Holy Cross

Policies and Procedures Manual

Title:	Incident Reporting and Handling
Policy Administrator:	General Counsel
Effective Date:	Jan-31-2012
Approved by:	Information Security Task Force

Purpose:

The purpose of this policy is to provide a process to report suspected data breaches or exposures (including unauthorized access, use, or disclosure) to appropriate individuals; and to outline the response to a confirmed theft, data breach, or exposure based on the type of data involved.

Procedures:

Any individual who suspects a theft, breach, or exposure of Holy Cross Protected data or Holy Cross Sensitive data has occurred must immediately contact one of the following individuals or offices:

Holy Cross Public Safety Office, safety@holycross.edu, 508-793-2224
Information Technology Services director, ekeohane@holycross.edu, 508-793-2477
Human Resources office (staff), hr@holycross.edu, 508-793-3391
Office of the Dean (faculty), dean@holycross.edu, 508-793-2541

Holy Cross' Department of Public Safety is responsible for coordinating all investigations. They will form a Data Security Team to support the investigation. This team will include, at a minimum, someone from Public Safety and the ITS Information Security Officer (presently David Shettler). Public Safety will determine whether or not a local, state or federal law enforcement agency should be contacted, based on the location and details of the incident. If a local law enforcement agency is contacted, the name of the agency and the agency incident report number will be provided to Holy Cross' Department of Public Affairs.

1.0 Initial Investigation and Categorization

Subsequent to the initial report and Security Team formation, the Security Officer and the Security Team members will conduct an initial investigation to determine the nature of the data breach, the types of data involved based on the data classifications set forth in the Written Information Security Plan, and the physical nature of the data, be it electronic or paper.

1.1 Investigation Worksheet

Once a report has been made the Investigation Worksheet (Appendix A) will be completed and kept on record with the Information Security Officer. If an incident is deemed a data loss event, a copy of the Investigation Worksheet and all evidence gathered during the investigation will be turned over to the College's General Counsel.

2.0 Response

After confirmation of theft, data breach, or exposure of Holy Cross data, the Security Officer will chair an Incident Response Team to handle the breach or exposure. The Incident Response Team will include members from:

- Public Safety
- The Office of the General Counsel
- The College's Risk Management Advisor
- Information Technology Services
- Public Affairs
- Selected representatives from the affected functional area(s) whose data may have been breached or exposed.
- Selected representatives from departments based on the data type involved.
- Additional individuals as deemed necessary by the Incident Response Team.

2.1 Unauthorized electronic acquisition of Protected or Sensitive Data

After confirmation of theft, data breach, or exposure of Holy Cross Protected data or Holy Cross Sensitive data the affected system(s) will have access removed to preserve evidence of theft and to identify the amount of data compromised. The functional owners of the system will be notified and plans of action will be put into place to protect the system(s) and regain functional access to the system(s). If the information is available on a site outside of Holy Cross, that site will be contacted to have the information removed as soon as possible.

2.1.1 Controls and Investigation

The IT Security Officer; and/or delegates, will evaluate the extent of the breach, exposure or theft. They will analyze the breach or exposure to determine the root cause. ITS will work with the appropriate parties to remediate the root cause of the breach or exposure. ITS will also examine any involved systems to ensure that the adjacent system(s) did not also house any Holy Cross Protected data or Holy Cross Sensitive data. If the systems are found to also contain Holy Cross Protected data or Holy Cross Sensitive data, the Security Team will immediately be notified. If a theft of physical property occurred, the Security Team will notify the Director of Public Safety. The Department of Public Safety will determine if it is also appropriate or necessary to involve other law enforcement agencies.

2.1.2 Digital Forensics

If the IT Security Officer; and/or delegate, determines that there is evidence that Protected or Sensitive data might have been exposed. The IT Security Officer may engage a third party digital forensics expert(s) to assist in the detailed analysis of the data loss to determine the extent of potential data exposed.

2.2 Unauthorized acquisition of Protected or Sensitive paper data

After confirmation of theft, data breach, or exposure of Holy Cross Protected data or Holy Cross Sensitive data, the affected physical area(s) will have access removed to preserve evidence of theft and to identify the amount of data compromised. The functional owners of the area(s) will be notified and plans of action will be put into place to protect the area(s) and regain functional access to the area(s) during the investigation. If the data loss was outside of Holy Cross, the proprietor of that location will be notified and restrictions to the location will be requested so that a proper investigation can take place and the necessary authorities notified. If a theft of physical property occurred, the Security Team will notify the Director of Public Safety. The Department of Public Safety will determine if it is also appropriate or necessary to involve other law enforcement agencies.

2.2.1 Controls and Investigation

If data that was being transported off-site or moved between secure and unsecure locations was exposed, the responsible department will be asked to produce a list of all records that were exposed or criteria necessary to evaluate the extent of the exposure. Using electronic or paper records, an evaluation will be made to the extent of the records exposure to confirm the size of the data set.

2.3 Unauthorized wireless devices

After confirmation of the detection of an unauthorized wireless device, the Information Security Officer will review the findings to determine if a threat exists and how to mitigate it.

3.0 Reporting to the MA Attorney General

The team, as described above, will provide information to the College's General Counsel, who under the advisement of the Data Security Officer, will decide on any necessary disclosure to the Massachusetts Attorney General and coordinate all communications with the MA AG office.

4.0 Reporting to the Public

The team, as described above, will provide information to the Department of Public Affairs and, if deemed appropriate, the Office of the President, regarding how the breach or exposure occurred, the types of data involved, the Holy Cross classifications of those data types, any protective measures around the involved data (such as encryption), and the number of internal/external individuals and/or organizations impacted. The Department of Public Affairs will handle all communications about the breach or exposure.

APPENDIX A -
Incident Worksheet

Incident Number

Incident	Date	Method Of Report
Reported	____/____/____	❑ Phone
Initial Investigation	____/____/____	❑ Email
Start Investigation	____/____/____	❑ Help Desk Ticket
End Investigation	____/____/____	❑ Anonymous
Final Report	____/____/____	❑ Other

A General

- ❑ Reporting Method Narrative and Follow-Up comments
- ❑ Security Team Member Roster
- ❑ Data Assessment and Classification Findings
- ❑ Functional User(s) Notification(s) / Other Correspondents to Community / Campus.

B Electronic

- ❑ Involved Systems List
- ❑ ITS Forensics and electronic Exhibits list with disposition
- ❑ 3rd Party Digital Forensics Team Contact Information
- ❑ Forensics Report
- ❑ IT Security Team Report

C Paper

- ❑ Involved Location(s) Report
- ❑ Physical Assessment Report
- ❑ Functional Area material access records / reports
- ❑ Public Safety Report

D Final Report

- ❑ Final Report by Risk Management Team

Policy # 350000-011
Date of Last Review Jan-31-2012