Privacy and Safeguards

Last Modified on 08/15/2023 4:18 pm EDT

Note: This documentation applies to the OP Cloud environment.

Office Practicum has implemented the following policies and procedures to safeguard the confidentiality and security of data stored in our hosted environment:

- Our hosting facility is SSAE 16 certified.
- The minimum number of personnel required for optimal support are given access to the servers and related hardware.
- Security cameras monitor the data center environment 24x7.
- The hardware that stores your data is protected by use of electronic card readers and/or biometric verification for access.
- Data at rest is encrypted with AES-256 encryption.
- Data is replicated within the data center environment to provide redundancy.
- Firewall rules are used to restrict the type of external traffic that can enter the hosted environment from the internet.
- Communications between client workstations and the data center are SSL/TLS encrypted to protect PHI.
- We segment servers into separate networks based on their purpose (web/application/database) and use restrictive firewall rules within the environment to segregate your data and operations from other clients'.
- Unnecessary software has been removed from all servers to reduce the risk of interference with the operation of OP and to reduce the environment's attack surface.
- Policies have been applied to restrict the functionality available to end users on the servers hosting OP. The policies isolate the practices from each other and from the operations of the server environment itself to reduce the likelihood of users making inadvertent (or malicious) changes to the environment.
- We have implemented a network level intrusion prevention system which helps reduce the likelihood that certain attacks against the network will succeed.
- Host-based intrusion and malware detection systems are installed on all servers.
- OP employees with access to our hosted environment are required to employ strong passwords, multi factor authentication, and regular password rotation.
- Security patches are applied on a regular basis.
- We audit all successful and failed logon attempts.
- Practice data is backed up daily. Daily backups are retained for 30 days. After 30 days, monthly backups are retained for 24 months. All backups are encrypted using AES-256 (which meets FIPS-140 standard).