INFORMATION SECURITY PROGRAM

Trocaire has developed this Information Security Program ("ISP") to describe safeguards it has implemented to protect and maintain the confidentiality of covered non-public personal information received by the college in the course of providing financial services and products. This ISP is integral to the policies and procedures Trocaire has established on an institutional level to conform to legal requirements regarding information security, including compliance with the Federal Trade Commission's Safeguards Rule under the Gramm-Leach-Bliley Act ("GLBA").

Policy

It is Trocaire's policy to comply fully with the requirements of GLBA and other federal, state, and international laws regarding the protection of personal data. To that end, Trocaire's ISP describes how the college has addressed each critical component of GLBA's mandates:

- Appointing individuals to coordinate the Information Security Program;
- Conducting an assessment of foreseeable risks to the security of protected personal data received by the college;
- Designing and implementing administrative, physical, and technical controls to mitigate foreseeable security risks;
- Training employees whose job duties require access to protected personal data;
- Monitoring and overseeing service providers and vendors whose obligations involve receiving protected personal data; and
- Evaluating and adjusting the ISP periodically in response to changes in college operations.

Protecting Non-Public Personal Information

The financial products and services provided by Trocaire are most often related to student loans or financial aid, and procedures associated with arranging and paying for educational services received from the college. Personally identifiable information collected for such purposes may include non-public information concerning students, parents and guardians, spouses, or other third parties. GLBA's mandates apply to non-public personal information ("NPI") provided to Trocaire by a student or other customer, provided by a financial institution to the college, or otherwise obtained by Trocaire for purposes of providing a financial product or service.

NPI may include such information as addresses, phone numbers, email addresses, date of birth, asset statements, bank and credit card account numbers, tax returns and information, income and credit histories, drivers' licenses, and Social Security numbers. All such NPI, whether received in paper or electronic form, is subject to the requirements of GLBA and the terms of this ISP.

Coordination of Trocaire's Information Security Program

The Chief Information Officer is the designated individual responsible for coordinating Trocaire's Information Security Program.

Information Security Risk Assessment

Trocaire recognizes that the unauthorized use, disclosure, manipulation or compromise of NPI can have a detrimental financial, operational, legal and reputational impact on the college, its students and other stakeholders. Trocaire has completed an institution-wide risk assessment process to identify internal and external threats and vulnerabilities in order to protect the college's infrastructure and NPI. The risk assessment process includes:

- Completion of an inherent risk profile for discrete financial service functions performed by the college;
- Assessment of cybersecurity risks and preparedness represented by maturity levels across five domains; and
- Development of an agenda of actions items to improve risk management in relation to specific identified risks.

Information Security Risk Management and Mitigation

Trocaire has designed and implemented safeguards respecting its information systems, including controlled levels of access, firewalls and encrypted electronic mail for the protection of NPI. Physical security procedures have been implemented to ensure that information technology assets, network servers, and all hardware are housed in a manner to protect such assets from destruction, loss or damage. Incident response procedures have been implemented to address breaches of NPI, and to mitigate adverse affects of such losses. Trocaire has developed disaster recovery and continuity plans to protect and recover NPI in the event of a catastrophic system failure. The ISP coordinator regularly tests and monitors the effectiveness of the administrative, physical and technical safeguards surrounding Trocaire's information systems, to ensure that key controls and procedures remain effective to protect NPI.

Workforce Awareness and Training

Trocaire provides regular training for workforce members whose job duties involve access to NPI. The hiring process for such employees includes performing background checks, as appropriate based on the job position. New employees are provided with an orientation regarding the proper use and confidentiality of NPI, focusing on essential controls and procedures to prevent unauthorized disclosure. Information system user education and awareness is undertaken institution-wide, regardless of job duties, to further minimize information security risks and safeguard NPI. Adherence to Trocaire policies and procedures involving information security are an essential job function of all employees, and workplace discipline and sanctions for violations may be imposed, consistent with such policies.

Selecting and Overseeing Service Providers

Trocaire requires third-party vendors, service providers and outsourcing entities to maintain appropriate administrative, physical and technical safeguards regarding NPI. Trocaire's procurement process includes security reviews of service providers related to their handling of NPI, and the college engages in ongoing oversight of such entities. Contracts with service providers contain terms requiring the implementation and maintenance of safeguards regarding NPI.

Evaluating and Adjusting Information Security Program

Trocaire reviews this ISP annually and periodically repeats the risk assessment process described above to ensure that these information security safeguards remain appropriate for the college's operations. The ISP coordinators will evaluate and adjust administrative, physical and technical safeguards, as part of their ongoing administration and maintenance of the program. Any material changes in the college's operations that may impact the ISP will be reviewed and additional safeguards developed to address any newly identified risks or threats to NPI.

Effective Date/Last Revised:

July 21, 2022

Main Contact Information:

Kamu Pindiprolu
Chief Information Officer
Trocaire College
360 Choate Avenue
Buffalo, NY 14220
(716) 827-2421
pindiproluk@trocaire.edu

Other Contact Information:

Michael F. Cucinotta, MBA
Vice President of Finance and Administration
Trocaire College
360 Choate Avenue
Buffalo, NY 14220
(716) 827-2512
CucinottaM@trocaire.edu

Related Policies and Procedures:

Policy # 181 – Software Implementation and Standardization
Policy # 182 – Acceptable Use of Technology – Employees and Guests
Policy # 183 – Information Technology Incident and Recovery
Policy # 184 – Payment Card Processing and Cardholder Data Security
Policy # 772 – Technology Equipment Distribution
Policy # 773 – Personal Laptop, PDA and Other Equipment on Campus
Policy # 774 – Transfer or Disposal of College Technology Equipment