email encryption or SFTP (secure file transfer protocol).
    - It is recommended that email encryption, SFTP (secure file transfer protocol), or SSL encryption be used when transmitting moderately sensitive data.
    - Employees using the SBU wireless must access the secure wireless network (SBUSEC) to transmit any highly or critically sensitive data.
2. Storage:
    - Critically sensitive data may only be stored and shared by designated servers and/or applications (such as Colleague or Raiser's Edge).
    - Highly sensitive data may only be stored on a file and/or web server with appropriate access controls (such as SBU share drive).
    - Users may store highly or moderately sensitive data on their SBU owned desktop or encrypted laptop.
    - Any files that meet the highly sensitive or critically sensitive level in data classification may only be stored on a secured SBU server/computer or a trusted 3rd party solution certified by the Chief Information Officer.

Implementation Guidance:

1. File transfers
    - Encrypted file transfers can be done by using an encrypted transmission protocol or service such as SFTP (secure file transfer protocol). If an unencrypted mechanism is used to transfer a file containing sensitive data, the file must be encrypted before being transferred. Information Technology provides assistance with SFTP transfers for all faculty, and staff.

2. Web Applications
    - Sensitive data communicated between a web application and the client machine should be encrypted using TLS/SSL or other secure protocols. This can be determined by looking at the URL of the site you are sending data from. If the URL contains "https" then you are ok, however if it is only "http" please be cautious.

3. Email
    - Regular email is not considered a secure method for sharing critically sensitive data.

- No SBU email (internal or external) will include data that meets critically sensitive level in data classification

4. Virtual Private Network
    - The university provides a virtual private network that can provide encrypted access to services that don't offer encryption services natively. VPN is provided upon request to employees with university computers at openvpn.sbu.edu.

Data Classification Standard
St. Bonaventure University

Protected University Data

Any university information such as financial and legal documentation should be protected and should not be shared unless there are legitimate business reasons. Examples of such data include:

1. User account information
2. Financial information
3. Other sensitive university information

Personally Identifiable Information (PII)

Personally Identifiable Information is considered sensitive information that can be used to identify a specific individual. It has been divided into groups: Moderately Sensitive, Highly Sensitive and Critically Sensitive. Our PII covers students, employees, donors, alumni and any other person(s) associated with the university or personal information held under the auspices of the university.

Moderately Sensitive - Information is that which is generally available to those with a legitimate need.

1. Student directory information (See FERPA policy): student name, home and campus address, telephone number, email address, major, dates of attendance, degree(s) earned, enrollment status (full- or part-time), and images and video collected
2. Employee university directory information: position, campus phone, campus address, campus email and images/video
3. Alumni and donor directory information: name, home/business address, email and phone, class year

Highly Sensitive - Any information that can be used to distinguish or trace a person's identity will require written authorization of release.

1. University ID number (unless for legitimate business use)
2. Race, ethnicity, age, sex, gender identity, religion and sexual orientation
3. State or federal action items or documents
4. Medical information and records (including 504s)
5. Employment data and salary verification
6. Employee home address and phone number
7. Student transcripts, grade reports, schedules and financial aid awards
8. Giving Information: donation amounts and purposes
9. Alumni and prospect wealth information

Critically Sensitive - This information in combination with other personally identifiable information (including Moderately Sensitive information) could specifically identify a person.

1. Names and Numbers
    a. SSN
    b. Date of birth
    c. Mother's maiden name
    d. Official state-issued driver's license or identification number
    e. Alien registration number
    f. Government passport number
    g. Employer or taxpayer identification number
    h. Medicaid or food stamp account number
    i. Bank account number
    j. Credit or debit card number
2. Unique biometric data such as a fingerprint, voice print, or retina or iris scan
3. Images of signatures
4. Other number or information that can be used to access a person's financial resources

Document Retention Standard
St. Bonaventure University

Purpose:

The purpose of this standard is to provide for the systematic review, retention and destruction of documents received or created by the University in connection with the transaction of organization business. This standard covers all records and documents, regardless of physical form (including electronic documents), contains guidelines for how long certain documents should be kept and how records should be destroyed. This standard is designed to ensure compliance with federal and state laws and regulations, to eliminate accidental or innocent destruction of records and to facilitate the University's operations by promoting efficiency and freeing up valuable storage space.

When developing departmental guidelines, consideration should be given to preserving institutional history by identifying materials that are suitable for the University Archives and arranging for transfer of appropriate materials at the appropriate time.

With the exception of the guidelines for computer systems and network backup and information retrieval adopted by the Information Technology Department, this standard applies to all records generated in the course of University operations including paper, digital and electronic records.

Document Retention:

Documents should be retained in their original form unless otherwise specified.

