NIAGARA UNIVERSITY	**Category** *Select one or more:*	*Employment & Workplace:* *Operations & Finance:* *Compliance:*
	Sector: **Dept:**	*Executive Vice President*
	Approved By:	
	Effective date: **Revision date:**	

Niagara University Cybersecurity and Awareness Training (CAT) Policy

Purpose

Niagara University's Cybersecurity Awareness and Training (CAT) Program strives to ensure that the University community achieves and maintains at minimum a basic level of understanding of information security matters, such as general obligations under various information security policies, standards, procedures, laws, regulations, contractual terms and generally held standards of ethics and acceptable use of information resources.

CAT activities are initiated as soon as practical after faculty, staff and/or a student worker has been employed. The awareness activities are conducted on a continuous basis thereafter in order to maintain a reasonably consistent level of awareness.

Scope and Applicability

This policy applies to the University Community. Adherence to this policy helps safeguard the confidentiality, integrity, and availability of Niagara University's information assets, and protects the interest of Niagara University, its students, personnel, and business partners.

Definitions and Compliance

- **Cybersecurity Awareness Training (CAT)** - a formal process for educating employees about the internet and computer security. A good CAT Program must educate employees about institutional policies and procedures for working with information technology (IT).
- **University Community** - Includes faculty, administrators, staff, student workers and graduate/technical assistants.
- **Business Partners/Contractor** - someone officially attached or connected to Niagara University who is not a student or employee (e.g., contractors, vendors, interns, temporary staffing, volunteers.)
- **Personally Identifiable Information (PII)** - any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data is considered PII.
- **The Family Educational Rights and Privacy Act (FERPA)** - a Federal law that protects the privacy of student education records.

- **Health Insurance Portability and Accountability Act (HIPAA)** - demands that all HIPAA covered businesses prevent unauthorized access to "Protected Health Information" or PHI. PHI includes patients' names, addresses, and all information pertaining to the patients' health and payment records.
- **Gramm-Leach-Bliley ACT (GLBA)** - Requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data.
- **Stop Hacks and Improve Electronic Data Security Act (NYS SHIELD ACT)** - The SHIELD Act requires any person or business that maintains private information to adopt administrative, technical and physical safeguards.
- **Computing Resources***:* All Niagara University information processing resources, including all Niagara University's owned, licensed, or managed computing services, hardware, software, and use of Niagara University's network via physical or wireless connection regardless of the ownership of the computer or device connected to the network.

Policy

All authorized users with access to Institutional Data and Computing Resources shall receive sufficient training to allow them to protect Computing Resources adequately.

Additional and specific training are required for personnel with responsibilities related to programming, administering, and securing systems and for specific University community members with access to Protected Data or PII in accordance with compliance laws and regulations. Appropriate security training is completed before access is granted to Niagara University's Computing Resources.

The IT Department, ISOC and the Human Resources Department are responsible for developing and maintaining a program and provide:

- Initial and ongoing security awareness training on acceptable use of IT resources to the University community on an annual basis.
- Proper information security training as related to functional responsibilities.
- Educational opportunities to ensure information security personnel are equipped with the necessary security skills, knowledge, and competencies.
- All employees' acknowledgement in writing that they have read and understood Niagara University's Acceptable Use Policy.
- CAT that is incorporated into the new hire and new contractor orientation processes. Access to systems may not be provided until training is completed and a signed acknowledgment of security training has been received by the IT Department.
- Annual CAT refresher training that must be completed by all administrators, faculty, staff, student workers and authorized users.

Compliance

Niagara University reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy. Instances of non-compliance must be presented to, reviewed, and approved by the CISO, the Director of Information Technology, or the equivalent officer(s).

All breaches of information security, actual or suspected, must be reported to, and investigated by the CISO and the Director of Information Technology.

Those who violate security policies, standards, or security procedures are subject to disciplinary action up to and including loss of computer access and appropriate disciplinary actions as determined by Niagara University.