The Commonwealth of Massachusetts

DEPARTMENT OF PUBLIC UTILITIES
TRANSPORTATION NETWORK COMPANY DIVISION
One South Station, 5th Floor ▪ Boston, MA 02110

PERMIT APPLICATION FORM
TRANSPORTATION NETWORK COMPANIES

G.L. c. 159A½; St. 2016, c. 187; 220 CMR 274
Order Adopting Final TNC Regulations, D.P.U. 17-81-A (Sept. 7, 2017)

https://www.mass.gov/orgs/tnc-division

Table of Contents

Article I. INTRODUCTION

The Commonwealth of Massachusetts regulates Transportation Network Companies (TNCs) — also known as rideshare companies — through the Department of Public Utilities, Transportation Network Company Division (Division). To operate as a TNC in Massachusetts, a Permit Application must be completed with the Division every year. G.L. c. 159A½, § 3. This Permit Application is intended to inform the Applicant of the requirements of operating as a TNC in Massachusetts. There is no filing fee for the Permit Application, although by statute the Applicant will have other payment obligations that are described in this document.

Throughout this form, the Applicant is required to enter and affirm certain information, as well as submit additional information as part of the Permit Application. **Such additional information submitted to the Division must be in color copy, PDF format, and paginated with a table of contents**. The Division may request other information as deemed necessary. G.L. c. 159A½, § 8(a).

Failure to comply with the requirements of this Permit Application may result in the denial of a Permit, at which point the Applicant must wait six months before filing a revised Permit Application.

The Division assesses each Permit Application to determine whether it is consistent with the rules and regulations for operating as a TNC and is in accordance with the public interest. The Division welcomes all Applicants and will work closely with each throughout the Permit Application process. Before completing the Permit Application, the Division recommends that the Applicant make itself available for a meeting to discuss the requirements listed herein.

All capitalized terms not specifically defined herein shall have the meaning ascribed to such terms in 220 CMR 274.02.

Article II. CHECKLIST OF ADDITIONAL REQUIRED INFORMATION

For ease of reference, the following information is identified as an additional required submission, which is outlined further throughout this Permit Application.

- ☐ Map of the Applicant's service location(s), identifying geographic locations for each contracted Transportation Network Service (if applicable)
- ☐ Proposed Certificate of Insurance
- ☐ Screenshots of insurance disclosures to Drivers
- ☐ Plan for ensuring Transportation Network Vehicles are validly inspected, registered, and insured
- ☐ Proposed Transportation Network Vehicle decal or trade dress
- ☐ Plan for ensuring compliance with the Driver Background Check requirements
- ☐ Proposed plan for obtaining a Driver's consent & authorization for the Division background check
- ☐ Proposed Transportation Network Driver Certificate
- ☐ Screenshots for complaint reporting by phone, email, and webpage
- ☐ Copy of the Applicant's price structure for Rides, including whether that structure differs based on geographic location
- ☐ Screenshots/photographs of the Applicant's sample waybill that for both Riders and Drivers
- ☐ Proposed Rider accessibility policy
- ☐ Proposed hours of service policy

Article III. BUSINESS INFORMATION

Section 3.01 Type of Business

Select all that apply:

- ☐ Corporation
- ☐ Limited Liability Company
- ☐ General Partnership
- ☐ Limited Partnership
- ☐ Limited Liability Partnership
- ☐ Sole Proprietorship
- ☐ Doing Business As
- ☐ Other (specify)

Section 3.02 Contact Information

- Name
- Address
- City/Town
- State
- Zip Code
- Phone
- E-mail

Section 3.03 Business Affiliation

- Identify all entities operating in Massachusetts that are subsidiaries of the Applicant
  - Describe the nature of the relationship(s)

- Identify all entities of which the Applicant is a subsidiary
  - Describe the nature of the relationship(s)
  - Describe the nature of the relationship(s) between the Applicant and other subsidiaries

Section 3.04 Executive & Regional Personnel

- List all corporate officers and titles

- List all primary personnel responsible for Massachusetts business activities[1]

Article IV. TYPES OF SERVICES & LOCATIONS

Section 4.01 Service Description

Identify the types of Transportation Network Services to be provided by the Applicant. Select all the apply.

- ☐ Door-to-Door (pick-ups and drop-offs are at specific addresses)
- ☐ Curb-to-Curb (drivers assist passengers between the vehicle and sidewalk or other waiting area)
- ☐ Walk-to (riders walk a short distance to or from either a pick-up or drop-off location)
- ☐ Non-Emergency Medical Transportation
- ☐ Pupil Transportation
- ☐ Other [specify]

If other, please specify.

[1] For example, the Applicant may have personnel responsible for matters at the Division, the Massachusetts Department of Transportation, the Massachusetts Executive Office of Public Safety and Security, the Massachusetts Port Authority, City of Boston, etc.

Identify types of Transportation Network Vehicles (sedan, SUV, etc.):

-

Identify largest and smallest Transportation Network Vehicle:

-

Specify approximate number of Transportation Network Vehicles per year:

-

Specify approximate number of Drivers per year:

-

Specify approximate number of Rides per year:

-

Specify approximate number of Riders per year:

-

Section 4.02 Contracted Services

- List all entities with which the Applicant has contracted to provide Transportation Network Services in Massachusetts[2]
- Specify term of contract(s)
- Explain purpose of the contractual relationship(s):

The Division may require the Applicant to furnish contract information related to any contracted Transportation Network Services. The Division may inspect the contract provisions to ensure compliance with TNC rules and regulations. G.L. c. 159A½, § 8(a).

[2] For example, the Applicant may have contracted to provide Transportation Network Services on behalf of a municipality, regional transit authority, state agency, health care or educational institution, etc.

If the Applicant does not contract to provide any Transportation Network Services in Massachusetts, please affirm by checking the box below.

☐ **Applicant affirms no Transportation Network Services are provided in Massachusetts through contract.**

Section 4.03 Location of Services

Provide a map of the Applicant's location(s) of service(s).

If the Applicant is providing Transportation Network Services through contract, identify in the map the geographic locations for each contracted service.

Article V. INSURANCE

Section 5.01 Required Insurance Coverage

At the time of operation, the Applicant is required to have an insurance policy that is compliant with the requirements of G.L. c. 159A½, § 5, identified below. The Applicant is not required to have entered into a contract for the requisite insurance until it has been permitted by the Division.

(a) General Provisions

- Insurance policy contains no language that precludes coverage from being conditioned on a driver's carrier denying a claim (G.L. c. 175, §228(f)); and
- Insurance policy provides the required coverage on a first dollar basis where insurance maintained by the Driver has lapsed, failed to provide the required coverage, denied a claim for the required coverage or otherwise ceased to exist. G.L. c. 175, §228©.

(b) Phase 1 Requirements

When a Driver is logged onto the Digital Network and is available to receive a Ride, but is not yet engaged in a Ride, insurance policy requirements must provide for:

- Bodily injury coverage limit for automobile liability of at least $50,000 per individual, per vehicle (G.L. c. 175, §228(c));
- Bodily injury coverage limit for automobile liability of at least $100,000 of total coverage (G.L. c. 175, § 228(c));
- Property damage coverage limit for automobile liability of at least $30,000 (G.L. c. 175, §228(c));
- Uninsured motorist coverage of at least $20,000 per person, $40,000 per accident (G.L. c. 175, §§ 113L and 228(c); and
- Personal injury protection coverage of at least $8,000 for any one person. G.L. c. 90, §34A and G.L. c. 175, §228(c).

(c) Phase 2 & Phase 3 Requirements

When a Driver is transporting a Rider or has accepted a Ride request and is on the way to pick-up the Rider, insurance policy requirements must provide for:

- Death, bodily injury and property damage coverage limit for automobile liability of at least $1,000,000 per occurrence, per vehicle (G.L. c. 175, §228(d));
- Uninsured motorist coverage of at least $20,000 per person, $40,000 per accident (G.L. c. 175, §§ 113L and c. 228(d)); and
- Personal injury protection coverage of at least $8,000 for any one person. G.L. c. 90, §34A and G.L. c. 175, §228(d).

The Applicant must submit its proposed Certificate of Insurance to the Division, which demonstrates compliance with these requirements.

The Division may coordinate with the Massachusetts Division of Insurance to ensure the Applicant's compliance with these requirements.

Section 5.02 Required Insurance Disclosure to Drivers

Before a Driver provides Transportation Network Services, the Applicant is required to conspicuously disclose the following to each Driver:

(a) A statement that the Driver's own automobile insurance policy may not provide coverage during the provision of Services;

(b) A statement of the automobile insurance coverage that the TNC provides, including the types of coverage and the limits for each coverage, in each circumstance:

(1) A Driver logged onto the Digital Network and available to receive transportation requests, but not engaged in a Pre-arranged Ride;

(2) A Driver engaged in a Pre-arranged Ride; and

(3) A Driver not logged onto the Digital Network nor engaged in a Pre-arranged Ride; and

(c) Within seven business days of receiving a Driver Certificate, the Driver shall disclose to the automobile insurance carrier, whose coverage applies to the Vehicle(s) used by the Driver to provide Services, that the Vehicle is used to provide Services.

The Applicant is required to submit screenshots demonstrating how the insurance disclosures are conspicuously communicated to the Driver.[3]

[3] One form of acceptable compliance is surfacing of the disclosure to the Driver (and acknowledgment of receipt by the Driver) after the Driver has signed the Division background check consent and authorization form.

Article VI. VEHICLE REQUIREMENTS

Section 6.01 Inspection, Registration, & Insurance

All Transportation Network Vehicles (Vehicles) must maintain compliance with Massachusetts insurance requirements. Massachusetts-registered Vehicles must maintain compliance with the vehicle registration and inspection requirements of Massachusetts. Out-of-state registered Vehicles must maintain compliance with the vehicle registration and inspection requirements of the state in which the Vehicle is registered.

Additionally, each Vehicle is required to have a secondary Massachusetts inspection, regardless of whether the vehicle is registered out-of-state. Drivers must obtain the secondary Massachusetts Vehicle inspection at their next annual emissions testing or within 12 months of obtaining an initial approval (positive suitability determination) by the Division. The Driver must keep this secondary Vehicle inspection certificate with them at all times while providing Transportation Network Services and is required to produce it to law enforcement upon request.

A list of frequently asked questions from the Massachusetts Department of Transportation regarding the secondary Vehicle inspection is located at ***Appendix 1***.

Rules and regulations regarding the Vehicle registration and inspection requirements may be found at:

- St. 2016, c. 187, § 3
- G.L. c. 159A½, § 4(b)(ii)
- 220 CMR 274.04; 220 CMR 274.08
- 540 CMR 30

The Applicant is responsible for ensuring that a Vehicle cannot provide a Ride without proof of compliance with these requirements. The Applicant must submit a proposed plan to ensure compliance. The plan must include a narrative that:

1. **Describes in detail the processes that it will rely on to ensure that each Vehicle is validly registered, inspected, and insured;**

2. **Describes the documents that are proof of valid (a) state registration, (b) state inspection, (c) motor vehicle insurance, and (d) secondary Massachusetts Vehicle inspection; and**

3. **Identifies any third parties with which the Company contracts or intends to contract to administer compliance with 220 CMR 274.04(1)(c) and specifies the nature of their roles and responsibilities.**

Section 6.02 Trade Dress/Removable Decal

The Applicant is required to issue its Drivers a removable decal or trade dress, which the Drivers must apply to the front and rear of their vehicles. The removable decal or trade dress must be reflective, illuminative or otherwise visible at night or in low-light environments. 220 CMR 274.08(1). A permanent paper trade dress/removable is not acceptable.

The purpose of the trade dress/removable decal is to (1) provide an added means of vehicle identify verification to riders and (2) notice to law enforcement and others on the road that a particular motor vehicle is engaged in Transportation Network Services. *Order Adopting Final TNC Regulations*, D.P.U. 17-81-A at 59 (Sept. 7, 2017).

