APP DRIVERS UNION

WRITTEN INFORMATION SECURITY PROGRAM

LAST UPDATED OCTOBER 31, 2025

I. OBJECTIVE

The objective of App Drivers Union ("Union") in the development and implementation of this comprehensive written information security program ("WISP"), is to create effective administrative, technical and physical safeguards for the protection of Personally Identifiable Information ("PII"), Payment Card Information cardholder data ("PCI"), and Protected Health Information ("PHI"). The WISP sets forth the Union's procedure for evaluating its electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting PII, PHI and PCI.

For purposes of this WISP, "PII" means an individual's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such individual:

- Social Security number;
- Driver's license number or government-issued identification number;
- Personal cellular or home phone number;
- Home address;
- Email address;
- Financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to an individual's financial account;
- Passwords, personal identification numbers, or other access codes;
- Any other numbers or information that can be used to access a person's financial resources;
- Digital signatures;
- Passport number;
- Date of birth;
- A birth or marriage certificate;
- The maiden name of the individual's mother;
- A private key that is unique to an individual and that is used to authenticate or sign an electronic record;
- An individual's taxpayer identification number or an identity protection personal identification number issued by the IRS;
- Medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional or health insurance information;
- Health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify an individual, or any information in an individual's application and claims history, including any appeals records;
- Username or email address coupled with a password or security question and answer that would permit access to an online account;
- Shared secrets or security tokens that are known to be used for data-based authentication;

It also includes the following regardless of whether it is combination with an individual's first and last name or first initial and last name:

- Username or email address coupled with a password or security question and answer that would permit access to an online account;
- Account number or credit card number or debit card number in combination with any required security code, access code, or password that would permit access to that account;
- Any of the above data elements if the information compromised would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose information was compromised.

For purposes of this WISP, "PHI" includes information that is created, received, and/or maintained by Union related to an individual's health care (or payment related to health care) that directly or indirectly identifies the individual.

"PII" or "PHI" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public, information provided by bargaining unit members for purposes of investigating a complaint/grievance and/or health information that is not governed by HIPPA.

"PCI**"**, at a minimum, includes cardholder name, primary account number, expiration date, service code and/or PIN.

II. PURPOSE

The purpose of the WISP is to better:

- Ensure the security and confidentiality of PII, PHI and PCI;
- Protect against any anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud.
- Ensure that employees receive ongoing training in order to ensure the ongoing security and confidentiality of PII, PHI and PCI.

III. SCOPE

In formulating and implementing the WISP, the Union is in the process of addressing and incorporating the following protocols:

(1) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing PII, PHI and PCI;

(2) Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the PII, PHI and PCI;

(3) Evaluate the sufficiency of existing policies, procedures, information systems, and other safeguards in place to control risks;

(4) Design an implemented and updated WISP that puts safeguards in place to minimize those risks, consistent with the requirements of the regulations; and

(5) Implement regular monitoring of the effectiveness of those safeguards.

(6) The Union has identified that the following paper, electronic or other records, computing systems and storage media contain could contain PII, PCI or PHI: dues records, employee human resource files, grievance records, employee computers, laptops and cellular phones, Union email systems and third-party vendors including Action Builder, Action Network, Waiver Forever, Scale to Win, and Microsoft Office 365.

IV. COMPLIANCE WITH 456 CMR 24.00

Any PII provided to the Union may be securely shared with the Massachusetts Department of Labor Relations ("DLR") for the purposes of the administration of M.G.L. ch. 150F and 456 CMR 24.00. The Union shall limit the disclosure of PII to the uses necessary to effectuate M.G.L. c. 150F. The Union shall promptly notify the DLR of any suspected or actual data breach.

V. DATA SECURITY COORDINATOR

Union has designated David Torre to supervise and maintain the WISP. The designated employees (the "Data Security Coordinators") will be responsible for overseeing:

a. Initial implementation of the WISP;

b. Training employees;

c. Regular testing of the WISP's safeguards;

d. Evaluating the ability of each of the Union's third-party service providers to implement and maintain appropriate security measures for the PII, PHI and PCI to which the Union has permitted them access, consistent with the regulations; and requiring such third-party service providers by contract to implement and maintain appropriate security measures;

e. Reviewing the scope of the security measures in the WISP at least yearly, or whenever there is a material change in Union operational practices that may implicate the security or integrity of records containing PII, PHI and PCI; and

f. Conducting training sessions for all managers, employees and independent contractors, including temporary and contract employees who have access to PII, PHI and PCI on the elements of the WISP. All attendees at such training sessions are required to certify their attendance at the training, and their familiarity with Union's requirements for ensuring the protection of PII, PHI and PCI.

VI. INTERNAL RISKS

To combat internal risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing PII, PHI and PCI, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are mandatory and are effective immediately:

Internal Threats

- The Union shall only collect PII, PHI and PCI of members, suppliers, vendors or employees that is necessary to accomplish Union's legitimate need to access said records, for a legitimate job-related purpose or necessary for the Union to comply with municipal, state or federal regulations.

