

MEMORANDUM OF UNDERSTANDING

TERMS AND CONDITIONS FOR TAXI AND LIMOUSINE COMMISSION AUTHORIZATION

between

New York City Taxi and Limousine Commission and
_____ to conduct a pilot program testing
a smartphone application

TERMS AND CONDITIONS FOR TLC AUTHORIZATION (the “Agreement”) effective as of this _____ day of _____, 2013 between the City of New York (the “City”), acting by and through the Taxi and Limousine Commission, located at 33 Beaver Street, New York, New York 10004 (the “TLC” or “Commission”), and _____, a _____ corporation having a place of business at _____ (“E-Hail Pilot Participant”).

Whereas, the Commission is authorized by the New York City Charter to license and regulate for-hire vehicle transportation in the City;

Whereas, the Commission is authorized pursuant to Section 2303(b)(9) of the New York City Charter to approve pilot programs to test innovative and experimental types of modes of transportation service and manner of operation, and adopted the pilot programs rules, codified in Chapter 52 of Title 35 of the Rules of the City of New York;

Whereas, by resolution adopted on December 13, 2012 the Commission approved a pilot program (the “E-Hail Pilot”) for the testing of the viability of the use of smartphone applications for hailing taxicabs and for allowing taxicab passengers to pay fares by smart phone applications. The purpose of the pilot program is to test and evaluate the usefulness and effectiveness of such applications, and whether such applications can integrate with existing taxi information systems. The Commission approval authorized the negotiation and entry into this Agreement;

Whereas, the E-Hail Pilot Participant has filed an application with the Commission to participate in the E-Hail Pilot and the Commission has determined that the E-Hail Pilot Participant, on the basis of its application, has met the preliminary conditions for participation in the E-Hail Pilot;

Whereas, the E-Hail Pilot Participant is willing to comply with all Commission required terms and conditions for participation in the E-Hail Pilot; and

Whereas, the Commission, based on the E-Hail Pilot Participant’s agreement and subject to E-Hail Pilot Participant’s ability to meet and continue to meet all requirements for approval of Participant’s App for use in the E-Hail Pilot, is prepared to authorize Participant’s App for use in the E-Hail Pilot.

Now therefore, the TLC and the E-Hail Pilot Participant agree as follows:

§1 Definitions

- (a) *Chair* means the Commissioner/Chair of the TLC, or his or her designee.
- (b) *Credit, Debit, and Prepaid Card Services.* The portion of the E-Hail App used to process Passenger payment of fare in a Vehicle by credit, debit, or prepaid card.
- (c) *Digital Wallet Application.* An application residing on an electronic device which passes user payment data to a point-of-sale device using Near-Field Communication (“NFC”) technology, does not receive payment amount information regarding the transaction, and does not modify or edit the amount to be paid.
- (d) *Driver* has the meaning described in Section 51-03 of the Rules of the TLC.
- (e) *E-Hail App.* A Software program approved by the TLC residing on a smartphone which performs one or more of the following functions:
 - 1) allows a Passenger to identify the location(s) of available Taxicabs in a given area and allows a Driver to identify the location of a Passenger who is currently ready to travel;
 - 2) allows a Passenger to hail a Taxicab via the electronic device; and/or
 - 3) allows a Driver to receive a hail request from such a Passenger if the application provides for connecting a Passenger to a Driver.
- (f) *E-Hail App Provider or Provider* is the E-Hail Pilot Participant when authorized to offer an E-Hail App.
- (g) *E-Hail App Provider Authorization or Authorization.* The authorization issued to an E-Hail App Provider pursuant to this Agreement.
- (h) *E-Payment* means a feature of an E-Hail App that
 - 1) Allows a Passenger to pay through the E-Hail App; and
 - 2) Is limited to taxi fare, tip, and tolls charged to the Passenger by the E-Hail App.

E-Payment does not include payments through Digital Wallet Applications which pass payment data to T-PEP, do not receive fare information from T-PEP, and do not modify or edit the amount to be paid.

- (i) *Licensee.* When the term “Licensee” is used by itself, it refers to the holder of a License issued by the Commission that is NOT an Authorization issued under this Agreement.

- (j) *Modification of E-Hail App.* Any modification to the E-Hail App or related services after the Commission has issued an Authorization for such E-Hail App that would materially alter any of the following:
- (1) functionality, performance characteristics, security measures, or technical environment of the E-Hail App or related services;
 - (2) interfaces to T-PEP or to the Software, Hardware, network, or other E-Hail App components;
 - (3) the manner in which the E-Hail App or related services are provided.

The addition or modification of a component allowing payment through the E-Hail App constitutes a Modification.

