pirana cmms

SECURITY STATEMENT

Easy to use, affordable maintenance software

Thousands of users use Pirana CMMS with their CMMS data, and we make it a priority to take security and privacy concerns seriously. We strive to ensure that user and system data is handled securely. Shire Systems uses industry standard technology for security. This Security Statement is intended to provide transparency about our security infrastructure and practices, to help reassure you that your data is appropriately safeguarded.

Customer Data Security

- **Privacy:** We have a comprehensive privacy policy that provides a transparent view of how we use, share and retain customer data.

Organisational & Administrative Security

- **Information Security Guidelines:** We maintain internal information security guidelines and routinely review and update them.
- **Service Providers:** We screen our service providers and only select proven accredited service providers.
- **Backups:** Backups occur daily and are replicated off-site for disaster recovery purposes.
- Uptime: We are committed to making Shire Pirana CMMS available to our customers 100% of the time, 24x7x365 excluding scheduled maintenance. Shire is not responsible for user error, hardware breakdown and connectivity problems outside of our control.

Network Security

- **Antivirus & Malware:** All Shire Systems desktop computers, workstations, laptops and servers are required to have continually operating, approved anti-virus and malware software with the current virus/malware definitions.
- **Firewalls:** Our inbound Cisco firewall is configured in a default deny mode with ports explicitly opened to allow inbound traffic. Traffic can be restricted by protocol, service port, and source IP address. This firewall is designed to prevent hackers from entering the system and searching files and information.
- **Encryption:** Where appropriate, network traffic is encrypted in transit.
- **Access to Customer Data:** Shire staff do not have access to customer data as part of normal company operations. Only for support purposes or where required by UK Law, will we interact with customer's data but only at the request of the customer.

Physical Security

- **Employee Access Control**: Shire Systems' premises are protected by 24 hour security monitoring systems and electronic user access control systems.
- **Data Centres:** All Shire Systems' information systems and infrastructure are maintained at our head office or hosted in world-class data centres. These data centres include all the necessary physical security controls such as 24/7 monitoring.
- **Passwords:** By default, the main password mush be at least six characters long and have at least one non-alphanumeric character.

023 8022 4111 The UK No 1 info@shiresystems.com

pirana cmms

SECURITY STATEMENT

Easy to use, affordable maintenance software

- **Data Encryption:** Network traffic can be encrypted using SSL Certificates in Microsoft IIS.
- **Data Portability:** Data is exportable through the main application in the form of the Export to Excel feature in Grids and Reports. It can also be accessed directly through SQL Server, and this is protected through the use of SQL Server Security. This can be configured to use Network Security or a specific SQL Server user account. An external interface is provided for SOAP/XML communication. This is limited to HTTP/HTTPS and its use is restricted by the use of Special Tokens (Licenses) and the use of a PIN number.
- **Security Patches:** Code is regularly reviewed or any potential Security risks. If one is ever found, a patch if raised for the latest version as soon as possible. Likewise, if a security issue is found with any 3rd Party Library or tool, at patch is produced for the current latest version as soon as possible.

Software Development

- **Code:** Code is maintained in Microsoft Visual Studio Team System, and restricted to only Shire Personnel. No security details are hard coded into the system.
- **Coding standards:** The Shire Systems development team follow C# and Microsoft guidelines for naming conventions, code formatting and code construction.
- **Deployment:** The application may be deployed via an Installation Package. This relies on the user entering the account details for their SQL Server if they are not installing the default packaged version.
- **Compliance and Certifications:** The Shire Systems development team are Certified Microsoft Developers and Testers.

Security Breaches

Due to the nature of modern day security threats and despite best efforts, we cannot guarantee 100% security. However, if we learn of a security breach, we will notify affected users immediately so that they can take appropriate action. Notifications may take the form of email or website notices.

Your Responsibilities

It is your responsibility to keep your data secure by using sufficiently complex passwords and storing them securely. You are responsible for ensuring that you assess security risks and that you have sufficient security on your own IT network and systems. It is also your responsibility to ensure that your user accounts are configured to control appropriate levels of user access.
In addition to your regular backups, you should take a special backup copy of your data when updating to a new version of Pirana or before systems / network maintenance.

Customer Requests

Due to the number of customers using our systems, specific security questions or security forms cannot be dealt with on an individual basis.

This policy should be read in conjunction with The Shire Systems Data Protection Policy and The Shire Systems Limited Privacy Statement. Both of these are available from the Shire Systems website. Last updated: May 2018