



## Paycor Security Statement

### Purpose

Systems security and data safeguarding are extremely important to Paycor. Paycor systems are designed and managed to provide security. This document describes the policies and procedures in place to safeguard our systems and your data from unauthorized access, as well as recover your data if it is lost. Our systems are as follows: Perform, Paycor Payroll, and Online Services (including Online Reporting, Employee Online Check Stubs, and HR Application). If you have any questions about the security of your data, please contact our security administrator at [info@paycor.com](mailto:info@paycor.com).

### Security

Paycor has taken the necessary steps to ensure your data is protected in accordance with industry standards. Paycor's servers reside at Paycor's primary data center, a third-party tier-3 data center located in Lebanon, OH. Paycor maintains a data center at its headquarters for limited processing. All of Paycor's servers are managed by Paycor employees.

Users are not able to access any Paycor systems until they are logged in and authenticated. All user sessions are maintained via SSL/HTTPS to ensure that all data passed between the browser, client, and Paycor servers is encrypted during transmission both from and to the client. When necessary, data file transfers are password protected, encrypted and maintained via Web Services to ensure that all data passed between client and Paycor servers is protected.

All source code is designed and extensively tested by Paycor to ensure data security. Authenticated users are granted access only to the applications and functionality for which they have permission. All requests and actions within the system are checked to verify that user permissions exist.

All uploaded files are stored in an unpublished directory and are not accessible directly by URL. All requests to view or download these files must be authenticated by the Paycor system.

### Data Archival and Backup

To ensure that no client data is lost, Paycor performs daily backups of its databases, uploaded files, and source code. The backups are replicated daily to Paycor's disaster recovery data center. Then, the monthly backup files are written to tape and sent offsite to a third-party storage facility.

Paycor's corporate headquarters, primary data center, and backup data center are protected by power generators.