



ROCHESTERWORKS'
COMPREHENSIVE POLICY
FRAMEWORK FOR DATA
SECURITY

RochesterWorks' Comprehensive Policy Framework for Data Security is a document that outlines the policies and procedures that RochesterWorks, a workforce development organization based in Rochester New York, has put in place to protect sensitive data from unauthorized access, use, or disclosure. This comprehensive framework is designed to meet compliance with the New York Shield Act, which requires all businesses operating in the state to implement reasonable data security measures to protect personal information. Additionally, as a state agency, RochesterWorks must also comply with data security regulations set forth by the New York State Department of Labor.

The document not only applies to RochesterWorks' employees but also extends to contractors and third-party vendors who may have access to the organization's sensitive data. The policy framework requires these parties to adhere to the same data security measures as RochesterWorks' employees to ensure the safety and confidentiality of personal information.

The document covers various aspects of data security, including access controls, data classification, data retention and disposal, incident response, and training and awareness. The policy framework provides detailed guidance on how to safeguard personal information, such as social security numbers, driver's license numbers, and financial account information, from theft, loss, or misuse.

In addition to describing the policies and procedures, the document also outlines the roles and responsibilities of different stakeholders within the organization, such as the Executive Director, the Director of Technology, the Technical Assistance and Training Manager, and the Director of Finance & Administration, and the employees who handle personal information. It also specifies the consequences of violating the data security policies and the process for reporting security incidents and breaches.

Overall, RochesterWorks' Comprehensive Policy Framework for Data Security is a comprehensive and essential resource for all employees, contractors, and third-party vendors who handle personal information at RochesterWorks. It provides a clear and concise set of guidelines for protecting personal information and ensuring compliance with the New York Shield Act and the regulations set forth by the New York State Department of Labor.

Table of Contents

Data Retention and Destruction Policy.....	4
Purpose:	4
Scope:.....	4
Retention:	4
Destruction:	4
Responsibility:	4
Communication:.....	5
Employee Training:	5
Subrecipient Training:	6
Document Classification Policy	7
Purpose:	7
Scope:.....	7
General Classification:	7
Confidential Classification:	7
Responsibilities:.....	7
Enforcement:.....	7
Document Classification:	8
General Classification	8
Confidential Classification	8
Personally Identifiable Information (PII) and Protected Personal Security Information (PPSI) Incident Reporting Policy	9
Introduction:	9
Scope.....	9
Definitions.....	9
Reporting Requirements.....	9
What is an example of a reportable PII/PPSI Incident?	10
Incident Response Procedure	11
Policy Review and Updates	12
Employee Training and Awareness.....	12
Monitoring and Auditing.....	12
Record Retention and Disposal.....	12
Cooperation with Regulatory Authorities.....	13

Third-Party Vendor Management.....	13
Non-Compliance and Corrective Actions.....	13
Roles and Responsibilities.....	13
Escalation Procedures.....	14
Legal and Regulatory Compliance.....	14
Policy for Third-Party Service Providers for Data Protection.....	15
Purpose:.....	15
Overview:.....	15
Scope:.....	15
Requirements:.....	15
Vendor Management Questionnaire:.....	15
Risk Assessment Survey:.....	15
Online PII Training:.....	15
Compliance with Data Protection Laws and Regulations:.....	15
Incident Response and Breach Notification:.....	16
Security Controls:.....	16
Data Retention and Disposal:.....	16

Data Retention and Destruction Policy

Purpose:

The purpose of this policy is to establish guidelines for the retention and destruction of data collected and processed by RochesterWorks in accordance with state and federal regulations, including the New York State Stop Hacks and Improve Electronic Data Security Act (SHIELD Act).

Scope:

This policy applies to all data collected and processed by RochesterWorks, including public personally identifiable information (PII), sensitive PII, and employee information. This policy also applies to any subrecipient agreements and contracts with third-party service providers that handle data on behalf of RochesterWorks.

Retention:

RochesterWorks will retain data only for as long as necessary to accomplish the purposes for which it was collected and processed and in accordance with applicable state and federal regulations. The retention periods for each type of data are as follows:

The retention periods for certain types of data may vary depending on the applicable state and federal laws and regulations. Under New York State law, employment contracts should be retained for a minimum of six years, while under federal law, legal contracts should be retained for a minimum of three years.

The retention period for federal grants is three years after submission of the final expenditure report. The retention period for state grants is six years after the most recent renewal of the master contract. Retention periods for local or other grants must be followed.

