

GLBA Compliance

Automate and simplify GLBA compliance using DataSecurity Plus



Automate and simplify GLBA compliance using DataSecurity Plus

The Gramm-Leach-Bliley Act (GLBA)—also known as the Financial Services Modernization Act—mandates the standards that financial institutions, such as commercial banks, security firms, insurance companies, and credit unions, need to follow to ensure the confidentiality and security of their customers' financial records and personal information. Failure to comply can result in dire consequence for businesses, including imprisonment of directors and officers for up to five years, penalties up to \$100,000 per violation, or both.

Become GLBA compliant using DataSecurity Plus

DataSecurity Plus' audit tools help protect your organization's critical information against loss, misuse, unauthorized access, or modification by proactively identifying and addressing potential threats using preconfigured alerts. In addition, DataSecurity Plus' robust auditing and reporting capabilities help ensure data integrity, prove regulatory compliance, and verify role-based access, ensuring business continuity.

Below is a list of reports you can use to prove that your organization is GLBA compliant.

GLBA standards	DataSecurity Plus report or alert
Track all modifications to files in order to assess risks to data integrity and resolve violations, if any.	All file/folder changes report
	Deleted/overwritten files report
	Security permission changes report
	Most modified file report
	File modified after N days report
	Create events report
	Renamed/moved events report
Periodically review all attempts to access critical data, including both successful and failed attempts.	All failed attempts report
	Read events report
	Most accessed file report
	Most accesses by processes/user report
	File accessed after N days report
Review access rights and file permissions periodically to ensure that no excessive permissions are assigned beyond what is needed.	NTFS permissions report
	Share permissions report
Utilize customizable alerts to enable timely detection of any user actions that violate your data protection policies.	File/folder moved or renamed alert
	File/folder security changes alert
	File/folder removed alert
	Media files alert
Use preconfigured alerts to detect and respond quickly to potential data breaches.	Ransomware file alert
	Threshold-based alert

* You can also generate customized reports based on file path, users, business hours, etc..

DataSecurity Plus

ManageEngine DataSecurity Plus is a unified data visibility and security platform. It audits file changes in real time, triggers instant responses to critical events, shuts down ransomware intrusions, and helps organizations comply with numerous IT regulations. It analyzes file storage and security permissions, deletes junk files, and detects security vulnerabilities. Users can assess the risks associated with sensitive data storage by locating and classifying files containing personally identifiable information (PII), payment card information (PCI), and electronic protected health information (ePHI). It also prevents data leaks via USBs, email, printers, and web applications; monitors file integrity; and audits cloud application usage. Together, these capabilities ensure the all-round protection of data at rest, data in use, and data in motion.

To explore these features and see DataSecurity Plus in action, [check out the online demo](#). To learn more about DataSecurity Plus, visit www.datasecurityplus.com.

↓ Download free trial

\$ Get a quote

Explore DataSecurity Plus' capabilities



File server auditing

Audit and report on file accesses and modifications, with real-time alerts and automated responses for critical file activities.

[Learn more](#)



File analysis

Analyze file security and storage, manage junk files, optimize disk space usage, and identify permission vulnerabilities.

[Learn more](#)



Data risk assessment

Discover and classify files containing sensitive data such as PII, PCI, and ePHI by combining content inspection and contextual analysis.

[Learn more](#)



Data leak prevention

Detect and disrupt data leaks via USBs, email, web applications, and printers; monitor endpoint file activity; and more.

[Learn more](#)



Cloud protection

Track enterprise web traffic and enforce policies to block the use of inappropriate, risky, or malicious web applications.

[Learn more](#)