- Access to records containing PII, PHI and PCI shall be limited to those persons who are reasonably required to know such information in order to accomplish Union's legitimate business purpose or to enable the Union to comply with state or federal regulations.

- Access to PII, PHI and PCI shall be restricted to active users and active user accounts only.

- The Union shall retain PII, PHI and PCI of members, suppliers, vendors or employees only for the time period(s) necessary to accomplish Union's legitimate need to access said records, for a legitimate job-related purpose or necessary for the Union to comply with municipal, state or federal regulations.

- Any PII, PHI and PCI stored shall be disposed of when no longer needed for business purposes or required by law for storage. Paper or electronic records (including records stored on hard drives or other electronic media) containing PII, PHI and PCI shall be disposed of only in a manner that complies with the regulations and as follows:

    - Paper documents containing PII, PHI and PCI shall be either redacted, burned, pulverized or shredded upon disposal so that PII, PHI and PCI cannot be practicably read or reconstructed; and

    - Electronic media and other non-paper media containing PII, PHI and PCI shall be destroyed or erased upon disposal so that PII, PHI and PCI cannot be practicably read or reconstructed.

Procedures for Terminated Employees (whether voluntary or involuntary)

- Terminated employees must return all records containing PII, PHI and PCI, in any form, that may at the time of such termination be in the former employee's possession (including all such information stored on laptops or other portable devices or media, and in files, records, email, work papers, etc.)

- A terminated employee's physical and electronic access to PII, PHI and PCI must be immediately blocked. Such terminated employee shall be required to surrender all keys, IDs or access codes or badges, business cards, and the like, that permit access to the Union's staff-only areas or information. Moreover, such terminated employee's remote electronic access to personal information must be disabled; their voicemail access, e-mail access, Internet access, and passwords must be invalidated.

Physical Assets Protocol

- All assets must be secured from theft by locking up and maintaining a secure workplace, whether that work takes place in Union's offices, client site, a car, hotel or a home.

- All laptops must be placed in the trunk of vehicle when and wherever they are parked. If no secure trunk or other storage is available, employees must keep their laptops in their possession.

- Laptops, PDAs, and other portable devices left in the office or at home over night should be kept in a locked and secure location.

- Employees must have assets secured or within their physical possession while on public or private transportation, including air travel.

- Any document that contains any PII, PCI or PHI must be secured in the trunk of a vehicle when and wherever they are parked. If no secure trunk or other storage is available, employees must keep such documents in their possession.

- Documents with PII, PHI or PCI left in the office or at home over night should be kept in a locked and secure location.

Access Control Protocol

- Access to electronically stored PII, PHI and PCI shall be electronically limited to those Union employees having a unique login ID.

- Employees must ensure that all computer systems under their control are locked when leaving their respective workspaces. Employees must not disable any logon access.

- Employees must log off of VPN when they are not directly using those resources.

- All computers that have been inactive for 15 or more minutes shall require re-log-in.

- All encrypted laptops require a password
- After 5 unsuccessful log-in attempts by any user ID, that user ID will be blocked from accessing any computer or file stored on any computer until access privileges are reestablished by the Data Security Coordinator.

- After multiple unsuccessful log-in attempts an email is sent to our IT consultants

- Employees must maintain the confidentiality of passwords and access controls:
    - All passwords used for Union systems and laptops are required to adhere to strong password rules.
    - All passwords used for Union systems and laptops are required to be changed every 6 months.
    - Passwords are required to be a minimum of 12 characters long
    - Password cannot repeat themselves with 12 months.
    - Employees must not share accounts or passwords with anyone.
    - Employees must not record passwords on paper or in a document.

Vendor and Visitor Protocols

- The Union will investigate vendors to ensure that they have implemented and maintained commercially reasonable security protocols and practices.

- The Union will require in all vendor contracts that they implement maintain commercially reasonable security protocols and practices that are consistent with Massachusetts Office of Consumer Affairs and Business Regulation 201 CMR 17.00.

- Where practical, all visitors are restricted from areas where files containing PII, PHI and PCI are stored. Alternatively, visitors must be escorted or accompanied by an approved employee in any area where files containing PII, PHI and PCI are stored.

- Where practical, all visitors are restricted from areas where files containing PII, PHI and PCI are stored. Alternatively, visitors must be escorted or accompanied by an approved employee in any area where files containing PII, PHI and PCI are stored.

VII. EXTERNAL RISKS

To combat external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing PII, PHI and PCI, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are mandatory and are effective immediately:

External Threats

- Firewall protection, operating system security patches, and all software products shall be reasonably up-to-date and installed on any computer that stores or processes PII, PHI and PCI.

- All system security software including, anti-virus, anti-malware, and internet security shall be reasonably up-to-date and installed on any Union issued computer that stores or processes PII, PHI and PCI.

