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.