

Prenger Solutions Group Security Policy

At Prenger Solutions Group (PSG), we take the security and reliability of your data seriously. Our team works diligently to ensure that your data remains safe and that our systems are accessible when you need them by continuously improving our policies, governance and technologies, and follow NIST standards as the guiding framework for our operations. These documents reflect our PSG security practices including internal governance, operations and our approach to partnering with other platforms. Our Privacy Policies, which describe how we collect and use data from our customers, can be found at prengersolutions.com/privacy-policy.

Internal Systems

Devices and Network

Inventory, maintenance and network security on equipment and software used by PSG staff is outsourced to a US-based IT firm.

Inventory, maintenance and network security on PSG technology assets is overseen by InfiNet, a US-based IT firm which utilizes Sentinel One's software for cybersecurity. See Sentinel One Compliance for credentials.

Internal network user accounts are managed by Microsoft with MFA and are monitored for suspicious activity. Incident recovery operations are practiced on a regular basis.

File storage, transmission and backup are done on Microsoft SharePoint and best practices are followed for security policy governance and user management with authenticated access.

Internal Security Training and Processes

At Prenger Solutions Group new employees are educated on security and data privacy, customer data rights, sharing methods, cybersecurity, and confidentiality agreements. Employee and contractor onboarding includes education or review of security procedures, multifactor authentication, LastPass password security, and confidentiality agreements. Regular training and professional development happen on an ongoing basis. PSG has secure access and remote wipe protection on all laptops. Employee and contractor offboarding includes collection of all PSG equipment which is then scanned and reviewed to ensure the former employee or contractor cannot access internal files or information. Employee or contractor owned phones must remove email and all other apps.

Our Products and Services

Data Access and Processing

Our approach to managing transmission of and access to client data is based on a Role-Based Access Control (RBAC) system, which grants access based on the principles of least privilege and need-to-know.

Within this system, administrative access to client data is reserved exclusively for limited support staff and based on client request. Our DevOps processes maintain clear segregation between development and production environments, which creates an additional layer of security. This

separation ensures that only authorized production-level employees have access to client data, safeguarding it from any unauthorized access and potential risks.

See our Privacy Statement at prengersolutions.com/privacy-policy for information on how PSG collects and uses data on its customers.

Applications

PSG platforms are powered by AWS (Amazon Web Services), known for its top-notch cloud solutions and security measures. By relying on AWS for hosting, disaster recovery and identity management PSG eliminates the need to manage any internal hardware or software that could potentially impact the uptime and security of our application. AWS handles all aspects of application infrastructure and uptime.

In addition to ongoing monitoring of native AWS security features we are reviewed annually for our compliance with AWS Well Architected framework review (WAFR) by an AWS WAFR partner. This review includes both security and architecture best practices. WAFR reviews assess excellence in development operations, security, reliability, performance, cost optimization and sustainability.

Third-Party Governance

PSG undertakes a thorough vetting of all third-party tools used to process data or integrate our existing platforms. This includes a review of security statements, certifications and governance processes.

In addition, PSG assigns staff to each application who are responsible for monitoring of third-party updates, downtime and changes so that we can act quickly on behalf of our customers should an incident arise.

Compliance

PSG maintains SOC 2 compliance. Our current SOC 2 trust report is available at app.vanta.com/prengersolutions.com/trust/vs95ddqmm3yc6w5zmedmg.