

# Canisius College Information Security Plan<sup>1</sup>

## I. Preamble

In order to protect critical information and data, and to comply with Federal Law<sup>2</sup>, the CIMS Security Steering Committee (CISSC)<sup>3</sup> proposes certain practices in the Canisius College information environment and institutional information security procedures. While these practices mostly affect the information processing in Information Technology Services (ITS), some of them will impact diverse areas of the College, including but not limited to the Business Office, the Office of Student Records and Registration, College Relations, Student Life, the Library, Admissions and Financial Aid, and third party contractors, including food services and the book store. The goal of this document is to define the College's Information Security Program, to provide an outline to assure ongoing compliance with federal regulations related to the Program and to position Canisius College for likely future privacy and security regulations.

## II. Gramm Leach Bliley (GLB) Requirements

GLB mandates that the College appoint an Information Security Plan Coordinator, conduct a risk assessment of likely security and privacy risks, institute a training program for all employees who have access to covered data and information, oversee service providers and contracts, and evaluate and adjust the Information Security Program periodically.

## III. Information Security Plan Coordinator

In order to comply with GLB, the College has designated the Chair of the CISSC to serve in the role of Information Security Policy Coordinator. The Chair of this Committee as well as the Committee members must work closely with college legal counsel as well as all relevant academic and administrative Schools and Departments throughout the College. The chair of CISSC is the Associate Vice President for Library & Information Services.

---

<sup>1</sup> Adapted from Catholic University

<sup>2</sup> The Financial Services Modernization Act of 1999 (also known as Gramm Leach Bilely (GLB) 15 U.S.C. §6801

CIMS Security Steering Committee Members:

- Associate Vice President for Library & Information Services (Chair),
- Controller
- Dean of Students
- Dean of Registration and Student Records
- Director of Administrative Computing
- Director of Financial Aid
- Director of Human Resources
- Director of Network Services
- ITS Security Officer

The Coordinator or the Coordinator's designee must help the relevant offices of the College identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information; evaluate the effectiveness of the current safeguards for controlling these risks; design and implement a safeguards program, and regularly monitor and test the program.

#### **IV. Risk Assessment and Safeguards**

The Coordinator or the Coordinator's designee must work with all relevant areas of the College to identify potential and actual risks to security and privacy of information. Each Department head, or designee, will conduct an annual data security review, with guidance from the Coordinator. Vice Presidents will be asked to identify any employees in their respective areas that work with covered data and information. In addition, the relevant departments of ITS will conduct an annual review of procedures, incidents, and responses, and will document all relevant materials. Selective publication of these materials is for the purpose of educating the College community on network security and privacy issues. ITS will assure that procedures and responses are appropriately reflective of those widely practiced at other institutions of higher education, as measured by four advisory groups: The Educause Security Institute, The Internet2 security working group, the SANS Top Twenty risks list, and the Federal NIST Computer Security Resource Center.

In order to protect the security and integrity of the College network and its data, ITS will develop and maintain a registry of all computers attached to the College network. This registry will include, where relevant, IP address or subnet, MAC address, physical location, operating system, intended use (server, personal computer, lab machine, dorm machine, etc.), the person, persons, or department primarily responsible for the machine, and whether the machine has special access to any confidential data covered by relevant external laws or regulations.

ITS assumes the responsibility of assuring that patches for operating systems or software environments are reasonably up to date for systems that it administers, and will keep records of patching activity. Furthermore, ITS will seek to enforce: i) currency with respect to security level of all systems attached to the network; and ii) virus and worm protection of all systems attached to the network. ITS will review its procedures for patches to operating systems and software, and will keep current on potential threats to the network and its data. Risk assessments will be updated annually.

ITS bears primary responsibility for the identification of internal and external risk assessment, but all members of the College community are involved in risk assessment. ITS, working in conjunction with the relevant College offices, will conduct regular risk assessments, including but not limited to the categories listed by GLB. Department heads will cooperate with the Committee and play an active role in addressing security in their areas.

The CISSC, working in cooperation with relevant College departments, will develop and maintain a data handbook, listing those persons or offices responsible for each covered data field in relevant software systems (financial, student administration, development,

etc.). ITS and the relevant departments will conduct ongoing (at least annual) audits of activity, and will report any significant questionable activities.