Destruction:

RochesterWorks will securely destroy data at the end of its retention period. Paper data will be sent to a secure shredding operation, and electronic data will be deleted from the server. It is important to ensure that all copies of the data are deleted, including backups and archives. Additionally, if the data is stored in cloud-based services or with third-party vendors, it is important to verify that the data is securely deleted from those systems as well.

Responsibility:

The Technical Assistance and Training Manager is responsible for ensuring that the data retention and destruction policy is followed. This includes providing training to employees and third-party service providers who handle data on behalf of RochesterWorks, monitoring compliance with the policy, and periodically reviewing and updating the policy as needed.

Communication:

The data retention and destruction policy will be communicated to all employees, subrecipients, and third-party service providers who handle data on behalf of RochesterWorks. The policy will be included in subrecipient agreements and contracts with third-party service providers. Employees, subrecipients, and third-party service providers will receive training on the policy and will be required to acknowledge their understanding and agreement to follow the policy. The policy will also be periodically reviewed and updated as needed to reflect changes in laws and regulations and changes in the organization's data handling practices.

Employee Training:

All employees who handle data on behalf of RochesterWorks should receive training on the data retention and destruction policy. The training should cover the following topics:

The purpose of the policy and the legal requirements for data retention and destruction.

The types of data collected and processed by RochesterWorks.

The retention periods for each type of data and the reasons for the retention periods.

The proper procedures for securely destroying paper and electronic data at the end of the retention period.

The consequences of failing to follow the policy.

After completing the training, employees should be required to acknowledge their understanding of the policy and their agreement to follow the policy.

Subrecipient Training:

Any subrecipients that handle data on behalf of RochesterWorks should also receive training on the data retention and destruction policy. The training should cover the same topics as the employee training, but may also include additional topics specific to the subrecipient's role and responsibilities.

Subrecipients should be required to acknowledge their understanding of the policy and their agreement to follow the policy as a condition of their contract with RochesterWorks.

The frequency of employee and subrecipient training should be determined by RochesterWorks based on the frequency of changes in laws and regulations and changes in the organization's data handling practices. Additionally, periodic refresher training may be necessary to reinforce the importance of the policy and to ensure that employees and subrecipients remain compliant.

Reviewed by:	Title
Lee Koslow	Technical Assistance and Training Manager
Shawn Curran	Director of Technology
Jeanine Frenz	Director of Finance & Administration

Reviewed: 4/4/2023

Document Classification Policy

Purpose:

The purpose of this policy is to establish guidelines for the classification and handling of documents containing Personally Identifiable Information (PII) at RochesterWorks.

Scope:

This policy applies to all employees, contractors, and vendors who have access to documents containing PII.

General Classification:

General documents are those that contain publicly available PII, such as a person's name or job title. These documents require a low level of protection to prevent misuse or inappropriate sharing. Employees may share General documents with individuals inside and outside of RochesterWorks as needed to fulfill their job responsibilities.

Confidential Classification:

Confidential documents are those that contain PII that is more sensitive in nature, such as social security numbers, medical or financial information. These documents require a higher level of protection than General documents. Confidential documents may only be accessed by individuals with a legitimate need to know. Confidential documents must be encrypted or stored in a locked cabinet when not in use. Employees may only share Confidential documents with individuals who have been authorized by RochesterWorks management.

Responsibilities:

It is the responsibility of all employees to classify documents containing PII according to their sensitivity level and to ensure that they are handled and stored appropriately. Employees, contractors, and vendors who handle Confidential documents must complete the RochesterWorks PII awareness training and contractors, and vendors must complete the Vendor Management Questionnaire and the PII Risk Assessment Survey. Any suspected or actual breach of confidentiality must be reported immediately to RochesterWorks and follow the PII-PPSI Incident Reporting Policy.

Enforcement:

Violation of this policy may result in disciplinary action, up to and including termination of employment or termination of contract.

Document Classification:

The chart below provides a list of common document types and their classifications based on the sensitivity of the Personally Identifiable Information (PII) they contain. It is important to note that while this chart covers many types of documents, there may be other documents that require classification based on the sensitivity of the PII they contain. It is the responsibility of all employees to properly classify documents containing PII according to their sensitivity level, and to ensure that they are handled and stored appropriately to protect the privacy and security of our customers and employees.