The Applicant must submit a copy of its proposed removable decal or trade dress for approval by the Division.

Section 6.03 Commercial Tolls

The Applicant is required to ensure that its Drivers pay commercial rates on a toll road, bridge, or tunnel. G.L. c. 159A½, § 2(j).

The Applicant is required to submit its Ride data to the Massachusetts Department of Transportation. That the agency will cross-reference its toll data with the Ride data submitted by the Applicant in order to ensure payment of commercial tolls by Drivers are accurate.

To ensure compliance, the Applicant may either enter into a Memorandum of Understanding with the Massachusetts Department of Transportation or require its Drivers obtain a commercial toll transponders. In either scenario, the Massachusetts Department of Transportation will upcharge the toll rate on the Driver's account to the commercial toll rate (noted on statement as "rideshare commercial upcharge").

Further details on the Applicant's obligations with respect to commercial tolls may be found on the EZDriveMA website (https://www.ezdrivema.com/rideshare), which is also found at ***Appendix 2***.

The Division will consult with the Massachusetts Department of Transportation to determine the most appropriate method of ensuring commercial toll payments.

Article VII. BACKGROUND CHECK REQUIREMENTS

Section 7.01 Overview: Two-Part Background Check

All Drivers must be in compliance with the Division's suitability standard, which is found at 220 CMR 274.21 (Suitability Standard) as well as G.L. c. 159A½, § 4. The suitability standard contains criminal offenses, driving violations, and other conditions.

Each Driver must undergo a two-part background check. 220 CMR 274.06. The Applicant must conduct the first check, which is a nationwide background check. The Applicant must conduct this check on each Driver once every six months.

After the initial and successful background check, the Applicant must electronically submit the Driver's personal information to the Division for a state-run background check. The Division will notify the Applicant of whether the Driver is approved, denied, or suspended.

Section 7.02 TNC Background Check

The Applicant must have a background check provider accredited by the Professional Background Screening Association (https://thepbsa.org/accreditation/).

At a minimum, the Applicant's background check must include the following:

(1) Multi-state criminal history database;
(2) Multi-state motor vehicle driving history database; and
(3) U.S. Department of Justice National Sex Offender public website search.

The Applicant must submit a proposed plan for compliance with this requirement. At a minimum, this narrative must explain in detail:

1. **How the Applicant plans to ensure compliance with the Driver Background Check requirements of 220 CMR 274.06(2)(a), including identifying any third-party contractors the Applicant plans to use and the nature of their roles and responsibilities; and**

2. **The types of checks (e.g., Federal Criminal Checks, National Criminal Database Checks, County Criminal Checks, etc.) that the Company's background-check provider(s) will report to the Company in connection to 220 CMR 274.06(2)(a).**

To ascertain compliance with rules and regulations, the Division may inspect the Applicant's contract with its background check provider(s) upon request. G.L. c. 159A½, § 8(a); 220 CMR 274.17. The Division will determine whether the quality of the background check is consistent with public safety. G.L. c. 159A½, § 2(a).

Section 7.03 Driver Background Check Consent & Authorization

In order for the Division to conduct a background check, the Massachusetts Department of Criminal Justice Information Services requires the Applicant to conduct the following process:

(1) Obtain consent and authorization from the Driver for the Division to conduct a background check;
(2) Prepare to submit the Driver's personally identifying information to the Division (specified in Section 7.04); and
(3) Verify the Driver's identity by
    (a) Comparing the Driver's personally identifying information with their driver's license; and
    (b) Comparing the driver's license with an up-to-date facial image of the Driver.

Each year, the Applicant is required to ensure that the Driver re-consents to the Division background check and affirms that the Driver's personally identifying information that was submitted to the Division is current and accurate. If any information is different at all, the Applicant is required to submit a new application for the Driver to the Division. In particular, if the Driver's name or date of birth is different, the Applicant is required to verify the Driver's identity again. 803 CMR 2.09, 2.11.

A Driver's failure to re-consent to the Division background check or update their personal information shall result in the Applicant preventing the Driver from providing Transportation Network Services and notifying the Division of the Driver's non-compliance. Such a Driver shall not provide Transportation Network Services until the Applicant submits a new application to the Division and the Division processes their application.

The Applicant must submit a proposed plan for compliance with this process.

The required Background Check Consent & Authorization Form that the Applicant must require every Driver to sign upon their initial enrollment and every year is located at *Appendix 3.*

Section 7.04 Driver Submission Process

In order for the Division to conduct a background check the Applicant must electronically submit the Driver's information either by (1) an Application Program Interface (API) connection, or (2) through a spreadsheet in CSV file format. The Division will provide the Applicant with guidance for the appropriate submission format.

Required Driver information is as follows:

- Legal first name;
- Legal last name;
- Former name(s) (if known);
- Driver's license number;
- Driver's license state;
- Date of birth;
- Last six digits of social security number;
- Electronic mail address; and
- Date of background check consent & authorization.

Section 7.05 Division Background Check

At a minimum, the Division processes a Driver's personally identifying information through databases at the Department of Criminal Justice Information Services, Sex Offender Registry, Warrant Management System, and Registry of Motor Vehicles. The Division examines other databases and sources of information as well.

Generally, the Division will communicate background-check results (i.e., suitability decisions) to the Applicant within 72 hours.

Section 7.06 Suitability Notifications

The Division will communicate suitability decisions (approval, denial, suspension) to the Applicant and Driver electronically. The Division does not inform the Applicant of the specific reason for a negative suitability determination, only that the Driver was approved, denied, or suspended.

The Applicant is required to promptly prohibit a Driver from providing Transportation Network Services upon receipt of a negative suitability decision and under no circumstances over 12 hours.

Article VIII. CERTIFICATES FOR DRIVERS

Section 8.01 Background Check Clearance Certificate

A Background Check Clearance Certificate (Clearance Certificate) is issued by the Division to the Applicant and Driver. G.L. 159A½, § 1.[4] A Driver cannot provide Transportation Network Services without a valid Clearance Certificate. A Driver's failure to produce a Clearance Certificate upon request by law enforcement is a $100 fine for the 1st offense, $500 fine for the 2nd offense, and not more than a $1,000 fine for a third or subsequent offense. G.L. c. 159A½, § 7(d).

Section 8.02 Transportation Network Driver Certificate

The Applicant must issue a Transportation Network Driver Certificate (Driver Certificate) to a Driver in order to provide Transportation Network Services. 220 CMR 274.05. A Driver Certificate is not valid unless the Applicant confirms that the following are true:

(a) Driver has an approved Clearance Certificate;
(b) Driver's vehicle is in compliance with Transportation Network Vehicle inspection requirements; and
(c) Driver has required automobile insurance.

The Driver Certificate must include:

(a) Driver's legal name;
(b) An up-to-date facial image of the Driver;
(c) The license plate number of the Transportation Network Vehicle in use;
(d) A statement or recognizable logo to identify that the Applicant issued the Driver Certificate; and
(e) A statement that the Driver successfully completed the two-part background check as required by the Massachusetts Department of Public Utilities.

The Applicant must submit a copy of its proposed Driver Certificate to the Division for review and approval.

[4] A copy of a Clearance Certificate is appended to this Permit Application at ***Appendix 4***.

Article IX. REPORTING REQUIREMENTS

Section 9.01 Weekly

Weekly, the Applicant is required to submit a list of Drivers that it has permanently prevented from providing Rides due to reasons of public safety. The details of this requirement are outlined in *An Order Clarifying Suitability Notice Requirements for Transportation Network Companies* (June 2, 2021), which is included in this Permit Application form at ***Appendix 5***.

Section 9.02 Monthly

(a) Driver Roster Sync

Monthly, the Division will examine the Applicant's Driver roster to ensure that both the Division and the Applicant have an accurate and current Driver roster. G.L. c. 159A½, § 3(c)(vii). This requires the Applicant to extract the Driver roster information from its system, along with the current Driver status (e.g., approved, denied, deactivated, active), and transmit that information to the Division via an excel spreadsheet. The Division and Applicant will meet monthly to review this information. If there are any discrepancies between the Applicant's and Division's Driver roster information, the Division may require the Applicant to, at minimum, resubmit Driver information.

(b) Complaint Reporting

Monthly, the Applicant is required to submit to the Division a detailed, numerical accounting of the number of Driver and Rider complaints that the Applicant has received for the previous month, from whatever source and by whatever means, and an accounting of the actions that the Applicant has taken to resolve the complaints. 220 CMR 274.12(3).

The Applicant must have the following, easily accessible methods by which a consumer can submit a complaint: (1) Phone Number; (2) Email Address; and (3) Online Webpage. G.L. c. 159A½, § 3(c)(viii); 220 CMR 274.03(2)(d).

- [Insert Phone Number]
- [Insert Email Address]
- [Insert Webpage]

The Applicant is required to submit screenshots that depict how and where a consumer may access these methods of registering a complaint.

Section 9.03 Quarterly

Quarterly, the Division will audit the Applicant's Driver certification and background check processes. G.L. c. 159A½, § 4(f); 220 CMR 274.13(3). The Division will identify a random sample of Drivers to audit. The Division will, among other actions, issue an engagement letter, a request for records, a request for a preliminary meeting, a request for audit interviews, and a

request for remedial action plans. The Applicant is required to respond to the Division's record requests within 10 business days. 220 CMR 274.12(4).

Section 9.04 Annually

By February 1st of each year, the Applicant is required to submit to the Division the number of Rides for the previous calendar year, which shall include:

- City or town where each Ride originated;
- City or town where each Ride ended;
- Aggregated and anonymized trip route and length (miles and minutes); and
- Location of vehicle accidents.

The Division will provide the Applicant with a format by which to submit the Ride data. 220 CMR 274.12(2).

Section 9.05 Ad-Hoc

Frequently, the Division will direct the Applicant to provide information in order to review a Driver's suitability, such as for a suitability review hearing. This information may include:

- ❖ Criminal background check records;
- ❖ Motor vehicle background check records;
- ❖ Rider complaints and compliments;
- ❖ Information on whether the Applicant has ever suspended the Driver, including:
  - Reason(s) for suspension;
  - Date(s) of suspension;
  - Length(s) of suspension;
- ❖ Correspondence between the Applicant and Driver;
- ❖ Correspondence between the Applicant and Rider;
- ❖ Vehicle(s) associated with the Driver;
- ❖ Vehicle registration, inspection, and insurance documents; and
- ❖ Driver license(s) submitted to the Applicant by the Driver.

The Applicant is required to respond to the Division's record requests within 10 business days. 220 CMR 274.12(4).

Article X. PAYMENT OBLIGATIONS

Section 10.01 Per-Ride Assessment

By February 1st of each year, the Applicant must remit to the Division a payment of $0.20 for each Ride that originated within the Commonwealth of Massachusetts. St. 2016, c. 187, § 8.

The Division will provide the Applicant with information on how to remit the required payment to the Division.

Section 10.02 Surcharge

By March 31st of each year, the Applicant must submit to the Division its intrastate operating revenues for purposes of establishing a surcharge payment to fund the Division's operating activities. G.L. c. 25, § 23(b). If the Applicant does not submit its intrastate operating revenues, the Division may estimate them.

The Division will issue a surcharge order and the Applicant is required to remit the surcharge payment to the Division within 30 days of notice.

Article XI. RATES

Section 11.01 Rate Structure

The Applicant is required to provide Riders with a clear and conspicuous explanation of the total cost and pricing structure for its Rides. G.L. c. 159A½, § 2(d).

The Applicant must submit a copy of its price structure for Rides, including whether that structure differs based on geographic location.

Section 11.02 Waybill

The Applicant must submit screenshots/photographs of its sample waybill for both Riders and Drivers.

Section 11.03 Surge Pricing

The Applicant shall not raise base fares, impose additional charges or otherwise increase the price that a Rider is charged for Transportation Network Services, including by imposing surge pricing or other formulas based on increased demand, during a federal or a governor-declared state of emergency. G.L. c. 159A½, § 2(e).

