

Part 5

IPERS Data Sharing Agreement

AGREEMENT made this ____ day of _____ 2019, between the Iowa Public Employees’ Retirement System (hereafter referred to as IPERS), and the _____ (hereafter referred to as Vendor).

Background

- 1. The IPERS is a participating agency and, therefore, must comply with the State of Iowa Enterprise Data Stewardship Security Standard. In addition IPERS must comply with state and federal laws pertaining to the confidentiality, use and disclosure of personal information.
2. Vendor is not participating agency for the purposes of the State of Iowa Enterprise Data Stewardship Security Standard but must comply with state and federal laws pertaining to the confidentiality, use and disclosure of personal information.
3. This agreement outlines the terms, by which the IPERS and Vendor will share data, including confidential and/or personally identifiable information and also provides the terms under which parties shall maintain the confidentiality of the data to be shared.

Terms and Conditions

- 1. Purpose of the Agreement. IPERS has agreed to share member’s confidential, personally identifiable information and other data to fill in variable data fields with Vendor, for the limited purpose for Vendor to accomplish tasks associated with the printing of IPERS forms.
2. Data Sharing Procedure. IPERS will provide Vendor with:
- Data containing members confidential and personally identifiable information to be used to fill in variable data fields on IPERS forms for printing
- Data will be supplied via ShareFile (ipers.sharefile.com)
3. Confidentiality of Information. Vendor agrees that access to the data will be restricted to authorized individuals.
4. Data Security. Vendor agrees to store the data securely.
- Paper documents, DVDs, or other removable media containing data shall be stored in a locked cabinet, in a restricted area, accessible only to authorized individuals.
- Workstations, laptops, or servers storing data shall be password protected using strong passwords.
- Laptops containing data shall be encrypted using whole disk encryption (AES 256-bit or stronger).
5. Data Destruction. Vendor agrees that when the intended use of the data has been completed, it shall dispose of the information through the following destruction methods:
- Wipe (e.g., scrub) hard drives, or any other electronic storage media, containing data using a DoD approved destruction method. Hard drives that cannot be wiped shall be physically destroyed by shredding;
- Shred hard copy data such that the resulting residue prevents any recovery of the data file content.
6. Redisclosure of Data. Vendor agrees not to redisclose the data received from IPERS to a third party not covered by the agreement unless written permission by IPERS is received and redisclosure is not prohibited under applicable law.
7. Data Breach. Vendor shall notify IPERS, OCIO – Information Security Division and all affected individuals if the data is lost, stolen or disclosed to non-authorized individuals. Vendor shall accept responsibility for any events caused by the disclosure.
8. Term. This agreement is effective on the last date signed by a party and shall remain in effect until destruction or return of the data.

Name _____

Signature and Date _____

Name _____

Signature and Date _____