General Classification	Confidential Classification
<ul style="list-style-type: none"> • Action plans that do not include PII or any personal information. • Workshop or class curriculums • Attendance sheets that do not include PII • Flyers and information sheets • Budget documents that do not contain staff names. • Job descriptions that do not include PII • Reports and planning documents that do not include PII • Program descriptions • Policy and procedure documents • Meeting agendas and minutes 	<ul style="list-style-type: none"> • MCDHS program participant records • MCDHS worksite records • WIOA Youth (and other NYSDOL youth grant) participant files • SYEP program records • ITA files • OJT files • Other Adult and Dislocated Worker participant files • Other employer records • Board member records • Personnel records • Payroll and benefits records • Procurement files • Contract documents • Invoices and supporting documentation. • Audit and monitoring records. • Grievance and complaint records • IT/Computer security records

Reviewed by:	Title
Lee Koslow	Technical Assistance and Training Manager
Shawn Curran	Director of Technology
Jeanine Frenz	Director of Finance & Administration

4/5/2023

Personally Identifiable Information (PII) and Protected Personal Security Information (PPSI) Incident Reporting Policy

Introduction:

RochesterWorks is committed to protecting the privacy and security of Personally Identifiable Information (PII) and Protected Personal Security Information (PPSI) collected, processed, and stored within the organization. Personally Identifiable Information (PII) and Protected Personal Security Information (PPSI) includes any information that can be used to identify an individual such as name, address, Social Security number, date of birth, and email address. It is the responsibility of all employees, contractors, and third-party vendors to report any incidents involving the unauthorized access, disclosure, or misuse of PII. This policy provides guidance on how to report PII incidents in a timely and effective manner in compliance with the New York State Department of Labor (NYSDOL) policy.

Scope

This policy applies to all employees, contractors, and service providers of RochesterWorks who may have access to, handle, or manage PII/PPSI in any format, including but not limited to, the One Stop Operating System (OSOS) and the Re-Employment Operating System (REOS), hard copy documents, and digital media.

Definitions

PII Incident: An event that results in the unauthorized access, loss, disclosure, modification, or destruction of PII/PPSI.

Reporting Requirements

All employees, contractors, and third-party vendors must immediately report any suspected or actual PII/PPSI incidents to their supervisor or member of management, who shall in turn report such incidents to the Director of Finance & Administration, and the Director of Technology. Supervisors or members of management shall immediately report any suspected or actual PII/PPSI incidents to the Director of Finance & Administration, and the Director of Technology immediately upon discovery. Unauthorized access to PII/PPSI includes:

- Accidental disclosure of PII/PPSI
- Loss or theft of PII/PPSI
- Intentional misuse or theft of PII/PPSI
- Inappropriate sharing of PII/PPSI
- Suspected or actual data breaches

What is an example of a reportable PII/PPSI Incident?

A PII/PPSI incident can refer to any situation where Personally Identifiable Information (PII) and Protected Personal Security Information (PPSI) has been accessed, disclosed, or used without authorization. Here are some examples of PII/PPSI incidents include but are not limited to:

- Accidental disclosure: An employee accidentally emails a spreadsheet containing the names, Social Security numbers, and home addresses of RochesterWorks clients to an unintended recipient.
- Intentional misuse: A former employee who still has access to the company's systems uses PII/ PPSI to impersonate clients and obtain sensitive information.
- Unauthorized access: A cybercriminal gains access to a database containing PII/PPSI and downloads the information for use in identity theft.
- Loss or theft: A laptop containing unencrypted PII/PPSI is stolen from an employee's car.
- Inappropriate sharing: An employee shares a client's PII/PPSI with a colleague who does not need the information to perform their job duties.
- Data breach: A hacker gains access to RochesterWorks' systems and steals PII/PPSI belonging to clients.
- Unauthorized access to PII/PPSI data in OSOS or REOS

In each of these examples, PII / PPSI has been compromised in some way, putting individuals at risk for identity theft, fraud, or other harms. It is important to report these incidents as soon as possible to minimize the damage and take appropriate measures to prevent future incidents.

Incident Response Procedure

Employees, contractors, or third-party vendors involved in or witness to a PII/PPSI incident, shall report the incident immediately to their direct supervisor or members of the management team. In turn, the manager document the incident utilizing the [PII-PPSI Incident Reporting Form](#) and contact the Director of Technology. The Director of Technology in coordination with Director of Finance & Administration, Technical Assistance and Training Manager and the Executive Director, will assess the incident and determine the appropriate response, including corrective actions and compliance with the New York State Breach Notification Act.