Type of Document:

FINANCE & ADMINISTRATION ACCOUNTING RECORDS

ACCOUNTS PAYABLE LEDGER AND SCHEDULES: 7 years

AUDITOR'S REPORT & ANNUAL FINANCIAL STATEMENTS: Permanently

BANK STATEMENTS AND DEPOSIT SLIPS: 7 years

BANK RECONCILIATIONS: 7 years

BANK RECORDS GENERAL: 7 years

CANCELED CHECKS:

- General: 7 years
- Payroll: 7 years
- Taxes (payroll related): 7 years

CASH DISBURSEMENTS JOURNAL: Permanently

CASH RECEIPTS JOURNAL: Permanently

CHART OF ACCOUNTS: Permanently

CORRESPONDENCE (general): 2 years

CORRESPONDENCE (routine) WITH CUSTOMERS AND/OR VENDORS: 2 years

DEEDS, MORTGAGES, BILLS OF SALE: Permanently

ELECTRONIC PAYMENT RECORDS: 7 years

EMPLOYEE EXPENSE RECORDS: 7 years

FACILITIES RECORDS: 3 years after last active

FINANCIAL (unless otherwise specified): 7 years

FIXED ASSET RECORDS (invoices, canceled checks, depreciation schedules): Permanently

GENERAL JOURNAL: Permanently

GENERAL LEDGER: Permanently

HAZARD MATERIALS MAINTENANCE AND DISPOSAL RECORDS: 5 years

INSTITUTIONAL PUBLICATIONS: 5 years

INTERNAL REPORTS (miscellaneous): 3 years

INVOICES: SALES TO CUSTOMERS/ CREDIT MEMOS: 7 years

LEASES: 6 years after expiration

LICENSES: 7 years after expiration

NOTES RECEIVABLE LEDGERS AND SCHEDULES: 8 years

NOTES PAYABLE LEDGERS AND SCHEDULES: Permanently

TRADEMARK REGISTRATION AND COPY RIGHTS: Permanently

PAYROLL JOURNAL: 7 years

PCARD AUDIT: 7 years

PCARD TRANSACTIONS AND SUPPORTING DOCUMENTS: 7 years

PETTY CASH VOUCHERS: 7 years

PURCHASE JOURNAL: Permanently

PURCHASE ORDERS: 7 years

REQUISITIONS: 1 year

TIME SHEETS: 7 years

TRIAL BALANCE - YEAR END: Permanently

VOUCHERS FOR PAYMENTS TO VENDORS, EMPLOYEES, ETC. (includes allowances and reimbursement of employees, officers, etc., for travel and entertainment expenses): 7 years

INSURANCE RECORDS

ACCIDENT REPORTS AND SETTLED CLAIMS: 7 years after settlement

INSURANCE POLICIES (still in effect): Permanently

INSURANCE POLICIES (expired): 3 years

INSURANCE RECORDS, CLAIMS AND POLICIES: Permanently

LEGAL DOCUMENTS

ARTICLES OF INCORPORATION AND BYLAWS: Permanently

CORRESPONDENCE (legal and important matters): Permanently

CHARTERS: Permanently

CONTRACTS AND LEASES (still in effect): Permanently, in fireproof safe and/or backed up digitally

CONTRACTS, MORTGAGES, NOTES AND LEASES (expired): 7 years

COURT DOCUMENTS AND RECORDS

- Employment cases: 7 years
- General litigation: 5 years
- Decision documents - all cases-permanently

EVIDENCE: Records relevant to pending or threatened litigation should be retained until litigation is resolved or threat of litigation is gone

EMPLOYMENT AGREEMENTS: 7 years

INCIDENT REPORTS: Permanently

LEGAL CORRESPONDENCE: Permanently

MINUTES OF BOARD OF TRUSTEES MEETING AND COMMITTEE MEETING: Permanently

TAX RECORDS

IRS OR STATE ADJUSTMENTS: Permanently

PAYROLL TAX RETURNS: 7 years

PROPERTY RECORDS, INCLUDING COSTS, DEPRECIATION RESERVES, YEAR-END TRIAL BALANCES, DEPRECIATION SCHEDULES, BLUEPRINTS AND PLANS: Permanently

SALES AND USE TAX RETURNS: Permanently

TAX RETURNS AND WORK SHEETS, REVENUE AGENTS' REPORTS, AND OTHER DOCUMENTS RELATING TO DETERMINATION OF INCOME TAX LIABILITY, CANCELED CHECKS FOR TAX PAYMENTS: Permanently

W-2, W-4: 7 years

PERSONNEL RECORDS

EMPLOYMENT APPLICATION AND SEARCH COMMITTEE RECORDS (from date of termination): 3 years

EMPLOYMENT ELIGIBILITY VERIFICATION (I-9 form) (from date of termination): 3 years