In the event of a state of emergency, the Division will issue notice to inform the Applicant of this requirement.

Article XII. RIDER ACCESSIBILITY

The Applicant must ensure the non-discrimination of Riders with disabilities and special needs, including Riders requiring accommodation of service animals and wheelchairs. G.L. c. 159A½, § 3(c)(vi).

The Applicant must submit a policy to the Division outlining its proposed compliance with this requirement, including:

1. **Ensuring adequate availability of wheelchair-accessible vehicles (WAVs) in all areas served by the Applicant;**
2. **That the Digital Network and complaint reporting process is accessible to Riders with special needs, including those with visual impairments; and**
3. **Any Driver training or documentation provided to Drivers regarding the provision of services to Riders with disabilities and special needs.**

Article XIII. HOURS OF SERVICES

A Driver is not permitted to provide Transportation Network Services for more than 12 consecutive hours. If a Driver provides Transportation Network Services for 12 hours within a 24-hour period, the Applicant must ensure that the Driver is logged out of its Digital Network for at least 8 consecutive hours. 220 CMR 274.07.

The Applicant must submit a policy to the Division outlining its proposed compliance with this requirement.

Article XIV. WRITTEN INFORMATION SECURITY POLICY (WISP)

☐ The Applicant certifies that it has a Written Information Security Policy (WISP) in accordance with G.L. c. 93H and 201 CMR 17.00: *Standards for the Protection of Personal Information of Residents of the Commonwealth*

The Division may inspect the Applicant's WISP to determine whether it meets statutory and regulatory requirements. G.L. c. 159A½, § 8(a).

A WISP checklist is found at *Appendix 6*.

A model WISP is found at *Appendix 7*.

Article XV. LOGAN AIRPORT

The Applicant must enter into an agreement with the Massachusetts Port Authority in order to operate at Logan Airport. St. 2016, c. 187, § 11.

A list of frequently asked questions regarding TNC operations at Logan Airport is found at ***Appendix 8***. The following website contains more information regarding the Applicant's operations at Logan Airport:

http://www.massport.com/logan-airport/to-from-logan/transportation-options/ride-app-tnc/

The Division will consult with the Massachusetts Port Authority to determine the most appropriate means by which the Applicant may be approved to provide Transportation Network Services at Logan Airport.

Article XVI. STATE & MUNICIPAL REGULATION OF TRAFFIC

Municipalities, as well as local and state entities, may regulate traffic flow and traffic patterns relative to the Applicant's Transportation Network Services in order to ensure public safety and convenience. G.L. c. 159A½, § 10. Generally, this involves the regulation of the Applicant's pick-up and drop-off locations.

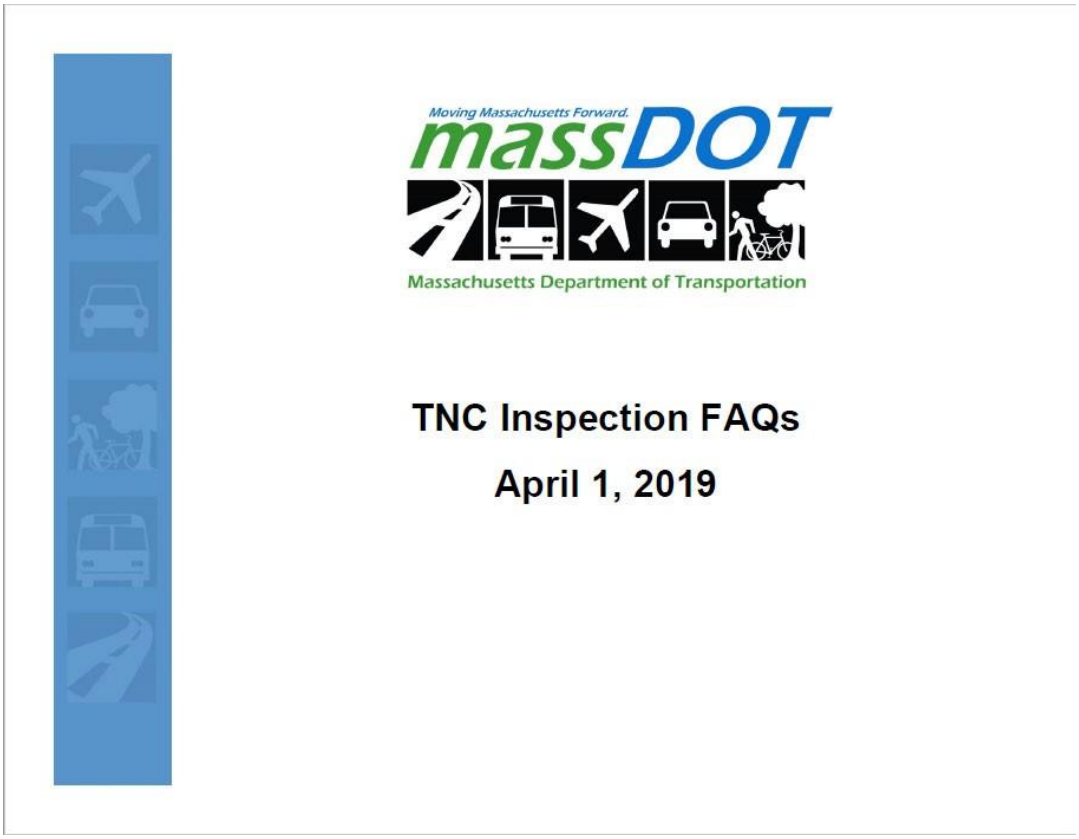
Article XVII. REGULATORY AUTHORITY

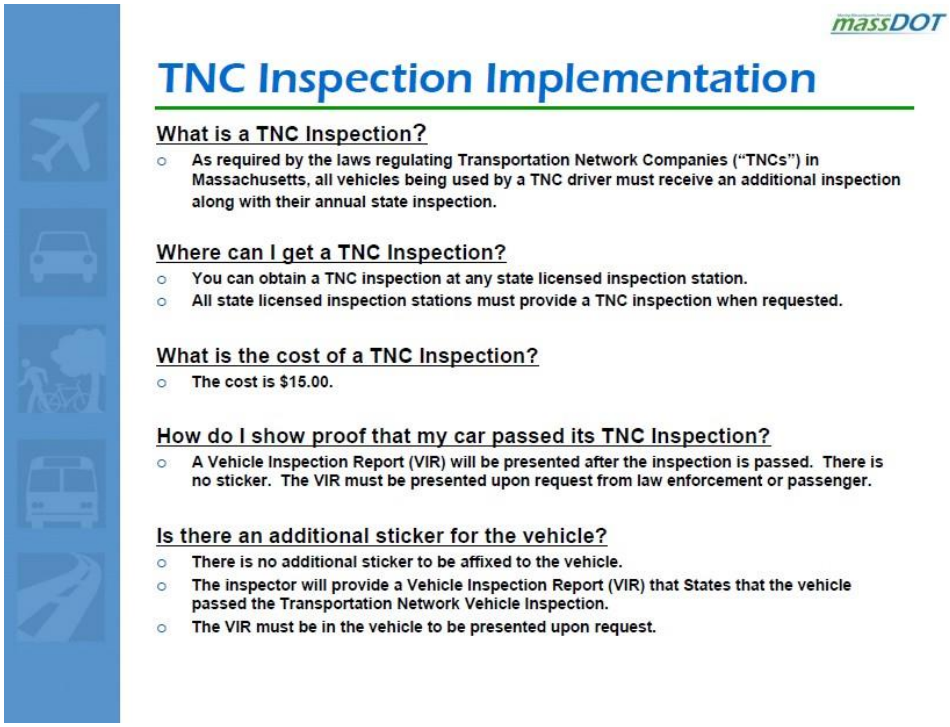
- Identify any jurisdiction where the Applicant is authorized to operate.

- Identify any jurisdiction where the Applicant's authority to operate has been suspended or revoked.
  - Include the reason(s) and length(s) for suspension(s) or revocation(s)

- Identify whether the Applicant has any pending regulatory violation/enforcement actions
  - Describe in detail:

Appendix 1


Moving Massachusetts Forward.
massDOT
Massachusetts Department of Transportation
TNC Inspection FAQs
April 1, 2019


massDOT
TNC Inspection Implementation
What is a TNC Inspection?
As required by the laws regulating Transportation Network Companies ("TNCs") in Massachusetts, all vehicles being used by a TNC driver must receive an additional inspection along with their annual state inspection.
Where can I get a TNC Inspection?
You can obtain a TNC inspection at any state licensed inspection station.
All state licensed inspection stations must provide a TNC inspection when requested.
What is the cost of a TNC Inspection?
The cost is $15.00.
How do I show proof that my car passed its TNC Inspection?
A Vehicle Inspection Report (VIR) will be presented after the inspection is passed. There is no sticker. The VIR must be presented upon request from law enforcement or passenger.
Is there an additional sticker for the vehicle?
There is no additional sticker to be affixed to the vehicle.
The inspector will provide a Vehicle Inspection Report (VIR) that States that the vehicle passed the Transportation Network Vehicle Inspection.
The VIR must be in the vehicle to be presented upon request.

massDOT

TNC Inspection Implementation

When is a TNC Inspection due?

- **Massachusetts Registered Vehicles:** TNC inspection is due at the vehicle's next state inspection and every year thereafter.
- **Out of State Registered Vehicles *With* a Home-State Inspection:** TNC inspection must be done by the last day of the month of the home-state inspection expiration and every year thereafter.
  - For example, if you have an April 2019 inspection sticker, you must have your TNC inspection completed by April 30, 2019.
- **Out of State Registered Vehicle *Without* a Home- State** inspection program (e.g., Connecticut) or one that is less frequent than every year (e.g., Rhode Island):
  - **Existing Network Vehicles -** TNC inspection must be done by September 30, 2019 and every year thereafter.
  - **Vehicles Entering *after* September 30, 2019 –** TNC inspection must be done within 60-days of joining the network.
- **Rental Vehicles:**
  - **Existing Network Vehicles -** TNC inspection must be done by September 30, 2019 and every year thereafter.
  - **Vehicles Entering *after* September 30, 2019 –** TNC inspection must be done within 60-days of joining the network.

massDOT

TNC Inspection Implementation

What if the vehicle fails the inspection?

- **If the vehicle does not pass inspection any defective items must be fixed.**
- **There is a free re-test within 20 days.**
- **After 20 days payment for the new test is required.**

What if I don't get my TNC Inspection?

- **If you fail to get a TNC Inspection within the time required you could be subject to a fine and a surcharge.**
- **Failure to comply may result in a revocation of a Driver's Background Check Clearance Certificate.**

massDOT

TNC Inspection Implementation

What is included in a TNC Inspection?

The vehicle must have a Current Valid Annual State Inspection

TNC inspection includes the brakes and suspension systems as well as the interior items listed below:

- The vehicle's heating, defrosting and air conditioning systems are in "good working order"
- All interior lights are operational and illuminate the interior of the vehicle.
- There are no holes, tears, sharp edges or springs or wires protruding in seats and interior panels.
- The open door warning devices are in proper operating condition for all doors.
- The vehicle's interior rear-view mirror is securely affixed.
- Both of the operator and passenger sun visors are in place.
- The door and window handles, locks and interior panels are in good working order.
- There are no loose items on the front dash or rear shelf.
- The seats, including the areas beneath them, and the rear floor area are free from debris.
- The vehicle's trunk is clean and free of debris.
- The vehicle's doors and windows operate as designed.