RochesterWorks will adhere to the guidelines and action items set forth in NYSDOL Technical Advisory 18-5, as described in the given policy and action sections. This includes, but is not limited to, the following key areas:

- Accessing and sharing PII/PPSI
- Security protocols related to OSOS and REOS
- Maintaining a secure environment
- Addressing breaches of confidentiality
- Confirm the incident and assess the scope and impact.
- Isolate the affected systems or devices to prevent further damage or exposure.
- Contain the incident to prevent further unauthorized access or disclosure.
- Notify appropriate stakeholders, including your direct supervisor, Director of Finance & Administration, Executive Director and depending on the extent of the incident, legal counsel.
- Coordinate with internal and external resources to investigate the incident and remediate any vulnerabilities.
- Provide regular updates to affected individuals, management, and other stakeholders as appropriate.
- Review and update incident response procedures and policies to prevent future incidents.
- Note: A breach or suspected breach of confidentiality regarding any federal- or state-funded programs must be reported to the Career Center Director immediately. The Career Center Director must immediately complete a New York State Security Breach Reporting Form. This form shall be emailed to InfoSec.IT@labor.ny.gov and OSOS.WDTD@labor.ny.gov copying in local area Security Coordinators (currently Lkoslow@rochesterworks.org and barbara.weymouth@labor.ny.gov). All such breaches are required to be reported in compliance with the New York State Breach Notification Act. The New York State Information Security Breach and Notification Act is comprised of section 208 of the State Technology Law and section 899-aa of the General Business Law.

Policy Review and Updates

This policy will be reviewed and updated periodically to ensure compliance with applicable regulations and to address any changes in technology or business practices. All employees and service providers are expected to stay informed of the latest policy updates and to adhere to them accordingly.

Employee Training and Awareness

All employees, contractors, and service providers must complete mandatory PII/PPSI training upon joining RochesterWorks and attend annual refresher training. This training will cover the handling, storage, and sharing of PII/PPSI, as well as reporting procedures for PII incidents.

Employees must acknowledge their understanding of this policy, including the safeguards they must comply with while handling PII/PPSI and the potential consequences of noncompliance.

Monitoring and Auditing

RochesterWorks will conduct regular audits twice a year to ensure compliance with this policy and adherence to the NYSDOL policy.

The Director of Technology in coordination with the Director of Finance & Administration, the Technical Assistance and Training Manager and the Executive Director will monitor and review PII/PPSI handling practices to identify potential risks and vulnerabilities and implement necessary measures to mitigate them.

Record Retention and Disposal

PII/PPSI obtained through grants/contracts funded with federal monies will be stored securely and retained only for the period necessary to fulfill the purposes stated in the grant/contract agreement or to satisfy applicable local, state, and federal records retention requirements.

After the retention period, PII/PPSI must be thoroughly and irretrievably destroyed using appropriate methods, such as shredding for paper files and secure deletion for electronic files, in accordance with the New York State Sanitization & Disposal Policy.

Cooperation with Regulatory Authorities

RochesterWorks will cooperate with the NYSDOL and the United States Department of Labor (USDOL) during inspections, audits, and investigations related to PII/PPSI confidentiality requirements.

RochesterWorks will make records available to the NYSDOL, the USDOL, and their authorized designees for inspection, review, and copying upon reasonable notice.

Third-Party Vendor Management

RochesterWorks will ensure that all third-party vendors handling PII/PPSI on our behalf comply with this policy and the relevant NYSDOL policy.

Contracts with third-party vendors must include clauses addressing data confidentiality, security measures, and incident reporting requirements.

RochesterWorks will regularly assess and monitor third-party vendors for compliance with this policy and the NYSDOL policy.

Non-Compliance and Corrective Actions

Failure to comply with this PII reporting policy may result in disciplinary action, up to and including termination of employment or contract, as well as potential civil and criminal sanctions.

In cases of non-compliance, RochesterWorks will work with the concerned individual(s) to identify the cause, provide necessary guidance and training, and implement corrective actions to prevent future incidents.

Roles and Responsibilities

The Director of Technology in coordination with the Director of Finance & Administration, Technical Assistance and Training Manager and the Executive Director will be responsible for overseeing the implementation and enforcement of the PII reporting policy.

The Director of Finance & Administration will be responsible for coordinating employee training and ensuring compliance with this policy.

