PARKLANE SYSTEMS

Parklane Privacy Policy
(Including Hosting Services)

Privacy and Security

Parklane Systems Inc. provides hosting services referred to as SAAS (Software as a Service). Our services are located onsite in London, Ontario, Canada, with backup facilities in Woodstock, Ontario, Canada. All data maintained by our hosting services resides wholly in Canada.

What We Collect

To use our SAAS services, our application collects and processes Employee Personal and Health information (data).
We respect your privacy and your data maintained in our application.

- We do not disclose, sell, or trade your data.
- We would not transfer your data to a third-party without your written consent.
- We do not give Parklane employees access to your data without your written consent (in a possible case of troubleshooting).

Security

We take security seriously, and the security of your data is important to us. We employ a variety of security measures to maintain the safety of your data.

- Your application and data is stored on secured servers.
- Our servers are encrypted-at-rest using AES-256-XTS LUKS and cryptographic keys.
- All data is transmitted via encryptions AES 256 and SSL technology.
- Your server, application and data can only be accessed by authorized personnel who are restricted to performing software updates, server upgrades and maintenance.

Our Hosting environment is designed to isolate/containerize each customer deployment. Firewalls and network access control rules are in place to limit the access to customer data and services if a breach were to occur. Alerts and monitoring are also in place for the Parklane IT Staff to monitor the hosting environment for security and availability issues.

No method of transmission over the internet or electronic storage is completely secure, so we cannot guarantee its absolute security; therefore you must make certain your responsibility. The application and data is protected by user passwords, which your users should choose carefully and keep secure. If they disclose a password to a third-party, you may lose considerable control over your data. If the security of any password has been compromised, for whatever reason, it should be changed immediately.

We provide additional methods that can be optionally employed by you to protect attempted malicious log-ins.

- Mandatory password strengths
- Mandatory password resets every X months
- Automatic application shut-down after 3 failed attempts
- Email alerts after X failed attempts within a specified number of hours
- Email alerts, plus prohibiting new log-ins after x failed attempts within a specified number of hours

Sensitive Information

When using Parklane Support Services we ask that you do not send or disclose to us any sensitive personal or health information, including social insurance, information related to racial or ethnic origin, political opinions, religion or other beliefs, or, health. In the case of data samples or screen shots, such information should be redacted.

Your Rights

You are afforded certain rights regarding your data. These include your right to access, manage and report on the data contained within the application. At no time does Parklane staff have the physical means to access your application or data.

Retention

Backups of your data are performed nightly with a 12 hour replication service. Backups will be used to restore your data or account in case the data corruption or damage.

We may retain backups of your hosting content for up to 3 months after your hosting service is terminated. If you wish your information to be deleted prior to this, you may request such in writing.