Appendix 2

TRANSPORTATION NETWORK/RIDESHARE DRIVERS

NOTICE OF COMMERCIAL TOLL RATE PROCEDURE
START DATE MONDAY, MAY 13, 2019

Please note that under Commonwealth of Massachusetts law, Chapter 187, of the Acts of 2016, adding to the General Laws Chapter 159A½ (see Section 2, paragraphs j and k) an Act Regulating Transportation Network Companies, transportation network drivers are required to pay the commerc toll rate when using their vehicle for transportation network services on a state road under the tolling authority of the Massachusetts Department of Transportation (MassDOT).

The Act further requires transportation network companies ("TNC") to have a process in place to ensure that tolls incurred by Transportation Network/Rideshare Drivers ("Driver"), while providing Transportation Network Services, are paid to MassDOT at the commercial toll rate.

In order to fulfill the requirements of the law, please note the following:

- It is recommended that Drivers have an E-ZPass MA account (an E-ZPass MA account and transponder issued by MassDOT).
- Drivers must have a TNC-approved decal at all times when providing transportation network services.
- TNCs will provide certain Driver and Ride Data to MassDOT, and then MassDOT will cross-reference toll data to ensure that tolls incurred by a Driver providing Transportation Network Services are paid at the commercial toll rate (see Section 2, paragraph k of the Act). The commercial toll rate applies during all periods of Transportation Network Services, including when a rideshare app is on, available to receive a request or en route a rider, without a rider in the vehicle.
- Where appropriate, MassDOT will upcharge the toll rate on the Driver's account to the commercial toll rate (noted on statement as "rideshare commercial upcharge"). It may take up to two weeks for this adjustment to appear on your account. Therefore, it is necessary that your E-ZPass M account be appropriately funded at all times to avoid any unnecessary fees. Please note that this process may result in an adjustment to the replenishment amount on your account. The easiest way to ensure that your account stays in good standing is by funding your account with a cre card.
- Please ensure that the name, address and license plate information on your E-ZPass MA account is the same information you have provided to th TNC.

IF YOU HAVE A VALID E-ZPASS MA ACCOUNT YOU DO NOT NEED TO OPEN ANOTHER ACCOUNT.

If you do not have an account, sign up for a *NEW* E-ZPass MA account as soon as possible click here to sign up.

To convert your existing Pay by Plate MA account to an E-ZPass MA account, please contact the EZDriveMA Customer Service Center at 877-627-7745.

Login to verify your existing E-ZPass MA account information. Click here to login.

Appendix 3

BACKGROUND CHECK CONSENT & AUTHORIZATION

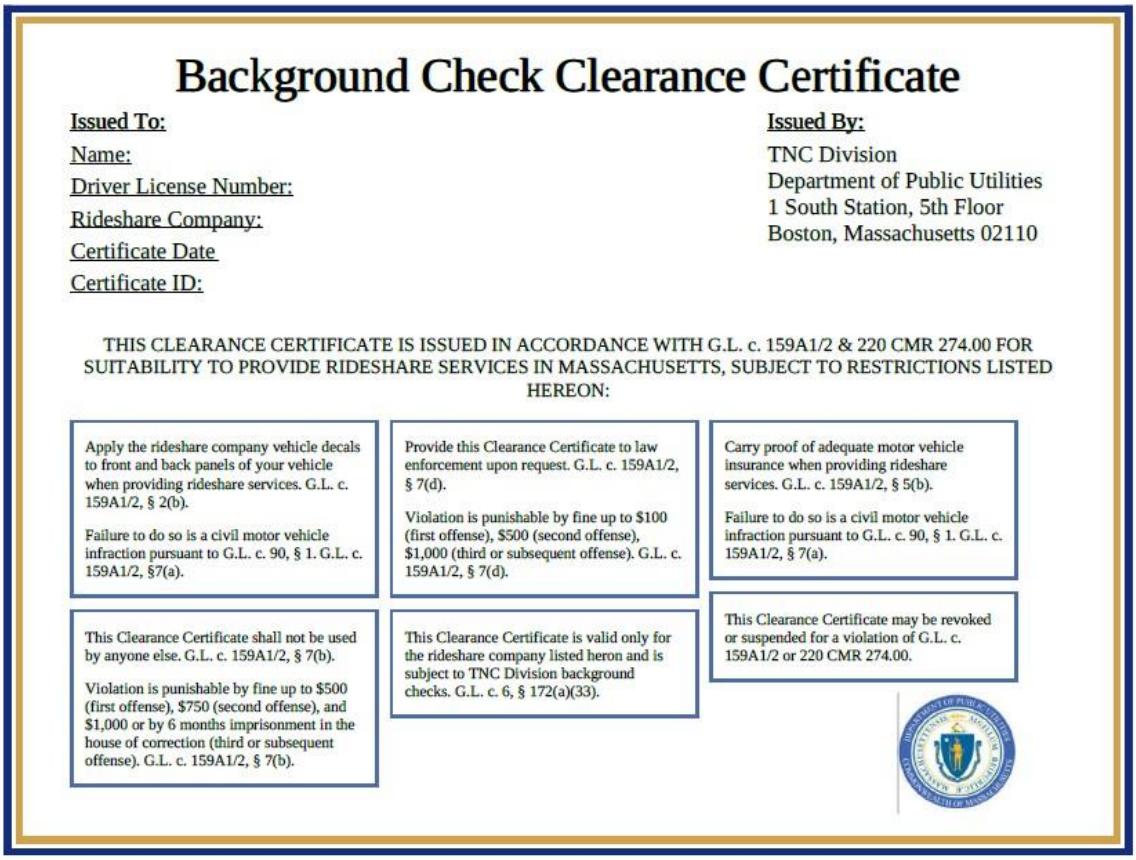
As a prospective or current Transportation Network Driver, I understand that the Department of Public Utilities' Division of Transportation Network Companies ("Division") shall review Criminal Offender Record Information, Sex Offender Registry Information, and Registry of Motor Vehicles driving record information ("Background Information") from the Department of Criminal Justice Information Services for the purpose of evaluating whether I am suitable to perform Transportation Network Services ("Suitability Review"). I hereby acknowledge that the Division is authorized to review Background Information and provide permission to [Insert Company Name] (the "Company") to submit my information to the Division for the purpose of performing this Suitability Review [and for the purposes of testing the Suitability Review system].

This authorization is valid for one year from the date of my signature or until the conclusion of my affiliation with the Company, whichever comes first. I understand that the Division may perform a Suitability Review multiple times during this period of time.

I may withdraw this authorization at any time by providing the Company and the Division with written notice of my intent to withdraw my consent. By withdrawing my consent, or if my Suitability Review Consent and Authorization form is not renewed after this one-year period, I understand that (1) the Division may make an adverse decision on my Background Check Clearance Certificate, including suspending or revoking my Background Check Clearance Certificate, and (2) the Company may make an adverse decision on my suitability to perform Transportation Network Services, including suspending or revoking my Background Check Clearance Certificate.

By clicking "Yes, I agree" I provide my consent to [Insert Company Name] to submit my information to the Division, and I consent to the Division's use of this information to perform a Suitability Review [and for the purposes of testing the Suitability Review system]. I affirm that the information I have provided to conduct a Suitability Review is true and accurate.

Appendix 4



Background Check Clearance Certificate

Issued To:

Name:

Driver License Number:

Rideshare Company:

Certificate Date

Certificate ID:

Issued By:

TNC Division
Department of Public Utilities
1 South Station, 5th Floor
Boston, Massachusetts 02110

THIS CLEARANCE CERTIFICATE IS ISSUED IN ACCORDANCE WITH G.L. c. 159A1/2 & 220 CMR 274.00 FOR SUITABILITY TO PROVIDE RIDESHARE SERVICES IN MASSACHUSETTS, SUBJECT TO RESTRICTIONS LISTED HEREON:

Apply the rideshare company vehicle decals to front and back panels of your vehicle when providing rideshare services. G.L. c. 159A1/2, § 2(b).

Failure to do so is a civil motor vehicle infraction pursuant to G.L. c. 90, § 1. G.L. c. 159A1/2, §7(a).

Provide this Clearance Certificate to law enforcement upon request. G.L. c. 159A1/2, § 7(d).

Violation is punishable by fine up to $100 (first offense), $500 (second offense), $1,000 (third or subsequent offense). G.L. c. 159A1/2, § 7(d).

Carry proof of adequate motor vehicle insurance when providing rideshare services. G.L. c. 159A1/2, § 5(b).

Failure to do so is a civil motor vehicle infraction pursuant to G.L. c. 90, § 1. G.L. c. 159A1/2, § 7(a).

This Clearance Certificate shall not be used by anyone else. G.L. c. 159A1/2, § 7(b).

Violation is punishable by fine up to $500 (first offense), $750 (second offense), and $1,000 or by 6 months imprisonment in the house of correction (third or subsequent offense). G.L. c. 159A1/2, § 7(b).

This Clearance Certificate is valid only for the rideshare company listed heron and is subject to TNC Division background checks. G.L. c. 6, § 172(a)(33).

This Clearance Certificate may be revoked or suspended for a violation of G.L. c. 159A1/2 or 220 CMR 274.00.

Appendix 5

COMMONWEALTH OF MASSACHUSETTS

DEPARTMENT OF PUBLIC UTILITIES
TRANSPORTATION NETWORK COMPANY DIVISION

CHARLES D. BAKER
GOVERNOR

KARYN E. POLITO
LIEUTENANT GOVERNOR

KATHLEEN A. THEOHARIDES
SECRETARY OF ENERGY
AND ENVIRONMENTAL AFFAIRS

ONE SOUTH STATION
BOSTON, MA 02110
(617) 305-3500

MATTHEW H. NELSON
CHAIR

ROBERT E. HAYDEN
COMMISSIONER

CECILE M. FRASER
COMMISSIONER

AMENDATORY ORDER

ORDER CLARIFYING SUITABILITY NOTICE REQUIREMENTS FOR TRANSPORTATION NETWORK COMPANIES

June 2, 2021

WHEREAS,[1] General Laws c. 159A½, § 2(l), requires Transportation Network Companies ("TNCs") to notify the Division upon receipt of information that (a) "a driver utilizing its network has violated a law or rule or regulation related to the provision of transportation network services" or (b) "that the driver is not suitable to provide transportation network services";

WHEREAS, General Laws c. 159A½, § 2(m) requires that, after a TNC notifies the Division of a Transportation Network Driver ("Driver") unsuitability, the Division shall verify the unsuitability and, if verified, shall suspend the Background Check Clearance Certificate ("Clearance Certificate") for each TNC that issued a Transportation Network Driver Certificate to the Driver;

WHEREAS, the Division finds that G.L. c. 159A½, §§ 2(l), (m) serve critical public safety objectives, including preventing an unsuitable Driver from providing Transportation Network Services ("Services") for any TNC;

WHEREAS, the Division finds that TNCs acknowledge the critical public safety objectives inherent in the process required under G.L. c. 159A½, §§ 2(l), (m) and currently engage in sharing information about Drivers that each TNC has determined are unsuitable;

---

1 All capitalized and abbreviated terms shall have the meaning as ascribed to them in 220 CMR 274.00.

WHEREAS, if a TNC notifies the Division of a Driver's unsuitability, the Division may temporarily suspend that Driver's Clearance Certificate while it verifies unsuitability in accordance with G.L. c. 159A½, § 2(m);

WHEREAS, when the Division verifies unsuitability, it must rely on substantial evidence in accordance with G.L. c. 30A and review suitability in accordance with 220 CMR 274.15;

WHEREAS, the Division finds that it cannot verify a Driver's unsuitability in accordance with G.L. c. 159A½, §§ 2(l), (m) without first considering the all information that the TNC relied upon to determine that Driver's unsuitability;

WHEREAS, the Division concludes that clarifying the process and requirements for a TNC's notice of unsuitability is "necessary for the administration, implementation and enforcement of chapter 159A½" as provided for in G.L. c. 25, § 23(a);

NOW, THEREFORE, in consideration of the statutory objectives and safety of the ride-hailing public, the Division hereby issues the following Order:

I. APPLICABILITY

(a) This Order is in addition to Deactivation Guidelines for TNCs and shall not replace those guidelines.

