

Disaster Recovery Policy

Purpose:

This policy provides a plan to protect all WIOA and other electronic information.

Policy Pertains to:

- NWPA Job Connect Board Staff
- Title I Provider
- One Stop Operator
- Fiscal Agent

Provider's Responsibilities:

Providers must ensure there is a documented process and procedures in place to restore critical systems, data, and operations following a disruptive event such as a natural disaster, cyberattack, or system failure.

Definitions:

Disaster Recovery Plan (DRP)- A documented process and set of procedures to enable NWPA Job Connect to restore critical systems, data, and operations following a disruptive incident such as natural disaster, cyberattack, or system failure.

Backup- The process of creating copies of data and storing them securely to be restored in the event of data loss, corruption, or system failure.

Cloud Storage- A service provided by third-party vendors, such as Advent, for storing data offsite on remote servers accessible via the internet for long-term security.

Catastrophic Event- An unforeseen and severe incident (e.g., fire, flood, cyberattack, hardware failure, or other disaster) that significantly disrupts the ability to operate normally.

Secure Server- A dedicated computer system hosted by the organization or its IT vendor that stores organizational data in a controlled environment with access restricted by password or passcode.

Subcontractor Disaster Recovery Plan- A documented plan maintained by each subcontractor working with NWPA Job Connect that outlines their strategies for safeguarding and recovering data and systems if disrupted.

Vendor- An external provider of technology, software, or services that support payroll, accounting, IT, or cloud services necessary for recovery.

Policy:

The entities listed below have the following processes in place:

NWPA Job Connect:

- Cloud service technology is utilized.
- Datto SaaS Protection backs up the following daily (SOC2 Type II Audited and General Data Protection Regulation (GDPR) compliant):
 - Sharepoint (shared files)
 - One Drive (local files)
 - Email
 - Microsoft Teams
- Contracted IT support provider
- Laptops and phones are secure and accessed by passcode.
- Third party software is purchased through industry recognized vendors.

Fiscal Agent:

- **Payroll:**
 - NWPA Job Connect utilizes a payroll company who ensures security and backing up of files.
- **Accounting:**
 - All files are backed up to a secure server.

Title I Provider:

- Contracted IT support provider
- Laptops and phones are secure and accessed by passcode.
- Third party software is purchased through industry recognized vendors.

One Stop Operator:

- Public Access Computers located in the PA CareerLink® centers are secured using third party software purchased through industry recognized vendors.
- All public access computers are reset nightly.

Note: NWPA Job Connect expects all subgrantees to have a disaster recovery plan.

REFERENCES:

20 CFR Part 683- Administrative provisions under WIOA

2 FCR Part 200- Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards- includes requirements for record retention, internal controls, and data safeguards.

29 CFR Part 38- WIOA Nondiscrimination and Equal Opportunity Regulations (protection of personally identifiable information).

HISTORY

Name	Date	Rev. Level	Description of change	Effective Date
Deb O'Neil	08/03/2021	A	New Policy	09/10/2021

Susan Richmond	02/10/2026	B	Update and reformat	07/10/2026
----------------	------------	---	---------------------	------------