FULLY ENFORCEABLE SINCE JUNE 2023

FTC Safeguards Rule Checklist

If your firm handles customers' financial information - and "financial institution" under GLBA means far more than banks - the Safeguards Rule requires a written security program. The full page:
www.crccloud.com/services/compliance/ftc-safeguards/

The nine required elements

- ☐ **Designate a Qualified Individual to run and be accountable for the security program.**
- ☐ **Conduct a written risk assessment of where customer information lives and how it's exposed.**
- ☐ **Implement access controls and a current inventory of customer data.**
- ☐ **Encrypt customer information at rest and in transit.**
- ☐ **Enforce multi-factor authentication for anyone accessing systems with customer information.**
- ☐ **Adopt secure development and change practices for apps that handle the data.**
- ☐ **Continuously monitor, or run regular penetration testing plus vulnerability scans.**
- ☐ **Oversee your service providers and require them to safeguard the data too.**
- ☐ **Maintain a written, tested incident-response plan and train your staff; keep it all documented.**

Don't forget

- ☐ **Report qualifying security events, 500+ consumers, to the FTC**
  a duty added in the amended rule.
- ☐ **Keep the written program current as your environment changes**
  it's a living document, not a one-time file.
- ☐ **If you're a tax firm, your IRS WISP and this rule are largely the same project, done once.**

CRC Cloud operates the technical backbone the program stands on - encryption, MFA, monitoring, and the tested incident-response plan - inside Secure IT.

The free 30-minute assessment maps your current answers against the Safeguards Rule, honestly.