(b) This Order shall not apply when a TNC prevents a Driver from accessing its Digital Network for the following reasons:

(i) Expired license, motor vehicle document, or background check consent authorization;

(ii) Driver no longer wishes to provide Services for the TNC;

(iii) The TNC has a pending investigation into Driver unsuitability; or

(iv) Any other reason not substantially related to those set forth in sub-Sections I(c) and (d), below.

(c) Examples of situations that this Order shall apply include but are not limited to when a TNC permanently prevents a Driver from accessing its Digital Network for the following reasons:

(i) As required under 220 CMR 274.06(2)(d);

(ii) In response to Rider feedback regarding public safety;

(iii) Discovery of false information, counterfeit or altered documents, or any other fraudulent records submitted by the Driver; or

(iv) Account renting.[2]

(d) A TNC shall comply with the requirements of this Order for instances when the TNC permanently prevents a Driver from accessing its Digital Network for public-safety reasons that are not itemized in sub-Section I(c), above, including but not limited to a Driver who fails a TNC's bi-annual or continuous monitoring background check as it applies to the Division's Suitability Standard (220 CMR 274.21).

II. REQUIRED DOCUMENTATION

(a) A TNC shall affirmatively submit the information that it materially relied upon in determining that a Driver is unsuitable under sub-Sections I(c) and (d), above.

(b) The Division may require a TNC to provide additional documentation in order to administer the requirements of G.L. c. 159A½, §§ 2(l), (m), including but not limited to:

(i) A detailed description of the reason(s) for unsuitability;

(ii) All background check reports;

(iii) All licenses;

(iv) All Rider feedback;

(v) All correspondence between the TNC and Driver regarding the unsuitability determination; and

(vi) Any other information that the TNC relied upon in determining unsuitability.

[2] "Account renting" includes but is not limited to instances in which a Driver allows another person to impersonate the Driver or assume the Driver's credentials in order to provide Rides.

III. SUBMISSION FORMAT

(a) Responsive documents should be organized in folders labeled by the Driver's name (Last Name, First Name) and UUID (universally unique identifier) of the Driver the documents are associated with, i.e. "Smith, John UUIDEXAMPLE12".

(b) If multiple responsive documents of the same type exist for a Driver, the name of each should contain a date so that the Division can discern their proper order.

(c) Responsive documents should be converted PDF format, except when technical limitations would prevent legible conversion to this format.

(d) Multiple folders should be contained within a compressed (ZIP format) master folder that is named after the TNC and dated, i.e. "Acme TNC IR Responses 3.19.2021.zip". This compressed master folder should be transmitted to the Division via the Commonwealth Interchange or other Division-approved secure file transfer service.

IV. SUBMISSION CADENCE

(a) Within 24 hours, a TNC shall notify the Division by email of an unsuitable Driver under sub-Section I(c)(i), above. A TNC shall provide a brief description of the reason(s) for unsuitability.

(b) On Thursday of each week, a TNC shall notify the Division by email of an unsuitable Driver under sub-Sections I(c)(ii)-(iv) and sub-Section I(d), above. A TNC shall provide a brief description of the reason(s) for unsuitability.

(c) On Thursday of each week, a TNC shall submit to the Division the required information under sub-Section II(a), above, for any Driver that a TNC determines is unsuitable under sub-Sections I(c) and (d), above. The format submission shall comply with sub-Section III, above.

V. NON-COMPLIANCE

(a) Non-compliance with this Order shall constitute cause for the Division to refrain from issuing Clearance Certificates, issue monetary penalties, and take other action it deems necessary in accordance with 220 CMR 274.14(2).

VI. WAIVER

(a) The Division may waive requirements under this Order for good cause; provided, however, that any such waiver shall be consistent with G.L. c. 159A½ and the interest of public safety.

VII. ORDER

(a) Effective immediately, a TNC shall comply with sub-Section IV(a) and its corresponding document production requirement under sub-Section IV(c).

(b) Not later than July 1, 2021, a TNC shall comply with sub-Section IV(b) and its corresponding document production requirements under sub-Section IV(c), inclusive of the period from May 1, 2021, through July 1, 2021.

By Order of the Division,

Ryan Hawkins
Director

Appendix 6

CHARLES D. BAKER
GOVERNOR

KARYN E. POLITO
LIEUTENANT GOVERNOR

COMMONWEALTH OF MASSACHUSETTS
Office of Consumer Affairs and Business Regulation
10 Park Plaza, Suite 5170, Boston, MA 02116
(617) 973-8700 FAX (617) 973-8799
www.mass.gov/consumer

JAY ASH
SECRETARY OF HOUSING AND ECONOMIC DEVELOPMENT

JOHN C. CHAPMAN
UNDERSECRETARY

201 CMR 17.00 COMPLIANCE CHECKLIST

The Office of Consumer Affairs and Business Regulation has compiled this checklist to help small businesses in their effort to comply with 201 CMR 17.00. **This Checklist is not a substitute for compliance with 201 CMR 17.00**. Rather, it is designed as a useful tool to aid in the development of a written information security program for a small business or individual that handles "personal information." Each item, presented in question form, highlights a feature of 201 CMR 17.00 that will require proactive attention in order for a plan to be compliant.

The Comprehensive Written Information Security Program (WISP)

- ☐ Do you have a comprehensive, written information security program ("WISP") applicable to all records containing personal information about a resident of the Commonwealth of Massachusetts ("PI")?
- ☐ Does the WISP include administrative, technical, and physical safeguards for PI protection?
- ☐ Have you designated one or more employees to maintain and supervise WISP implementation and performance?
- ☐ Have you identified the paper, electronic and other records, computing systems, and storage media, including laptops and portable devices that contain personal information?
- ☐ Have you chosen, as an alternative, to treat all your records as if they all contained PI?
- ☐ Have you identified and evaluated reasonably foreseeable internal and external risks to paper and electronic records containing PI?
- ☐ Have you evaluated the effectiveness of current safeguards?
- ☐ Does the WISP include regular ongoing employee training, and procedures for monitoring employee compliance?

- ☐ Does the WISP include disciplinary measures for violators?
- ☐ Does the WISP include policies and procedures for when and how records containing PI should be kept, accessed or transported off your business premises?
- ☐ Does the WISP provide for immediately blocking terminated employees, physical and electronic access to PI records (including deactivating their passwords and user names)?
- ☐ Have you taken reasonable steps to select and retain a third-party service provider that is capable of maintaining appropriate security measures consistent with 201 CMR 17.00?
- ☐ Have you required such third-party service provider by contract to implement and maintain such appropriate security measures?
- ☐ Is the amount of PI that you have collected limited to the amount reasonably necessary to accomplish your legitimate business purposes, or to comply with state or federal regulations?
- ☐ Is the length of time that you are storing records containing PI limited to the time reasonably necessary to accomplish your legitimate business purpose or to comply with state or federal regulations?
- ☐ Is access to PI records limited to those persons who have a need to know in connection with your legitimate business purpose, or in order to comply with state or federal regulations?
- ☐ In your WISP, have you specified the manner in which physical access to PI records is to be restricted?
- ☐ Have you stored your records and data containing PI in locked facilities, storage areas or containers?
- ☐ Have you instituted a procedure for regularly monitoring to ensure that the WISP is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of PI; and for upgrading it as necessary?
- ☐ Are your security measures reviewed at least annually, or whenever there is a material change in business practices that may affect the security or integrity of PI records?
- ☐ Do you have in place a procedure for documenting any actions taken in connection with any breach of security; and does that procedure require post-incident review of events and actions taken to improve security?

Additional Requirements for Electronic Records

- ☐ Do you have in place secure authentication protocols that provide for:

- Control of user IDs and other identifiers?
- A reasonably secure method of assigning/selecting passwords, or for use of unique identifier technologies (such as biometrics or token devices)?
- Control of data security passwords such that passwords are kept in a location and/or format that does not compromise the security of the data they protect?
- Restricting access to PI to active users and active user accounts?
- Blocking access after multiple unsuccessful attempts to gain access?

☐ Do you have secure access control measures that restrict access, on a need-to-know basis, to PI records and files?

☐ Do you assign unique identifications plus passwords (which are not vendor supplied default passwords) to each person with computer access; and are those IDs and passwords reasonably designed to maintain the security of those access controls?

☐ Do you, to the extent technically feasible, encrypt all PI records and files that are transmitted across public networks, and that are to be transmitted wirelessly?

☐ Do you, to the extent technically feasible, encrypt all PI stored on laptops or other portable devices?

☐ Do you have monitoring in place to alert you to the occurrence of unauthorized use of or access to PI?

☐ On any system that is connected to the Internet, do you have reasonably up-to-date firewall protection for files containing PI; and operating system security patches to maintain the integrity of the PI?

☐ Do you have reasonably up-to-date versions of system security agent software (including malware protection) and reasonably up-to-date security patches and virus definitions?

☐ Do you have in place training for employees on the proper use of your computer security system, and the importance of PI security?

Appendix 7

Practical Law

View the online version at http://us.practicallaw.com/w-001-0073

Written Information Security Program (WISP)

MELISSA J. KRASNOW, DORSEY & WHITNEY LLP,
WITH PRACTICAL LAW INTELLECTUAL PROPERTY & TECHNOLOGY

A model Written Information Security Program (WISP) addressing the requirements of Massachusetts's Data Security Regulation and the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule. This Standard Document provides general guidance for developing a WISP as may be required by other state and federal laws and best practices. This Standard Document also includes integrated notes with important explanations and drafting tips.

DRAFTING NOTE: READ THIS BEFORE USING DOCUMENT

A Written Information Security Program (WISP) documents the measures that a business, or organization, takes to protect the security, confidentiality, integrity, and availability of the personal information and other sensitive information it collects, creates, uses, and maintains.

This model WISP:

- Addresses the requirements of Massachusetts's Data Security Regulation (Mass. Regs. Code tit. 201, §§ 17.01-17.05) and the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule (16 C.F.R. Part 314).
- Provides general guidance for developing a WISP as may be required by other state and federal laws and best practices.

Business Considerations

While this Standard Document serves as a helpful starting point for drafting any WISP, no model WISP is appropriate for all businesses. In developing a WISP, an organization should consider:

- The size, scope, and type of its business or other activities.
- Its information collection and use practices, including the amount and types of personal and other sensitive information it maintains.
- The need to secure both customer and employee personal information.
- Specific applicable legal requirements, which may depend on, among other things:
  - the nature and industry of the business or organization;
  - the type of information collected and maintained; and
  - the geographic footprint of the business, including the states where the organization's customers and employees reside.
- The resources available to implement and maintain an information security program.

Even when not explicitly required by law, a well-developed and maintained WISP may provide benefits, including:

- Prompting the business to proactively assess risk and implement measures to protect personal and other sensitive information.
- Educating employees and other stakeholders about the actions they need to take to protect personal and other sensitive information.
- Helping to communicate data security expectations and practices to leadership, customers, and other interested parties, such as regulators.

THOMSON REUTERS

- Establishing that the organization takes reasonable steps to protect personal and other sensitive information, especially in the event of a security incident where litigation or enforcement action could occur.

Legal Considerations

This model WISP is helpful in complying with the information security program requirements found in:

- Massachusetts's Data Security Regulation (Mass. Regs. Code tit. 201, §§ 17.01-17.05) (see Massachusetts Data Security Regulation).
- The GLBA Safeguards Rule (16 C.F.R. Part 314) (see Gramm-Leach-Bliley Act Safeguards Rule).
- Oregon's Identity Theft Protection Act (Or. Rev. Stat. § 646A.622) (see Oregon Identity Theft Protection Act).
- Other state laws and best practices with data security requirements (see Other State Data Security Safeguards Laws and Best Practices and Resources).

