PCI Compliancy

The Payment Card Industry Data Security Standard (PCI DSS) is a requirement of any company or organization that stores, processes, transmits or comes into contact with cardholder data as of June 30, 2005. Most companies with an e-commerce or transactional component to their model fall under this umbrella. The following information was pulled from https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml:

> The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.
>
> The core of the PCI DSS is a group of principles and accompanying requirements, around which the specific elements of the DSS are organized:
>
> **Build and Maintain a Secure Network**
> - *Requirement 1:* Install and maintain a firewall configuration to protect cardholder data
> - *Requirement 2:* Do not use vendor-supplied defaults for system passwords and other security parameters
>
> **Protect Cardholder Data**
> - *Requirement 3:* Protect stored cardholder data
> - *Requirement 4:* Encrypt transmission of cardholder data across open, public networks
>
> **Maintain a Vulnerability Management Program**
> - *Requirement 5:* Use and regularly update anti-virus software
> - *Requirement 6:* Develop and maintain secure systems and applications
>
> **Implement Strong Access Control Measures**
> - *Requirement 7:* Restrict access to cardholder data by business need-to-know
> - *Requirement 8:* Assign a unique ID to each person with computer access
> - *Requirement 9:* Restrict physical access to cardholder data
>
> **Regularly Monitor and Test Networks**
> - *Requirement 10:* Track and monitor all access to network resources and cardholder data
> - *Requirement 11:* Regularly test security systems and processes
>
> **Maintain an Information Security Policy**
> - *Requirement 12:* Maintain a policy that addresses information security

Print Tracker is PCI compliant because it does not store, process, transmit or come in contact with any cardholder data or other personal information.

> Print Tracker is a software tool that gathers meters and status information from imaging devices like copiers and printers. It contacts network devices using their IP addresses and requests device information via the Simple Network Management Protocol (SNMP). Communication is fulfilled via port 161. If SNMP provided information is incomplete, Print Tracker may request data from the device's embedded web server over port 80. The information gathered includes the device's network name, MAC address, model, serial number, total page counter, color page counter, prints, copies, faxes, scans, location, and status. Print Tracker CANNOT gather printed content or interpret user intent. If desired, IP addresses of devices may be blocked from reporting.
>
> Imaging device data that Print Tracker captures is encrypted and sent to a secure web server using the HTTPS protocol over port 443. The secure web server addresses used include https://secure.tc101.com and https://secure.nexation4.com. All data transfer is encrypted and initiated on site. There is no remote access option with Print Tracker and Print Tracker CANNOT receive incoming transmission.

If additional PCI Compliancy clarification is required, please contact Print Tracker Support at 866-629-3342 or email inquiries to: Support@PrintTracker.net.