The CISSC will work with the relevant offices (Business Office, Human Resources, Student Records and Registration, College Relations, and the Library, among others) to develop and maintain a registry of those members of the College community who have access to covered data and information. ITS in cooperation with these offices will work to keep this registry up to date.

ITS will assure the physical security of ITS administered computers, including servers, which contain or have access to covered data and information. ITS will work with other relevant areas of the College to develop guidelines for physical security of any covered computers in locations outside the central server area. The CISSC will conduct a survey of other physical security risks, including the storage of covered paper records in non-secure environments, and other procedures which may expose the College to risks.

While the College has discontinued usage of social security numbers as student identifiers, one of the largest security risks may be the possible non-standard practices concerning social security numbers, e.g. continued reliance by some College employees on the use of social security numbers. Social security numbers are considered protected information under both GLB and the Family Educational Rights and Privacy Act (FERPA).<sup>4</sup> By necessity, student social security numbers still remain in the College student information system.<sup>5</sup> The College will conduct an assessment to determine who has access to social security numbers, in what systems the numbers are still used, and in what instances students are inappropriately being asked to provide a social security number. This assessment will cover college employees as well as subcontractors such as the bookstore and food services.

ITS will develop a plan to ensure that all electronic covered information is encrypted in transit and that the central databases are strongly protected from security risks.

All Canisius College employees are expected to adhere to the Canisius College Standards of Ethical Conduct. It is recommended that relevant offices of the College decide whether more extensive background or reference checks or other forms of confirmation are prudent in the hiring process for certain new employees, for example employees handling confidential financial information.

ITS will develop written plans and procedures to detect any actual or attempted attacks on covered systems and will develop incident response procedures for actual or attempted unauthorized access to covered data or information.

The Information Security Coordinator will periodically review the College's disaster recovery program and data-retention policies and present a report to the Vice Presidents.

---

<sup>4</sup> 20 U.S.C. § 1232g

<sup>5</sup> Social Security Numbers are kept both for historical purposes and due to the requirements of 26 U.S.C. § 6050S, the tuition payment credit reporting requirements.

## **V. Employee training and education**

While directors and supervisors are ultimately responsible for ensuring compliance with information security practices, ITS and the CISSC will work in cooperation with the Human Resources department to develop training and education programs for all employees who have access to covered data. These employees typically fall into three categories: professionals in information technology who have general access to all college data; custodians of data as identified in the data handbook, and those employees who use the data as part of their essential job duties.

## **VI. Oversight of Service Providers and Contracts**

The Information Security Plan requires the College to take reasonable steps to select and retain service providers who maintain appropriate safeguards for covered data and information. The Business Office will develop and send form letters to all covered contractors requesting assurances of GLB compliance.

## **VII. Evaluation and Revision of the Information Security Plan**

GLB mandates that this Information Security Plan be subject to periodic review and adjustment. ITS will review its policy and procedures at least once each year. Processes in other relevant offices of the College such as data access procedures and the training program should undergo regular review. The plan itself as well as the related data retention policy should be reevaluated annually in order to assure ongoing compliance with existing and future laws and regulations.

## **VIII. Definitions**

***Covered data and information*** for the purpose of this policy includes student and employee financial information required to be protected under the Gramm Leach Bliley Act (GLB). In addition to this coverage which is required by federal law, Canisius College chooses as a matter of policy to also define *covered data and information* to include any credit card information received in the course of business by the college, whether or not such credit card information is covered by GLB. Covered data and information includes both paper and electronic records.

***Employee financial information*** is that information the college has obtained from an employee in the process of offering a benefit or service. Offering a benefit or service includes all college sponsored benefit plans and college financial services such as the Employer Assisted Housing Program, computer loans, flexible spending accounts, and personal payroll services. Examples of employee financial information include bank and credit card account numbers, income and credit histories and social security numbers, in both paper and electronic format.

***Student financial information*** is that information the college has obtained from a student in the process of offering a financial product or service, or such information provided to

the college by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student's parent when offering a financial aid package, and other miscellaneous financial services as defined in 12 CFR § 225.28. Examples of student financial information include bank and credit card account numbers, income and credit histories and social security numbers, in both paper and electronic format.

#### **IX. Revision History**

*11/23/2004 Initial adoption, President's Cabinet.*