Federal Trade Commission Safeguards Rule Amendments and how they impact higher education institutions

The deadline is approaching

What it is:

Effective June 2023, all higher education institutions that participate in the federal student financial aid programs authorized by Title IV of the Higher Education Act of 1965, as amended (Title IV) must adhere to the Federal Trade Commission (FTC) amended Safeguards Rule. Importantly, all Title IV institutions whether public, private nonprofit, or for-profit must comply with Gramm-Leach-Bliley Act (GLBA) cybersecurity requirements as a condition of Title IV participation.

The FTC has exempted institutions that maintain customer information concerning fewer than 5,000 consumers.

Information Security Elements of the Safeguards Rule

In order to develop, implement, and maintain the information security program, entities are required to:

- Designate a qualified individual (QI) to supervise the information security program.
- Create, maintain and manage an information security program (ISP) based on a risk assessment appropriate for the organization and in light of monitoring and material changes to operation.
- Create and maintain, periodically a written risk assessment of the environment and is modified as operations change
- Design and implement safeguards to control the risks including:
    1. Access controls in accordance with least privilege principle.
    2. Conduct periodic inventories of data and systems that handle it.
    3. Encrypt all customer information inflight and at rest.
    4. Adopt secure development practices for in-house app development.
    5. Implement MFA or equivalent for apps that access customer data.
    6. Implement and maintain secure disposal of customer information.
    7. Adopt change management procedures.
    8. Implement monitoring and logging of authorized user access and data manipulation.

- Regularly test or monitor the effectiveness of safeguards, key controls and systems.
- Put in place policies and procedures to ensure security personnel are able to enact the internet security program.
- Oversee/monitor service providers by taking reasonable steps to ensure they are capable, require them by contract to implement safeguards, periodically assess based on risk they present.
- Establish and maintain a written Incident Response Plan covering 7 categories.
- QI to report in writing at least annually to board or equivalent, covering:
  1. Overall status of the Internet security program.
  2. Material matters including risk assessment and management, control decisions, service provider arrangements, test results, security events and or violations and response.
  3. Recommendations for changes to Internet security program.

CBTS security experts can help you through each step on your journey to compliance

Step 1: Establish safeguard team

Step 2: Perform written risk assessment

Step 3: Establish written information security program

Step 4: Implement information security training program

Step 5: Perform phishing and penetration testing

Step 6: Assess vendor agreements and contracts

Step 7: Implement effective and verified access controls including MFA

Step 8: Ensure all PII data is encrypted at rest and inflight

Step 9: Create a written Incident Response plan

Step 10: Create an annual written report for board

If this impacts your business, we recommend reviewing the full **Safeguard Rule**, **What your business needs to know**, and **FTC Small Business Guidance.**

CBTS cybersecurity experts can ensure compliance within your required framework. **Contact us** to discuss how we can help.

From developing and deploying modern apps and the secure, scalable platforms on which they run to managing, monitoring, and optimizing their operations, CBTS is the trusted partner businesses need to thrive in the application era.

Contact us today.

cbts