Massachusetts Data Security Regulation

The Massachusetts Data Security Regulation (Mass. Regs. Code tit. 201, §§ 17.01-17.05) provides the most detailed WISP requirements, and applies to any business that collects Massachusetts residents' personal information, no matter where the business is located. This Standard Document follows the Massachusetts Data Security Regulation's requirements, and should be used together with Practice Note, Written Information Security Programs: Compliance with the Massachusetts Data Security Regulation (*http://us.practicallaw.com/7-523-1520*).

Gramm-Leach-Bliley Act Safeguards Rule

The GLBA applies to financial institutions that collect consumers' non-public personal information (NPI). The GLBA Safeguards Rule requires companies to develop, implement, and maintain a WISP that includes appropriate administrative, technical, and physical safeguards to protect consumer information (16 C.F.R. § 314.3). It also requires them to contractually obligate their service providers who handle NPI to implement and maintain similar safeguards (16 C.F.R. § 314.4).

The Safeguards Rule defines WISP requirements more broadly than the Massachusetts Data Security Regulation, so this Standard Document is also suitable to use as a basis for developing a GLBA-compliant WISP, using the alternative language to define personal information as explained in Drafting Note, Scope: Personal Information. See Practice Note, GLBA: The Financial Privacy and Safeguards Rules: The Safeguards Rule (*http://us.practicallaw.com/4-578-2212*).

Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act (HIPAA) applies to certain health care entities and their service providers (business associates). The HIPAA Security Rule requires covered entities and their business associates to:

- Implement and maintain specified administrative, technical, and physical safeguards.
- Implement reasonable and appropriate written policies and procedures.
- Maintain a written record of required activities, such as risk assessments.

(See 45 C.F.R. Part 164, Subpart C and Practice Note, HIPAA Security Rule: Safeguards and Related Organizational and Document Requirements (*http://us.practicallaw.com/5-502-1269*).)

Covered entities and their business associates should:

- Ensure that their information security policies and procedures are HIPAA-compliant.
- Recognize that a WISP may provide them with a convenient way to organize and describe their information security program.
- Develop and maintain a WISP, if required by other applicable laws, such as the Massachusetts Data Security Regulation.

Oregon Identity Theft Protection Act

Like Massachusetts, Oregon has enacted a comprehensive statute that mandates the implementation of safeguards to protect residents' personal information (Or. Rev. Stat. § 646A.622). Oregon requires that organizations develop, implement, and maintain **reasonable** safeguards to protect the security, confidentiality, and integrity of the personal information they use. A business meets the reasonableness standard if it either:

- Complies with the GLBA, HIPAA, or any federal or state law that affords greater protection of personal information than the Oregon statute.
- Implements an information security program that includes specific:
  - administrative safeguards;
  - technical safeguards; and
  - physical safeguards, similar to those required by Massachusetts, all with an emphasis on risk assessment (Or. Rev. Stat. § 646A.622(2)(D)).

Oregon also provides flexibility for small businesses to scale their programs in a manner that is appropriate to their size, complexity, activities, and the sensitivity of the personal information they collect (Or. Rev. Stat. § 646A.622(4)). The same leeway is granted to all organizations covered by the GLBA Safeguards Rule (16 C.F.R. § 314.3(a)), while the HIPAA Security Rule permits a similar "flexibility of approach" for covered entities and their business associates to choose security measures appropriate to their size, complexity, capabilities, and risks (45 C.F.R. § 164.306(b)).

Other State Data Security Safeguards Laws

Several other states have enacted statutes that require organizations to protect personal information by developing, implementing, and maintaining reasonable information security safeguards. These proactive data protection laws are in addition to the data breach notification statutes enacted by all but a few states. See Data Breach Notification Laws: State Q&A Tool (*http://us.practicallaw.com/3-578-0925*).

California, Texas, and Rhode Island Data Security Safeguards Statutes

Some other state laws also require that organizations implement reasonable and appropriate security measures to protect personal information even if they do not specifically mandate a WISP.

For example, businesses that own, license, or maintain California residents' personal information must:

- Implement and maintain reasonable security procedures and practices to protect personal information from unauthorized access, destruction, use, modification, or disclosure.
- Contractually require any nonaffiliated third party to whom they disclose personal information to implement and maintain reasonable security measures.
- Implement specific measures to protect personal information when disposing of it.

(Cal. Civ. Code §§ 1798.81, 1798.81.5.)

Similarly, Texas law requires that businesses protect what the law deems to be sensitive personal information by:

- Implementing and maintaining reasonable data protection procedures, including taking any appropriate corrective actions.
- Securely destroying personal information or rendering it unreadable or indecipherable when it is no longer to be retained.

(Tex. Bus. & Com. Code Ann. § 521.052.)

More recently, the Rhode Island Identity Theft Protection Act of 2015 (effective June 26, 2016) requires businesses to:

- Implement and maintain a risk-based information security program with reasonable security procedures and practices that protect personal information and are appropriate to:
  - the organization's size and scope;
  - the nature of the personal information; and
  - the purpose for which the personal information was collected.
- Retain personal information no longer than is reasonably required:
  - to provide requested services;
  - to meet the purposes for which the personal information was collected;
  - in accordance with a written retention policy; or
  - by law.
- Use secure methods to destroy personal information.
- Contractually require any nonaffiliated third party to whom they disclose personal information to implement and maintain similar reasonable security procedures and practices.

(R.I. Gen. Laws § 11-49.3-2 (effective June 26, 2016).)

Best Practices and Resources

Several state and federal agencies have issued guidance documents to assist large and small businesses and other organizations in performing risk assessments and developing, implementing, and maintaining their information security programs, including:

- The Federal Trade Commission's (FTC):
  - Protecting Personal Information: A Guide for Business, which provides a five-principle approach to building an information security plan; and
  - Start with Security: A Guide for Business, which offers ten lessons learned from its data security enforcement actions, with practical guidance on how to reduce risks for all businesses.
- The National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity (NIST Framework), which organizes various globally-recognized industry standards and best practices into a model that any organization can adapt and use to identify risks and build an information security program (see Practice Note, The NIST Cybersecurity Framework (*http://us.practicallaw.com/5-599-6825*)).

- The California Attorney General's Cybersecurity in the Golden State, which includes practical recommendations for managing information security risks focused on small to medium-sized businesses.

These resources' recommendations are comparable to the Massachusetts Data Security Regulation's requirements and other similar state and federal laws, while providing additional technical guidance in an accessible form.

Drafting and Implementation Considerations

An organization's WISP should be consistent with its current data collection and information security practices, unless specific program plan documentation is in place to close any gaps. Businesses create potential compliance, enforcement, and litigation risks by putting in place and committing to WISPs they do not follow.

Therefore, before developing a WISP, an organization should:

- Gather all relevant information regarding the personal and other sensitive information that it collects, creates, uses, and maintains, including current information security practices.
- Identify all applicable laws and standards that affect the organization's use of personal or other sensitive information, including any contractual obligations.
- Define the WISP's scope, including the personal information, any other sensitive information, and legal requirements it intends to address.

(See Drafting Note, Scope and Practice Note, Written Information Security Programs: Compliance with the Massachusetts Data Security Regulation: Preliminary Considerations (*http://us.practicallaw.com/7-523-1520*).)

Related Policies and Other Documents

While an organization's WISP outlines the purpose, scope, and core elements of its information security program, specific security measures are often defined in related documents, including:

- Risk assessment reports and remediation plans.
- One or more workforce-facing information security policy documents, such as those that that establish policies regarding:
  - information classification and handling practices;
  - user access management and passwords;
  - computer and network security;
  - physical security;
  - incident reporting and response;
  - employee and contractor use of technology, for example, Acceptable Use and Bring Your Own Device to Work (BYOD) policies (see Standard Documents, IT Resources and Communications Systems Policy (*http://us.practicallaw.com/8-500-5003*) and Bring Your Own Device to Work (BYOD) Policy (*http://us.practicallaw.com/1-521-3920*)); and
  - information systems acquisition, development, and maintenance.
- Process and procedures documents that detail how to implement and maintain particular safeguards, typically for use by technical or other support staff.

Awareness and Training

Organizations should also consider how to best distribute and build awareness of the WISP and related policies, processes, and procedures. For example, businesses may choose to integrate information security training with existing ethics and compliance programs.

At a minimum, the organization should:

- Specifically train all employees and contractors, especially those who handle personal and other sensitive information as part of their duties, on the WISP and relevant policies and procedures.
- Require all employees and contractors to formally acknowledge their receipt and understanding of the documentation and training, using written forms or an online learning system.
- Retain training and acknowledgment records.

Assumptions

This written information security program (WISP) assumes that:

- **The organization only collects, creates, uses, and maintains US residents' personal information.** If the organization handles personal information in non-US locations or plans to transfer personal information to the US, it may be subject to data security or privacy laws in those other jurisdictions. Privacy laws vary significantly, and are often more stringent outside the US, especially in the EU (see Data protection: Country Q&A Tool (*http://us.practicallaw.com/2-502-1510*) to compare laws in the US and selected non-US locations).

Written Information Security Program (WISP)

The objectives of this comprehensive written information security program ("WISP") include defining, documenting, and supporting the implementation and maintenance of the administrative, technical, and physical safeguards [COMPANY] has selected to protect the personal information it collects, creates, uses, and maintains. This WISP has been developed in accordance with the requirements of the Massachusetts Data Security Regulation, Mass. Regs. Code tit. 201, §§ 17.01-17.05, other similar US state laws, and [LIST ADDITIONAL APPLICABLE LAWS AND OBLIGATIONS].

In the event of a conflict between this WISP and any legal obligation or other [COMPANY] policy or procedure, the provisions of this WISP shall govern, unless the Information Security Coordinator specifically reviews, approves, and documents an exception (see Section 3).

DRAFTING NOTE: WISP OBJECTIVES: APPLICABLE LAWS AND OBLIGATIONS

In this section, the organization should identify all applicable laws, standards, policies, and contractual obligations that may affect its use of personal information or impose obligations on its information security program and as will be addressed by the WISP (see Drafting Notes, Legal Considerations and Drafting and Implementation Considerations).

1. Purpose. The purpose of this WISP is to:

(a) Ensure the security, confidentiality, integrity, and availability of personal [and other sensitive] information [COMPANY] collects, creates, uses, and maintains;

(b) Protect against any anticipated threats or hazards to the security, confidentiality, integrity, or availability of such information;

(c) Protect against unauthorized access to or use of [COMPANY]-maintained personal [and other sensitive] information that could result in substantial harm or inconvenience to any customer or employee; and

(D) Define an information security program that is appropriate to [COMPANY]'s size, scope, and business; its available resources; and the amount of personal [and other sensitive] information that [COMPANY] owns or maintains on behalf of others, while recognizing the need to protect both customer and employee information.

DRAFTING NOTE: PURPOSE

This purpose statement tracks the high-level WISP requirements stated in the Massachusetts Data Security Regulation and other similar state and federal laws, including the GLBA (see Practice Note, Written Information Security Programs: Compliance with the Massachusetts Data Security Regulation: Massachusetts Regulation: General WISP Requirements (*http://us. practicallaw. com/7-523-1520*)).

2. Scope. This WISP applies to [all employees, contractors, officers, and directors of [COMPANY]/[DEFINE SCOPE]]. It applies to any records that contain personal [and other sensitive] information in any format and on any media, whether in electronic or paper form.

