

|  |  |
| --- | --- |
| Governed By:Administration | Effective Date:3/21/2020 |
| **Procedure**: Data Security of private information procedure | Updated Last:4/15/2021 |

Agency staff are required to maintain compliance with the NY SHIELD Act and must take reasonable safeguards to protect the security, confidentiality and integrity of sensitive and/or private data to include the personal data consisting of any information in combination with any **one or more** of the following data elements;

* + social security number;
  + driver’s license number or non-driver identification card number;
  + account number, credit or debit card number, in combination with any required security code, access code, password or other information that would permit access to an individual’s financial account.
  + username or e-mail address in combination with a password or security question and answer that would permit access to an online account.

The procedures below will ensure ongoing compliance with the NY SHIELD Act:

**Computer/Electronics**

* If you are stepping away from your computer for any reason you must minimize your open screens or turn your monitor off.
* If you are serving customers and they are able to see your computer screen a privacy screen should be used.
* Do not share your passwords to any computer or database at any time.
* Do not save your username and password information if offered by the website or access location.
* Any personal data should only be accessed using an agency issued device.
* If any personal information is to be shared via email this must be done through encryption or secured process.
* Any email with personal information must have an approved confidentiality notice.

**Paperwork/Files**

* While serving a customer you must ensure there is no private data visible on your desk.
* Do not leave a customer unattended in your office space at any time.
* Any files or paperwork with sensitive data must be secured in a desk or filing cabinet any time you step away from your desk, and at the end of each shift.
* Only required data should be maintained in files. Paperwork containing personal data that is no longer needed must be properly labeled and stored according to program record retention requirements.
* Copies of personal information should not be made unless required by the program funding source.

**Transporting/Remote Work**

* Staff that may transport/remove files from their primary location will follow the established sign out process.
* Files containing personal information may not be left in a vehicle.
* Files must be secured at all times, and never left unattended, in any remote work environment.

In order to ensure compliance with all NYS SHIELD Act the following procedures must be followed by staff at all times. Any additional program specific procedures will meet or exceed these requirements be provided by your program supervisor. Please reach out to the program supervisor if you have any questions or need any additional guidance on the procedures outlined in this document.