RECORD MAINTENANCE POLICY

Policy Number: 259 R2
Effective Date: July 1, 2020
Date Last Revised: September 1, 2022

I. POLICY:

WorkFirst Contractors are required to maintain, retain and dispose of all fiscal and program records funded under the Commerce WorkFirst Programs. This policy sets forth the minimum requirements for records maintenance of confidential information. For more information on Data Security Requirements, see Attachment 1 Data Security Requirements. For more information on Data Sharing Requirements, see Attachment 2 Data Sharing Agreement.

II. RECORD RETENTION:

Any subcontractor of WorkFirst funds shall:

a. Retain all records pertinent to the grant, grant agreements, interagency agreements, contracts, or any other award, including financial, statistical, property, applicant or participant records, and supporting documentation for a period of at least six (6) years after submittal of the final expenditure report (closeout) for that funding period to the awarding agency.

b. Retain all records of non-expendable property for a period of at least three (3) years after the final disposition of property.
c. Retain records regarding complaints and actions taken on the complaints for a period of not less than three (3) years from the date of the resolution of the complaint.
d. After the files have been retained for six (6) years, refer to your organization's guidelines for destroying confidential information.
e. Retain all records beyond the required six (6) years if any litigation or audit is begun or a claim is instituted involving the grant or agreement covered by the records. The records shall be retained for an additional three (3) years after the litigation, audit, or claim has been resolved.

In the event of the termination of the relationship between the Board and the subcontractor, the subcontractor will be responsible for the maintenance and retention of their own records. Copies of records made by microfilming, photocopying, or similar methods may be substituted for the original records if they are preserved with integrity and are admissible as evidence. All records retained beyond the mandatory retention period are subject to audit and/or review.

When stored as physical paper documents, DSHS data will be physically segregated from non-DSHS data in a drawer, folder, or another container.

When it is not feasible or practical to segregate DSHS data from non-DSHS data, then both the DSHS data and the non-DSHS data with which it is comingled must be protected as described in Attachment 2: Data Sharing Agreement.

III. STORAGE:

Any paper records must be protected by storing the records in a secured area that is only accessible to authorized personnel. When not in use, such records must be stored in a locked container, such as a file cabinet, locking drawer, or safe, to which only authorized persons to have access.

Physically secure the paper records in the storage area by:

a. Keeping them in locked storage when not in use,
b. Using check-in/check-out procedures when they are shared, and
c. Taking frequent inventories.

IV. TRANSPORTING:

When being transported outside of a secure area, confidential information must be under the physical control of Contractor staff with authorization to access the data and in a locking portable file case.

V. NOTIFICATION OF COMPROMISE:

The compromise or potential compromise of DSHS shared data must be reported to the Board within one (1) business day of discovery. The Contractor must also take action to mitigate the risk of loss and comply with any notification or other requirements imposed by the Board, Commerce, or the law.

VI. DISPOSAL:

To protect the privacy of participant information and reduce the risk of fraud and

identity theft, a new federal rule is requiring businesses to take appropriate measures to dispose of sensitive information.

Any business or individual who uses a consumer report or confidential information for a business purpose is subject to the requirements of the Disposal Rule. The Rule requires the proper disposal of confidential information and records to protect against "unauthorized access to or use of the information". The Federal Trade Commission (FTC), the nation's consumer protection agency, enforces the Disposal Rule.

According to the FTC, the standard for the proper disposal of confidential information is flexible and allows the organizations and individuals covered by the Rule to determine what measures are reasonable based on the sensitivity of the information, the costs and benefits of different disposal methods, and changes in technology.

The Disposal Rule applies to people and both large and small organizations that use consumer reports. Among those who must comply with the Rule are:

- Consumer reporting companies
- Lenders
- Insurers
- Employers
- Landlords
- Government agencies
- Mortgage brokers
- Automobile dealers
- Attorneys or private investigators
- Debt collectors

- Individuals who obtain a credit report on prospective nannies, contractors, or tenants
- Entities that maintain information in consumer reports as part of their role as service providers to other organizations covered by the Rule

The Disposal Rule requires disposal practices that are reasonable and appropriate to prevent unauthorized access to – or use of – confidential information.

WorkFirst Contractors are required to establish and comply with policies for disposing of confidential information which could include:

- Burn, pulverize, or shred papers containing participant information so that the information cannot be read or reconstructed;
- Destroy or erase electronic files or media containing participant information so that the information cannot be read or reconstructed;
- Conduct due diligence and hire a document destruction contractor to dispose of the material. Due diligence could include:
    - Reviewing an independent audit of a disposal company's operations and/or its compliance with the FTC's Disposal Rule;
    - Obtaining information about the disposal company from several references;
    - Requiring that the disposal company be certified by a recognized trade association;
    - Reviewing and evaluating the disposal company's information security policies or procedures.

Data stored on:	Will be destroyed by:
Server or workstation hard disks, or Removable media (e.g., USB flash drives, portable hard disks) excluding optical discs	Using a "wipe" utility which will overwrite the Data at least three (3) times using either random or single character data, or Degaussing sufficiently to ensure that the Data cannot be reconstructed, or Physically destroying the disk
Paper documents with sensitive or Confidential Information	Recycling through a contracted firm provided the contract with the recycler assures that the confidentiality of Data will be protected.
Paper documents containing Confidential Information requiring special handling (e.g., protected health information)	On-site shredding, pulverizing, or incineration
Optical discs (e.g., CDs or DVDs)	Incineration, shredding, or completely defacing the readable surface with a coarse abrasive
Magnetic tape	Degaussing, incinerating, or crosscut shredding

Attachments:

1. Data Security Requirements
2. Data Sharing Agreement