GLBA & Institutes of Higher Education (IHE)

In 2003, the Institutes of Higher Education (IHE) were added to the list of those who must comply with the requirements of GLBA, however, the IHE were never audited specifically on the requirements outlined within the GLBA safeguards and guidelines.

As of 2018, the Education Department (ED) has added these requirements to the audit list for Institutes of Higher Education due to their work with financial aid and other financial transactions.

Key requirements for institutions that must comply with GLBA:

• Designating an employee or employees to coordinate the information security program.

> **Awareity can help identify members of the institution who should be a member of a multi-disciplinary threat assessment team (MTAT) within the institution in order to improve security and safety within the college or university.**

• Identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of customer information, and assessing the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in operational areas, including employee training and management; information systems, including network and software design, as well as information processing, storage, transmission and disposal; and detecting, preventing and responding to attacks, intrusions, or other systems failures.

> **Awareity offers award-winning information security awareness training modules as well as trainings on PCI, FERPA, and HIPAA. Additionally the Awareness & Accountability Vault (AAV) within the Community-wide Fusion & Awareness Platform allows for institutions to keep their employees, staff, and third-party partners continuously aware of ongoing threats, policy updates, and other institutional procedures.**

• Designing and implementing information safeguards to mitigate the risks identified in the required risk assessment, and regularly testing and monitoring the effectiveness of those safeguards.

> **Awareity offers institutions the ability to create surveys in order to aid risk assessment and gap assessment requirements.**

• Evaluating and adjusting the information security program in light of changed circumstances.

> **Awareity's Awareness & Accountability Vault (AAV) is an innovative solution that allows institutions the ability to keep employees, staff, and third-party partners aware of new or adjusted policies as threats and circumstances change, while also allowing leaders and administrators the ability to have audit-ready proof of who is compliant and who isn't.**

For other ideas on ways to use your Awareity Platform, go to: awareity.com/vault-examples