

Compliance with the Safeguarding Requirements of Gramm-Leach-Bliley Act (GLBA)

Products: TitleTec ELT, TitleTec Florida, TitleTec Georgia, TitleTec Maryland, TitleTec NAT, TitleTec Pennsylvania

At TitleTec, supporting you – our customers – is our top priority. We are aware that many of our dealer customers are concerned about the new Gramm-Leach-Bliley Act Safeguarding Rules (“GLBA Requirements”) that will come into effect on December 9, 2022. We have compared these requirements with the protections we have in place for the products you use. TitleTec already had a robust set of information security policies to ensure the safety of data entrusted to us. Below is an analysis of GLBA Requirements and a summary of current and planned compliance in the TitleTec Products.

§ 314.3 - Standards for safeguarding customer information.	
138 (a) Information security program.	TitleTec has policies covering: • <i>Acceptable user of assets</i> • <i>Asset Control</i> • <i>Change Management</i> • <i>Clear Desk and Screen</i> • <i>Cyber Security</i> • <i>Event Management</i> • <i>Incident Management</i> • <i>Information Classification</i> • <i>Information Security</i> • <i>Mobile Device</i> • <i>Physical Security</i> • <i>Remote Working</i> • <i>Supplier Relationship</i> TitleTec also has SOC2 Type 1 certification.
§ 314.4 – Safeguarding Elements.	
(c)(1) Access Control	We authenticate and permit access only to authorized users; we limit our authorized users’ access only to customer information needed to perform their duties & we limit customer access to their own information.

(c)(2) Data Mapping	We have mapping of data to identify and manage the data to securely provide services to our customers
(c)(3) Encryption	All data entrusted to us is encrypted in transit over external networks and at rest as part of our products and services
(c)(4) Secure Development Practices	TitleTec has internal policies for secure development practices. Customer data is stored only in production databases and is not available in lower development or testing environments.
(c)(5) Multi-factor Authentication	This will be implemented in production by June 2023.
(c)(6) Data Retention & Disposal	TitleTec maintains and disposes data in accordance with data retention compliance regulations from each state in which we do business. Data retention policies will be in place by June 9, 2023.
(c)(7) Change Management	We have a process for Change Management
(c)(8) Monitoring	TitleTec products are monitored to detect unauthorized activity. Logs are kept of authorized user activity.
(d)(1) System Testing & Monitoring	TitleTec has a security team responsible for monitoring and testing infrastructure to detect and control attempted intrusions.
(d)(2) Penetration Testing and Assessments	TitleTec's SaaS products are continuously monitored. Periodic penetration testing and vulnerability assessments are conducted.
(e)(1) Training	TitleTec employees are required to take monthly security trainings.
(e)(2) Information Security Program	TitleTec has a dedicated team of information security professionals led by a Chief Security Officer who is responsible for managing security risks.
(e)(3) Security Updates	Information security personnel receive periodic training on security practices and risks
(h) Incident Response Plan	TitleTec has an incident management plan and a business continuity plan.