GARNISHMENTS: 7 years

INDIVIDUAL EMPLOYEE CONTRACTS (from date of termination): 3 years

JOB ANNOUNCEMENTS/ADVERTISING: 1 year

PERSONNEL FILES (from date of termination): 7 years

RECORDS OF JOB INJURIES CAUSING LOSS OF WORK: 5 years

WITHHOLDING TAX STATEMENTS : 7 years

EMPLOYEE BENEFIT PLAN RECORDS

GENERAL LEDGER AND JOURNALS: Permanently

INTERNAL REVENUE SERVICE/ DEPARTMENT OF LABOR CORRESPONDENCE: Permanently

PARTICIPANT COMMUNCIATION RELATED TO DISTRIBUTIONS, TERMINATIONS, BENEFICIARIES: 7 years

PLAN AND TRUST AGREEMENTS: Permanently

RETIREMENT AND PENSION RECORDS: Permanently

ADVANCEMENT

DONOR CORRESPONDENCE: Permanently

DONOR GIFT AGREEMENTS: Permanently

STUDENT ACCOUNTS, ADMISSIONS AND FINANCIAL AID

ADMISSIONS RECORDS FOR ENROLLED STUDENTS: 5 years after date of last attendance

ADMISSIONS RECORDS FOR STUDENTS WHO DO NOT ENROLL: 1 year after application year

FINANCIAL AID RECORDS:

- Promissory notes- permanently
- All other - 5 years after last active date

STUDENT ACADEMIC RECORDS:

- Academic and degree-permanently
- Disciplinary-5 years after last enrollment
- FERPA requests- life of the requested record
- Student employment records, including sign in sheets and class schedule – 7years

DOCUMENT DESTRUCTION STANDARD

Destruction of all physical documents regardless of their nature will be accomplished by secure shredding. The security of the documents should be maintained prior to shredding.

Electronic records will be securely deleted. Although electronic records may be deleted, records containing confidential information can sometimes be recovered even if they have been erased. Software that deletes records from a drive is available and destruction of confidential records using these programs is recommended. Please contact Technology Services for further support.

When a computer or external drive reaches the end of its useful life, Technology Services should assist in proper disposal of the device so that confidential or proprietary information is not unintentionally made available to an unauthorized party.

Personnel who are responsible for destruction of paper or electronic records should maintain a record of destruction. This record should include a description of the records destroyed and the manner of disposition (shredding, deletion of files, etc.).

Department heads will be responsible for ensuring that documents are reviewed and destroyed at the times dictated by the retention period.

Document destruction will be suspended upon notification from the office of the Senior Vice-President of Finance and Administration in the event of an investigation or lawsuit.

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.

Endpoint Security Standard
St. Bonaventure University

When considering endpoint security one has to include any and all devices that potentially connect to SBU related services that could provide personally identifiable information (PII) and protected university data to unwanted users if not protected properly. At no point should any personally owned device be allowed to access SBU servers containing high or critical levels of PII or any protected university data.

The list below attempts to identify any and all devices that qualify as endpoints of concern as of this writing as well as recommendations by the Information Security Council for protection against breach of PII associated with St. Bonaventure students, employees and all constituencies who may rely on the confidentiality of such data.

Definitions

Personally owned devices – technology devices owned by an individual (computer, cell phone, etc.)

SBU Devices – technology devices used by SBU employees but owned by St. Bonaventure University

Data Security Levels – Critical, High and other levels of data sensitivity are defined in the St. Bonaventure Data Classification Standard

Endpoints of concern / recommendations

a. Computers

SBU Office Desktops

- All SBU desktops will enforce a screen saver password after a maximum of 15 minutes of system inactivity.
- All SBU desktops being disposed of or re-purposed will be wiped to ensure that no data can be recovered from the system's hard drive.

Laptops

- The university will continue to identify users who have access to highly or critically sensitive data and encrypt the hard drives of these systems.
- All SBU laptops will enforce a screen saver password after a maximum of 15 minutes of inactivity from the system.
- All SBU laptops being disposed of or re-purposed will be wiped to ensure that no data can be recovered from the system's hard drive.
- It is strongly recommend that any personally owned laptop being used for work purposes has a screen saver password after a period of 15 minutes of inactivity from the system.

- No SBU related data of high or critical sensitivity will be stored on personal owned devices.

b. Mobile Devices
   - All mobile devices connecting to SBU systems (i.e. SBU email) will require a lock code to access the device.
   - All mobile devices connecting to SBU systems will require a lock screen (screen timeout) to initiate upon a maximum of 5 minutes of inactivity on the device.
   - No mobile devices will contain files that meet the highly or critically sensitive level as defined in the Data Classification Standard.
   - SBU employees must report any missing mobile device that connects to SBU systems immediately, but no later than 48 hours after you discover it being lost.
     1. The user must change their password immediately upon noticing that their mobile device is missing.
     2. SBU mobile devices will be erased remotely in the event that a user reports their phone missing.
   - No passwords for apps linked to SBU databases will be stored on mobile devices.

c. Portable drives (i.e. flash drives, external hard drives, CD/DVD's)
   - Any files containing data classified as highly sensitive must be password protected prior to storing them on portable drives.
   - Any files that meet the critically sensitive level in data classification should not be stored on portable drives.

d. SBU Photocopiers
   - Any SBU photocopier containing an internal hard drive will have data wiped from the system prior to disposal and show a certificate verifying data removal from vendor

Securing Data in Public Areas:

- University computers and office spaces should both be locked by employees any time they leave their office for an anticipated time longer than 5 minutes. If an employee shares a workspace with other personnel the computer must be locked anytime you leave your immediate workspace area.
- Any employee using public computer systems (i.e. labs or classrooms) must log off the system immediately upon finishing use of the computer