HOUSING FIRST University
A program of Pathways to Housing PA

HousingFirstUniversity.org
5201 Old York Rd. Fourth Floor
Philadelphia, PA 19141
215-390-1500 x1708
Training@PathwaystoHousingPA.org

Security Policy

Pathways to Housing PA (PTHPA) will maintain the security of payment card data for all Housing First University (HFU) related activities, and will adhere to all applicable general requirements, standards, specifications, and maintenance requirements related to Payment Card Industry (PCI) Data Security Standards. PTHPA has appropriate safeguards in place to protect the integrity, confidentiality, and availability of payment card data that is received, or managed, by HFU.

HFU Payments

All payments made to HFU for training/events are collected through Soapbox, processed through Paypal, and then stored and tracked within the Salesforce database. Any information regarding the PCI Data Security Standards for each of these third parties may be found at their respective websites.

In the event that PTHPA is notified about a data breach by any of the above mentioned third parties, PTHPA will notify all individuals who have registered and/or attended any HFU related training and share all available information regarding the breach. PTHPA will continue to provide any information received from the third parties to those individuals until the matter is resolved.

Internal Data Security

All PTHPA devices adhere to the following security standards:

- All smartphones are password protected to ensure safety of all internal databases and PTHPA email accounts. If passwords are removed from individual phones, email and access to the internal server are automatically deactivated.
- All computers are password protected.
- Access to all internal databases and software require double-authentication to ensure security.

On a daily basis, the PTHPA Information Technology team monitors the system for any suspicious activity. Each morning the internal server logs are reviewed and Kaseya software is used to ensure that if any data breach is detected, the IT department is immediately notified.

In the event of an internal data breach, the IT department will receive immediate notification from the server. The individual whose device has been breached will be notified by the IT department and will be instructed to shut down all open applications, disconnect from the network, and then shut down their computer. The computer will then be returned to the IT department where they will erase the hard drive and restore the computer to its' original factory settings.