Union
Workers'
Union

# Data Policy

**Last updated: 20 November 2024**

## 1. Purpose

This Internal Data Policy outlines the principles and procedures for handling, managing, and securing data within the Union Workers’ Union ("the Union"). The policy is designed to ensure that all employees, members, contractors, and affiliates understand their responsibilities regarding the protection and appropriate use of the Union’s data.

## 2. Scope

This policy applies to all employees, members, contractors, volunteers, and third-party partners who have access to the Union’s data. It covers all types of data, including but not limited to:

- *Personal Data:* Information that can identify an individual, such as names, addresses, phone numbers, and email addresses.
- *Confidential Union Data:* Sensitive information related to union activities, negotiations, member records, financial data, and strategic plans.
- *Operational Data:* Information related to the Union’s operations, including process documentation, internal communications, and employee records.
- *Digital Assets:* All digital content, including files, databases, emails, and multimedia.

## 3. Data classification

All data within the Union should be classified according to its sensitivity and confidentiality:

- *Public Data:* Information that can be freely shared without any restrictions.
- *Internal Data:* Information that should only be accessible to Union employees, members, and authorised personnel.
- *Confidential Data:* Highly sensitive information that requires strict access controls and should only be accessible to specific individuals or groups.
- *Restricted Data:* Data that is subject to the highest level of security and is only accessible to a limited number of authorised individuals.

## 4. Data access

Access to data is granted based on the principle of least privilege, meaning that individuals are only given access to the data necessary to perform their roles within the Union. Access levels are determined by:

- *Role-based access control (RBAC):* Assigning access rights based on job roles within the Union.
- *Need-to-know basis:* Ensuring that only those who need access to specific data for their work are granted it.
- *Regular reviews:* Periodically reviewing and updating access permissions to ensure compliance with this policy.

### 5. Data handling

All employees, members, and authorised personnel are required to handle data in a manner that ensures its confidentiality, integrity, and availability:

- *Data Storage:* Sensitive data must be stored in secure systems with appropriate encryption and access controls. Physical documents should be stored in locked cabinets or secure areas.
- *Data Transmission:* Confidential and restricted data should be transmitted using secure methods, such as encrypted email or secure file transfer protocols (SFTP).
- *Data Retention:* Data should be retained only as long as necessary for Union or legal purposes. Regular audits should be conducted to identify and securely dispose of data that is no longer required.
- *Data Disposal:* When data is no longer needed, it must be disposed of securely. Digital data should be permanently deleted, and physical documents should be shredded or otherwise rendered unreadable.

### 6. Data breach and incident reporting

All employees and members must immediately report any suspected or actual data breaches, security incidents, or unauthorised access to data to the designated Data Protection Officer (DPO). The Union will investigate all reported incidents and take appropriate action to mitigate any risks and prevent future occurrences.

### 7. Employee and member responsibilities

Employees and members are expected to:

- *Adhere to this policy:* Follow all guidelines and procedures outlined in this policy.
- *Protect login credentials:* Use strong passwords and multi-factor authentication where applicable. Never share login credentials with unauthorised individuals.
- *Be vigilant:* Report any suspicious activity, phishing attempts, or potential security threats to the Union immediately.
- *Participate in training:* Complete all required data protection and security training as mandated by the Union.

### 8. Data Protection Officer (DPO)

The Data Protection Officer (DPO) is responsible for overseeing the implementation and enforcement of this policy. The DPO will:

- *Monitor compliance:* Regularly review data handling practices to ensure they comply with this policy.
- *Provide guidance:* Offer advice and support to employees and members on data protection matters.
- *Respond to incidents:* Lead the investigation and resolution of any data breaches or security incidents.

### 9. Compliance and disciplinary action

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or membership. In cases of severe violations, legal action may be pursued.

### 10. Review and updates

This policy will be reviewed annually or as necessary to address changes in technology, legal requirements, or Union practices. Any updates will be communicated to all employees, members, and relevant stakeholders.

### 11. Contact information

For questions or concerns regarding this policy, please contact:

Data Protection Officer
mail@unionworkersunion.org