- To the extent technically feasible, all PII, PHI and PCI stored on Union issued laptops or other portable Union devices shall be encrypted and records and files transmitted across public networks or wirelessly, to the extent technically feasible, will be transmitted through a VPN connection.

- To the extent technically feasible, Employees must not email any client information or documents containing PII, PHI and PCI without encryption.

- Multi-factor authentication must be enabled for any application or system that supports it. This includes but is not limited to our VPN, webmail and 3rd party applications.

- Internal computer systems and network traffic is constantly monitored by 3rd party managed detection and response (MDR) vendor to alert of suspicious activity on the network.

- There shall be secure user authentication protocols in place that:

    - Control user ID and other identifiers;

    - Assigns passwords in a manner that conforms to accepted security standards, or applies use of unique identifier technologies;

    - Control passwords to ensure that password information is secure.

- PII, PHI and PCI shall not be removed from the business premises in electronic or written form absent a legitimate business need and use of reasonable security measures, as described in this WISP.

- Any PII, PHI, or PCI collected in written form in the field shall either be kept on the person collecting the information, with reasonable precautions taken to avoid exposure, or should be locked in the trunk of a vehicle.

- To the extent technically feasible, systems shall be monitored for unauthorized use or access to PII, PHI and PCI.

VIII. PROCEDURES FOR MONITORING EMPLOYEE COMPLIANCE

- A copy of this WISP must be distributed to each current Union employee or contract employee with access to PII, PHI and PCI and to each new Union employee with access to PII, PHI and PCI at the commencement of their employment. It shall be the employee's responsibility for acknowledging in writing, by signing the attached Acknowledgment, that they have received a copy of this WISP and will abide by its provisions.

- All Union employees shall participate in the Union's training programs on the WISP and data security. Each such Union employee shall sign and acknowledge his/her completion of the training program and agreement to abide by the WISP. Immediate retraining of Union employees shall occur annually and/or when the Data Security Coordinators determines it is appropriate.

- Union employees are required to report suspicious or unauthorized use of PII, PHI and PCI to our IT consultants immediately.

- An employee's failure to adhere to this and other security policies of Union may result in disciplinary action and, in case of preventable loss or theft, employees may be held responsible for replacement in accordance with the employee handbook and/or relevant collective bargaining agreement.

- All persons who fail to comply with this WISP may be subject to disciplinary measures, up to and including termination, irrespective of whether PII, PHI and PCI was actually accessed or used without authorization.

- In the event of an actual or suspected breach of security, the procedure set forth in Appendix A shall be followed.

- If there is an incident that requires notification under any state breach notification statute or regulation, there shall be a mandatory post-incident review of events and action taken, if any, with a view to determining whether any changes in the Union's security practices are required to improve the security of PII, PHI and PCI for which the Union is responsible.

- All security measures shall be reviewed at least every year, or whenever there is a material change in Union's operations that may reasonably implicate the security or integrity of records containing PII, PHI and PCI. The Data Security Coordinators shall be responsible for this review and shall fully apprise David Torre and, if appropriate, Officers of the Union, of the results of that review and any recommendations for improved security arising out of that review.

IX. CONTACT IN CASE OF LOSS/THEFT OR SUSPECTED LOSS/THEFT

If you have reason to believe that any PII, PHI and PCI has been lost or stolen or *may* have been compromised or there is the potential for identity theft, regardless of the media

or method, report the incident immediately by contacting David Torre during normal and after working hours to report the incident.

APPENDIX A: Step-By-Step Incident Handling Procedures

Detection:

1. Staff notifies the IT helpdesk.
2. The IT Consultants evaluate the risk level of the incident.
   a. The IT consultants escalates any High or Medium-Risk incidents to the Executive Director.
   b. The IT consultants continues through the Incident Response Document to assist in handling any Low-Risk incidents.
3. Begin the documentation process.
4. Notify the Massachusetts Department of Labor Relations of the suspected or actual data breach.

Containment:

1. Take necessary steps to prevent incident from spreading.
2. Document containment steps.
3. The Executive Director determines whether to report insurance claim
5. The Executive Director determines whether to involve Officers and/or inform staff or bargaining unit members.

Remediation:

1. Determine incident cause based on information gathered during the detection phase.
2. Determine how attack was executed.
3. Remove threat.
4. Perform a vulnerability assessment and remediate vulnerabilities.
5. Return systems to trusted state and/or ensure that staff has offsite access to relevant systems/hardware/processes and communicate to staff how to access such systems.

Resolution:

1. Compare system against original baseline gathered during preparation phase.
2. Business units test the service/system to verify functionality.
3. Restore system to production environment.
4. Perform ongoing system monitoring to ensure system integrity and detect incident recurrence.

Closure:

1. Finalize incident handling documentation.
2. Review incident with Executive Director and/or Officers.
3. Attach documentation and incident description IT tracking system and provide copy to legal counsel.