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)