(a) For purposes of this WISP, "personal information" means either a US resident's first and last name or first initial and last name in combination with any one or more of the following data elements, or any of the following data elements standing alone or in combination, if such data elements could be used to commit identity theft against the individual:

(i) Social Security number;

(ii) Driver's license number, other government-issued identification number, including passport number, or tribal identification number;

(iii) 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 the individual's financial account [GLBA:, and any personally identifiable financial information or consumer list, description, or other grouping derived from personally identifiable financial information, where personally identifiable financial information includes any information:

(A) A consumer provides [COMPANY] to obtain a financial product or service;

(B) About a consumer resulting from any transaction involving a financial product or service with [COMPANY]; or

(C) Information [COMPANY] otherwise obtains about a consumer in connection with providing a financial product or service];

(iv) [Health information, including information [regarding the individual's medical history or mental or physical condition, or medical treatment or diagnosis by a health care professional/created or received by [COMPANY]]/[HIPAA: which identifies or for which there is a reasonable basis to believe the information can be used to identify the individual and which relates to the past, present, or future physical or mental health or condition of the individual, the provision of health care to the individual, or payment for the provision of health care to the individual]];

(v) Health insurance identification number, subscriber identification number, or other unique identifier used by a health insurer;

(vi) Biometric data collected from the individual and used to authenticate the individual during a transaction, such as an image of a fingerprint, retina, or iris; or

(vii) Email address with any required security code, access code, or password that would permit access to an individual's personal, medical, insurance, or financial account.

(b) Personal information does not include lawfully obtained information that is available to the general public, including publicly available information from federal, state, or local government records. [

(c) For purposes of this WISP, "sensitive information" means data that:

(i) [COMPANY] considers to be highly confidential information; or

(ii) If accessed by or disclosed to unauthorized parties, could cause significant or material harm to [COMPANY], its customers, or its business partners.

(iii) Sensitive information includes, but is not limited to, personal information. [See [COMPANY]'s information classification policy, available at [REFERENCE TO POLICY].]]

DRAFTING NOTE: SCOPE

The organization should determine whether the WISP applies enterprise-wide or only to selected business units or activities and adjust the scope statement as needed (see Practice Note, Written Information Security Programs: Compliance with the Massachusetts Data Security Regulation: Scope of the WISP (*http://us.practicallaw.com/7-523-1520*)).

Personal Information

The definition of personal information provided follows the generally-applicable Massachusetts Data Security Regulation and similar state laws, including those of Oregon and Rhode Island (Or. Rev. Stat. § 646A.602(11); R.I. Gen. Laws § 11-49.3-3 (effective June 26, 2016)). While there are similarities, each state's statute defines personal information differently, so this definition combines the elements in the Massachusetts, Oregon, and Rhode Island laws.

Generally, the WISP should define personal information considering:

- The data the business collects, creates, uses, or maintains.
- The organization's near-term business plans, such as the states where its customers or employees may reside.
- Applicable laws (see Drafting Note, Legal Considerations) to protect data that the organization references in its privacy policy or other public statements.
- What is otherwise considered personal information by the organization, including any information that it must protect by contract with third parties.

If applicable:

- Section 2(a)(iii) should include the additional text to meet GLBA's definition of non-public personal information (see 16 C.F.R. § 313.3(n)(1)).
- Section 2(a)(iv) should use the optional text regarding HIPAA to meet HIPAA's requirements (see 45 C.F.R. § 160.103).

Sensitive Information

If the ISP is intended to cover other data that the organization considers to be sensitive, in addition to personal information, then the optional text should be included in this section and throughout the WISP. For example, a business may wish to apply the same WISP to highly confidential information regarding its products, business plans, or certain operations (or may be required to do so by contract with third parties).

Sensitive or highly confidential information:

- Typically includes data that if accessed by or disclosed to unauthorized parties could cause **significant or material harm** to the organization, its customers, or its business partners.
- Includes, but is not limited to, personal information.
- May be contrasted to an organization's less sensitive, but still non-public internal use only or confidential information.

If the organization has an information classification policy, for example, as part of its information security policies and procedures (see Section 5), the WISP should include a reference as shown in the optional text.

3. Information Security Coordinator. [COMPANY] has designated [TITLE] to implement, coordinate, and maintain this WISP (the "Information Security Coordinator"). The Information Security Coordinator shall be responsible for:

(a) Initial implementation of this WISP, including:

(i) Assessing internal and external risks to personal [and other sensitive] information and maintaining related documentation, including risk assessment reports and remediation plans (see Section 4);

(ii) Coordinating the development, distribution, and maintenance of information security policies and procedures (see Section 5);

(iii) Coordinating the design of reasonable and appropriate administrative, technical, and physical safeguards to protect personal [and other sensitive] information (see Section 6);

(iv) Ensuring that the safeguards are implemented and maintained to protect personal [and other sensitive] information throughout [COMPANY], where applicable (see Section 6);

(v) Overseeing service providers that access or maintain personal [and other sensitive] information on behalf of [COMPANY] (see Section 7);

(vi) Monitoring and testing the information security program's implementation and effectiveness on an ongoing basis (see Section 8);

(vii) Defining and managing incident response procedures (see Section 9); and

(viii) Establishing and managing enforcement policies and procedures for this WISP, in collaboration with [COMPANY] human resources and management (see Section 10).

(b) Employee, contractor, and (as applicable) stakeholder training, including:

(i) Providing periodic training regarding this WISP, [COMPANY]'s safeguards, and relevant information security policies and procedures for all employees, contractors, and (as applicable) stakeholders who have or may have access to personal [or other sensitive] information;

(ii) Ensuring that training attendees formally acknowledge their receipt and understanding of the training and related documentation, through [written acknowledgement forms/[DESCRIBE ANY ONLINE ACKNOWLEDGMENT PROCESS]]; and

(iii) Retaining training and acknowledgment records.

(c) Reviewing the WISP and the security measures defined herein at least annually, or whenever there is a material change in [COMPANY]'s business practices that may reasonably implicate the security, confidentiality, integrity, or availability of records containing personal [or other sensitive] information (see Section 11).

(D) Defining and managing an exceptions process to review, approve or deny, document, monitor, and periodically reassess any necessary and appropriate, business-driven requests for deviations from this WISP or [COMPANY]'s information security policies and procedures.

(e) Periodically reporting to [COMPANY] management regarding the status of the information security program and [COMPANY]'s safeguards to protect personal [and other sensitive] information.

DRAFTING NOTE: INFORMATION SECURITY COORDINATOR

Considerations for designating an information security coordinator depend on the organization's specific circumstances and may include:

- The organization's size, industry, and regulators.
- The types of personal and other sensitive information the organization owns or maintains on behalf of others.
- The employees responsible for the organization's compliance with security requirements, including compliance with its internal policies and procedures, contracts, and relevant laws and industry standards.
- Leadership support and sponsorship to ensure the information security coordinator has sufficient authority to implement and enforce the WISP.

The organization should also consider the appropriate business units to involve in program oversight, which may include:

- Legal.
- Information technology (IT).
- Privacy or a broader ethics and compliance unit.

The specific title used for the information security coordinator role may also vary according to the organization's size, industry, and other characteristics. The WISP should be drafted to refer to the coordinator by current title, and not individual name, to minimize maintenance requirements and any potential confusion if personnel change.

4. Risk Assessment. As a part of developing and implementing this WISP, [COMPANY] will conduct a periodic, documented risk assessment[, at least annually, or whenever there is a material change in [COMPANY]'s business practices that may implicate the security, confidentiality, integrity, or availability of records containing personal [or other sensitive] information].

(a) The risk assessment shall:

(i) Identify reasonably foreseeable internal and external risks to the security, confidentiality, integrity, or availability of any electronic, paper, or other records containing personal [or other sensitive] information.

(ii) Assess the likelihood and potential damage that could result from such risks, taking into consideration the sensitivity of the personal [and other sensitive] information.

(iii) Evaluate the sufficiency of relevant policies, procedures, systems, and safeguards in place to control such risks, in areas that include, but may not be limited to:

(A) Employee, contractor, and (as applicable) stakeholder training and management;

(B) Employee, contractor, and (as applicable) stakeholder compliance with this WISP and related policies and procedures;

(C) Information systems, including network, computer, and software acquisition, design, implementation, operations, and maintenance, as well as data processing, storage, transmission, retention, and disposal; and

(D) [COMPANY]'s ability to prevent, detect, and respond to attacks, intrusions, and other security incidents or system failures.

(b) Following each risk assessment, [COMPANY] will:

(i) Design, implement, and maintain reasonable and appropriate safeguards to minimize identified risks;

(ii) Reasonably and appropriately address any identified gaps.

(iii) Regularly monitor the effectiveness of [COMPANY]'s safeguards, as specified in this WISP (see Section 8).

DRAFTING NOTE: RISK ASSESSMENT

Risk assessment is a critical element of any information security program. Information security risks are best understood using this simple equation: **risk = threat + vulnerability**.

Threats may include external bad actors or internal (employee or contractor) lapses, whether inadvertent or intentional. Vulnerabilities cover a wide range of issues related to process, people, and technology, such as:

- Untrained or inattentive individuals.
- Improperly secured facilities.
- Poor implementation, configuration, or maintenance practices.
- Flaws in network and computer assets, including hardware, software, and application issues.

See Drafting Note, Best Practices and Resources and Practice Note, Written Information Security Programs: Compliance with the Massachusetts Data Security Regulation: Identifying and Minimizing Reasonably Foreseeable Internal and External Risks (*http://us.practicallaw.com/7-523-1520*) for guidance on risk assessments.

Risks change over time as:

- Novel threats emerge.
- Vulnerabilities are identified and become widely-known.
- The business evolves, especially when it:
  - makes changes in data collection and handling practices;

- introduces new or materially changed products and services;
- alters its business processes and practices; or
- deploys new, or updates existing, network and computer environments.

Organizations should develop processes to assess risks on an ongoing basis and periodically update their formal risk assessment. These updates should be made at least annually or whenever there is a material change in applicable business practices.

5. Information Security Policies and Procedures. As part of this WISP, [COMPANY] will develop, maintain, and distribute information security policies and procedures in accordance with applicable laws and standards to relevant employees, contractors, and (as applicable) other stakeholders to:

(a) Establish policies regarding:

(i) Information classification;

(ii) Information handling practices for personal [and other sensitive] information, including the storage, access, disposal, and external transfer or transportation of personal [and other sensitive] information;

(iii) User access management, including identification and authentication (using passwords or other appropriate means);

(iv) Encryption;

(v) Computer and network security;

(vi) Physical security;

(vii) Incident reporting and response;

(viii) Employee and contractor use of technology, including Acceptable Use and Bring Your Own Device to Work (BYOD); and

(ix)Information systems acquisition, development, operations, and maintenance.

(b) Detail the implementation and maintenance of [COMPANY]'s administrative, technical, and physical safeguards (see Section 6).

DRAFTING NOTE: INFORMATION SECURITY POLICIES AND PROCEDURES

Information security policies:

- Serve as a foundational administrative safeguard by providing clear guidance and limits for employees, contractors, and other stakeholders.
- Explain how the organization classifies various forms of data, which in turn defines the level and nature of safeguards to be applied.
- Should be written for and accessible to all employees, contractors, and other stakeholders.
- Should be periodically reviewed and updated as risks and the business change.

Information security procedures:

- Document how the organization implements and maintains its selected safeguards.
- Often include technical details intended primarily for IT or other support staff.

6. Safeguards. [COMPANY] will develop, implement, and maintain reasonable administrative, technical, and physical safeguards in accordance with applicable laws and standards to protect the security, confidentiality, integrity, and availability of personal [or other sensitive] information that [COMPANY] owns or maintains on behalf of others.

(a) Safeguards shall be appropriate to [COMPANY]'s size, scope, and business; its available resources; and the amount of personal [and other sensitive] information that [COMPANY] owns or maintains on behalf of others, while recognizing the need to protect both customer and employee information.

(b) [COMPANY] shall document its administrative, technical, and physical safeguards in [COMPANY]'s information security policies and procedures (see Section 5).