The Executive Director will provide overall guidance and support for the policy and its implementation, ensuring that the organization prioritizes data privacy and security.

All employees, contractors, and service providers are responsible for understanding and adhering to this policy and reporting any PII/PPSI incidents.

Escalation Procedures

In the event of a high-risk or large-scale PII/PPSI incident, an escalation procedure will be followed to ensure that senior management and relevant stakeholders are promptly informed and involved in the decision-making process.

The Director of Technology in coordination with Director of Finance & Administration, Technical Assistance and Training Manager and the Executive Director will assess the severity of the incident and determine if escalation is necessary, based on factors such as the number of affected individuals, the nature of the PII/PPSI involved, and the potential impact on the organization and its customers.

Legal and Regulatory Compliance

RochesterWorks will regularly monitor changes to relevant laws and regulations related to data privacy and security, ensuring that the PII reporting policy remains up-to-date and compliant.

Any changes to legal or regulatory requirements will be promptly incorporated into the policy, and employees, contractors, and service providers will be informed of these changes.

These additional components help to ensure that the PII reporting policy remains effective, adaptive, and relevant to the changing landscape of data privacy and security. The cooperation and commitment of all employees, contractors, and service providers are essential for maintaining the privacy and security of PII/PPSI and upholding the reputation and integrity of RochesterWorks.

Contact Name	Title	Email
Dave Seeley	Executive Director	dseeley@rochesterworks.org
Jeanine Frenz	Director of Finance & Administration	jfrenz@rochesterworks.org
Shawn Curran	Director of Technology	scurran@rochesterworks.org
Lee Koslow	Technical Assistance and Training Manager	lkoslow@rochesterworks.org

Reviewed by:	Title
Lee Koslow	Technical Assistance and Training Manager
Shawn Curran	Director of Technology
Jeanine Frenz	Director of Finance & Administration

4/5/2023

Policy for Third-Party Service Providers for Data Protection

Purpose:

The purpose of this policy is to outline the requirements for third-party service providers who access or process Personally Identifiable Information (PII) on behalf of RochesterWorks. This policy ensures that all third-party service providers comply with the data protection requirements and protect the confidentiality, integrity, and availability of PII.

Overview:

Data protection is critical for RochesterWorks as a provider of workforce development services. PII is collected, processed, and stored by RochesterWorks to provide services to its customers, including job seekers and employers. RochesterWorks has a legal and ethical obligation to protect PII against unauthorized access, disclosure, modification, or destruction. Failure to comply with this policy may result in termination of the contract and/or legal action.

Scope:

This policy applies to all third-party service providers who access or process PII on behalf of RochesterWorks.

Requirements:

To ensure the protection of PII, all third-party service providers must comply with the following requirements:

Vendor Management Questionnaire:

All third-party service providers must complete a vendor management questionnaire that assesses their security controls and compliance with data protection laws and regulations.

Risk Assessment Survey:

All third-party service providers must complete a risk assessment survey that evaluates their risk posture and identifies potential security vulnerabilities.

Online PII Training:

All third-party service providers must complete the RochesterWorks online PII training program that covers topics such as data protection laws and regulations, confidentiality, integrity, and availability of PII, incident response, and breach notification.

Compliance with Data Protection Laws and Regulations:

All third-party service providers must comply with data protection laws and regulations applicable to RochesterWorks and the jurisdictions in which they operate. This includes, but is not limited to the New York State Shield Act, and the New York State Department of Labor's data protection guidelines.

Incident Response and Breach Notification:

All third-party service providers must familiarize themselves with the RochesterWorks incident response plan and breach notification process and effectively respond to any security incidents or data breaches that may occur.

Security Controls:

All third-party service providers must implement reasonable security controls to protect PII against unauthorized access, disclosure, modification, or destruction. This includes, but is not limited to, access controls, encryption, and monitoring and logging of system activity.

Data Retention and Disposal:

All third-party service providers must comply with RochesterWorks' data retention and disposal policies and procedures, including the secure disposal of PII when no longer required.

By implementing this policy, RochesterWorks ensures that all third-party service providers who access or process PII on its behalf comply with data protection requirements and protect the confidentiality, integrity, and availability of PII.

Reviewed by:	Title
Lee Koslow	Technical Assistance and Training Manager
Shawn Curran	Director of Technology
Jeanine Frenz	Director of Finance & Administration

4/5/2023