(c) [COMPANY]'s administrative safeguards shall include, at a minimum:

(i) Designating one or more employees to coordinate the information security program (see Section 3);

(ii) Identifying reasonably foreseeable internal and external risks, and assessing whether existing safeguards adequately control the identified risks (see Section 4);

(iii) Training employees in security program practices and procedures, with management oversight (see Section 3);

(iv) Selecting service providers that are capable of maintaining appropriate safeguards, and requiring service providers to maintain safeguards by contract (see Section 7); and

(v) Adjusting the information security program in light of business changes or new circumstances (see Section 11);

(D) [COMPANY]'s technical safeguards shall include maintenance of a security system covering its network (including wireless capabilities) and computers that, at a minimum, and to the extent technically feasible, supports:

(i) Secure user authentication protocols, including:

(A) Controlling user identification and authentication with a reasonably secure method of assigning and selecting passwords (ensuring that passwords are kept in a location or format that does not compromise security) or by using other technologies, such as biometrics or token devices;

(B) Restricting access to active users and active user accounts only, including preventing terminated employees or contractors from accessing systems or records; and

(C) Blocking access to a particular user identifier after multiple unsuccessful attempts to gain access or placing limitations on access for the particular system.

(ii) Secure access control measures, including:

(A) Restricting access to records and files containing personal [or other sensitive] information to those with a need to know to perform their duties; and

(B) Assigning unique identifiers and passwords (or other authentication means, but not vendor-supplied default passwords) to each individual with computer or network access that are reasonably designed to maintain security.

(iii) Encryption of all personal [or other sensitive] information traveling wirelessly or across public networks.

(iv) Encryption of all personal [or other sensitive] information stored on laptops or other portable or mobile devices [, and to the extent technically feasible, personal [or other sensitive] information stored on any other device or media (data-at-rest)].

(v) Reasonable system monitoring for preventing, detecting, and responding to unauthorized use of or access to personal [or other sensitive] information or other attacks or system failures.

(vi) Reasonably current firewall protection and software patches for systems that contain (or may provide access to systems that contain) personal [or other sensitive] information.

(vii) Reasonably current system security software (or a version that can still be supported with reasonably current patches and malware definitions) that (1) includes malicious software ("malware") protection with reasonably current patches and malware definitions, and (2) is configured to receive updates on a regular basis.

(e) [Company]'s physical safeguards shall, at a minimum, provide for:

(i) Defining and implementing reasonable physical security measures to protect areas where personal [or other sensitive] information may be accessed, including reasonably restricting physical access and storing records containing personal [or other sensitive] information in locked facilities, areas, or containers.

(ii) Preventing, detecting, and responding to intrusions or unauthorized access to personal [or other sensitive] information, including during or after data collection, transportation, or disposal.

(iii) Secure disposal or destruction of personal [or other sensitive] information, whether in paper or electronic form, when it is no longer to be retained in accordance with applicable laws or accepted standards.

DRAFTING NOTE: SAFEGUARDS

The safeguards detailed here track the Massachusetts Data Security Regulation and other similar state laws, including Oregon's statute, as well as the GLBA Safeguards Rule. Organizations that are subject to HIPAA should update the administrative, technical, and physical safeguards accordingly.

Organizations should not only examine applicable laws but also determine the feasibility of implementing and maintaining safeguards in their environments. According to guidance from the Massachusetts Office of Consumer Affairs and Business Regulation, "technically feasible" means that if there is a reasonable means through technology to accomplish a required result, the organization must use such reasonable means.

Legal requirements generally call for encrypting personal information when it is stored on mobile devices or transmitted wirelessly or over public networks. However, to better manage risk, organizations may choose to expand their encryption programs to include any stored personal information (data-at-rest) to the extent feasible, as shown in the optional text. For example, many federal and state data breach notification laws provide safe harbor from notice requirements when encryption is used (and encryption keys or other controls are not compromised by a breach).

To minimize potential compliance risk and liability, a business should meet the safeguards commitments it makes in its WISP or have a reasonable remediation plan in place and documented to close any gaps.

7. Service Provider Oversight. [COMPANY] will oversee each of its service providers that may have access to or otherwise create, collect, use, or maintain personal [or other sensitive] information on its behalf by:

(a) Evaluating the service provider's ability to implement and maintain appropriate security measures, consistent with this WISP and all applicable laws and [COMPANY]'s obligations.

(b) Requiring the service provider by contract to implement and maintain reasonable security measures, consistent with this WISP and all applicable laws and [COMPANY]'s obligations.

(c) Monitoring and auditing the service provider's performance to verify compliance with this WISP and all applicable laws and [COMPANY]'s obligations.

DRAFTING NOTE: SERVICE PROVIDER OVERSIGHT

Organizations should:

- Conduct data security due diligence on their service providers before engagement and monitor and audit ongoing performance.
- Identify their applicable existing service providers and, if necessary, amend their contracts to ensure compliance with applicable laws and the WISP.
- Include specific requirements in new service provider agreements involving personal or other sensitive information to address compliance with applicable laws and the WISP.
- Address service provider oversight in employee training.

See Practice Note, Written Information Security Programs: Compliance with the Massachusetts Data Security Regulation: Third-Party Service Providers (*http://us.practicallaw.com/7-523-1520*).

8. Monitoring. [COMPANY] will regularly test and monitor the implementation and effectiveness of its information security program to ensure that it is operating in a manner reasonably calculated to prevent unauthorized access to or use of personal [or other sensitive] information. [COMPANY] shall reasonably and appropriately address any identified gaps.

9. Incident Response. [COMPANY] will establish and maintain policies and procedures regarding information security incident response (see Section 5). Such procedures shall include:

(a) Documenting the response to any security incident or event that involves a breach of security;

(b) Performing a post-incident review of events and actions taken; and

(c) Reasonably and appropriately addressing any identified gaps.

10. Enforcement. Violations of this WISP will result in disciplinary action, in accordance with [COMPANY]'s information security policies and procedures and human resources policies. Please see [REFERENCE TO HR POLICIES] for details regarding [COMPANY]'s disciplinary process.

DRAFTING NOTE: ENFORCEMENT

Organizations must impose disciplinary measures for WISP violations under the Massachusetts Data Security Regulation. Other laws may require similar sanctions. To avoid employee confusion and potential conflicts, rather than creating its own disciplinary process, the WISP should refer to established human resources policies and processes. Information security policies and procedures may further define prohibited actions and compliance processes.

11. Program Review. [COMPANY] will review this WISP and the security measures defined herein at least annually, or whenever there is a material change in [COMPANY]'s business practices that may reasonably implicate the security, confidentiality, integrity, or availability of records containing personal [or other sensitive] information.

(a) [COMPANY] shall retain documentation regarding any such program review, including any identified gaps and action plans.

DRAFTING NOTE: PROGRAM REVIEW

The Massachusetts Data Security Regulation and best practices require that a business review its WISP on at least an annual basis or whenever there is a material change in business practices that may implicate the security or integrity of records that contain personal or other sensitive information.

12. Effective Date. This WISP is effective as of [DATE].

(a) Revision History: [Original publication/[NOTE SUBSEQUENT REVISIONS]].

DRAFTING NOTE: EFFECTIVE DATE

The WISP should include an effective date and identify any subsequent revisions. The organization should briefly note in the revision history any material updates and their drivers, such as a periodic program review or change in business processes, laws, or identified risks. The organization should retain prior versions of the WISP to demonstrate the program that was in effect at any particular time.

Appendix 8

Transportation Network Company (TNC) Drivers Frequently Asked Questions
Valid as of January 27, 2017
TNCs Permitted to Operate at Logan Airport Starting February 1, 2017: Uber and Lyft

Massport, owner and operator of Boston Logan International Airport ("Logan Airport"), has reached agreements with Uber and Lyft to permit TNC Drivers to pick customers up at Logan Airport starting February 1, 2017.

If you have questions for your specific company, please contact them directly.

Q: Can I pick passengers up at Logan Airport now?

A: Starting February 1, 2017, TNC Drivers for Uber and/or Lyft may pick customers up at Logan Airport **if and only if you have received a Background Check Clearance Certificate (BCCC) from the Department of Public Utilities (DPU)**.

Your Background Check Clearance Certificate must be current and valid to operate at Logan Airport. If your Background Check Clearance Certificate is revoked or suspended at any time you must **immediately stop** picking customers up at Logan Airport.

Q: Are all TNC Drivers now eligible to pick up at Logan Airport?

A: No. You must have a current and valid Background Check Clearance Certificate from the Department of Public Utilities (DPU) and drive for Uber and/or Lyft in order to pick up customers at Logan Airport. Not all Drivers have received a Background Check Clearance Certificate at this time, so being a current Uber and/or Lyft Driver does not necessarily mean you are eligible operate at Logan Airport yet.

Q: Can I drop passengers off at Logan Airport?

A: TNC Drivers may only drop off customers on the upper level (Departures) at Logan. Customers cannot be picked up on the upper level—if you have a current and valid Background Check Clearance Certificate and would like to pick a passenger up after dropping another customer off, you must first proceed to the APP Ride/TNC Pool Lot, which is the only location on Logan Airport where you are able to receive a ride request.

Q: Where can I receive a ride request from a customer at Logan Airport?

A: The APP Ride/TNC Pool Lot is the only location on Logan Airport where you can receive a ride request. Drivers may not pick a customer up from Logan Airport without first entering the APP Ride/TNC Pool Lot to receive a ride request. Drivers must depart from the APP Ride/TNC Pool Lot and proceed directly to the correct APP Ride/TNC Pick Up Area, following the route prescribed by Massport. Drivers may only pick customers up when they are ready with their luggage.

(Please see the Driver Flyer on the Massport website for a map of the APP Ride/TNC Pool Lot and pick up locations at Logan Airport, and directions to each Terminal APP Ride/TNC Pick Up Area.)

Q: Where can I pick passengers up at Logan Airport?

A: Drivers may only pick customers up at the Massport-designated APP Ride/TNC Pick Up Area at each Terminal, never at the curb or on the roadways.

(Please see the Driver Flyer on the Massport website for a map of the pick up locations at Logan Airport, and directions to each Terminal APP Ride/TNC Pick Up Area.)

Q: What do I do if my customer cancels the ride while I am on my way to pick them up at the Terminal APP Ride/TNC Pick Up Lot?

A: If a ride is cancelled by the customer after the Driver has accepted the ride and is on the way from the APP Ride/TNC Pool to the Terminal APP Ride/TNC Pick Up Area, the Driver has three (3) minutes to accept a new ride through the app while waiting in the nearest APP Ride/TNC Terminal Pick Up Area. If no ride is accepted within the three (3) minute period, the Driver must return to the APP Ride/TNC Pool Lot and wait for another ride request.

Q: What are the rules for TNCs at Logan Airport?

A: TNCs are subject to all Massport rules and regulations. Massachusetts State Police will be responsible for all safety and security matters occurring on Logan Airport property and will enforce all Massport rules. TNC Drivers must show their current and valid Background Check Clearance Certificate or proof of adequate insurance to a Massport Agent or Massachusetts State Trooper upon request. As required by Massachusetts state law, TNC drivers are not allowed to solicit customers or accept, arrange or provide transportation in any manner besides a pre-arranged ride on a digital network. Failure to comply with Massport rules may result in fines.

(Please see the Rules posted to the Massport website for more information.)

Q: I currently operate at Logan Airport with a livery plate—do I need a new Background Check Clearance Certificate to operate at Logan Airport now?

A: If you operate as a limo driver with livery plates at Logan Airport and plan to continue to do so, you must have a PSID per your Ground Access Agreement. If you will operate as a TNC with Uber and/or Lyft, you must have a current and valid Background Check Clearance Certificate from the Department of Public Utilities (DPU) and report to the APP Ride/TNC Pool Lot in order to receive a ride request.

Q: Are there additional costs associated with operating at Logan Airport?

A: There is not a direct cost to TNC Drivers to operate at the Airport. An Airport Fee of $3.25 is assessed as part of the overall cost for rides originating at Logan Airport, which TNC companies can pass on to customers. Fees associated with TNCs are common at major airports across the country and help ensure that service levels, public safety needs and operational costs are met.

Q: How do I get my decal?

A: Each TNC you are registered to drive for will issue you a decal.