A Modification of E-Hail App does not include:

- (4) fixes and/or maintenance patches necessary to conform the E-Hail App or any of its components or related services to the requirements set forth in §19 below; and
 - (5) security patches to the extent such fixes or patches are necessary in the E-Hail App Provider's good faith judgment to maintain the continuity of the E-Hail App or related services or to correct an event or occurrence that would, if uncorrected, substantially prevent, hinder or delay proper operation of the E-Hail App or related services.
- (k) *Passenger* has the meaning described in Section 51-03 of the Rules of the TLC.
- (l) *Passenger Information Monitor* has the meaning described in Section 51-03 of the Rules of the TLC.
- (m) *PCI Standards.* The Payment Card Industry Data Security Standards issued by the Payment Card Industry Security Standards Council as they may change from time to time. See www.pcisecuritystandards.org
- (n) *Service Levels.* The standards of performance of the E-Hail App and its components that are described in §§15 and 19 of this Agreement.
- (o) *T-PEP* has the meaning described in Section 51-03 of the Rules of the TLC.
- (p) *T-PEP Provider* has the meaning described in Section 51-03 of the Rules of the TLC.
- (q) Capitalized terms used herein which are not otherwise defined have the meanings provided in the Rules of the TLC

§ 2 Approval of Participation and Consequences of Termination

- (a) The Chair hereby authorizes the E-Hail App Provider to use, sell or lease the E-Hail App Provider's E-Hail App for use in connection with Taxicabs licensed by the Commission, subject to the terms hereof.
- (b) During the period when the E-Hail App Provider's Authorization is valid and in effect, the E-Hail App may be used by Drivers in Taxicabs licensed by the Commission consistent with the terms of this Agreement.
- (c) If the E-Hail App Provider's Authorization is revoked or terminated by the Commission, the E-Hail App Provider shall immediately notify each Licensee and Passenger who is using the E-Hail App approved under the revoked Authorization that:
- Any service agreement between a Licensee and the E-Hail App Provider will be deemed terminated as of the date of revocation or termination; and
 - The Licensee shall be blocked from continuing to use the E-Hail App.
- (d) Upon revocation or termination of the E-Hail App Provider's Authorization, the Provider shall not enter into any new or renewal service agreements with Licensees or Passengers for the use, sale, or lease in New York City of the E-Hail App approved under the revoked Authorization.
- (e) An E-Hail App Provider whose Authorization has been terminated or revoked shall cease offering the use, sale or lease in New York City of the E-Hail App to Licensees and/or Passengers.

§3 Authorization – Specific Requirements

- (a) *E-Hail App Approval for New Authorization.* The E-Hail App Provider agrees and understands that the Authorization for use of the Provider's E-Hail App is at sole the discretion of the Chair and is conditioned, among other things, on the E-Hail App and the E-Hail App Provider meeting, and continuing to meet, all the requirements and standards set forth in this Agreement. In addition, Authorization is conditioned on the E-Hail App Provider having submitted, and the Chair having approved, certain testing documentation as described in this section. In determining whether to approve the E-Hail App, the Chair will consider, in its sole discretion, whether the documentation required to be submitted by the E-Hail App Provider pursuant to subdivision (b) of this section

(as required) adequately demonstrates that the E-Hail App complies with all of the requirements set forth in Section 19 of this Agreement, or as such requirements may be waived or modified by the Commission pursuant to subdivision (g) of this section or Section 19 of this Agreement.

- (b) *Documentation for E-Hail App Approval.* The E-Hail App Provider has submitted with its application the following documentation if the E-Hail App includes E-Payment:
- (1) An acceptance test plan that uses information technology industry testing tools, techniques and methodologies designed to comprehensively test whether the E-Hail App and related services comply with all of the requirements set forth in §19 of this Agreement, or as such requirements may be waived or modified by the Commission pursuant to subdivision (g) of this section;
 - (2) Documentation demonstrating that an independent third party that is accredited by the American National Standards Institute-American Society of Quality National Accreditation Board (“ANAB”) to perform International Organization for Standardization (“ISO”) 9001 certifications has performed acceptance testing consistent with the acceptance test plan, and the successful results of the acceptance testing;
 - (3) A security test plan that uses information technology industry testing tools, techniques, and methodologies designed to comprehensively test whether the E-Hail App and related services comply with the security standards set forth in §19 of this Agreement, or as such standards may be waived or modified by the Commission pursuant to subdivision (g) of this section, and the successful results of the security testing.
 - (4) Documentation, to be renewed and resubmitted to the TLC every twelve (12) months if the Chair extends the E-Hail App Provider’s Authorization pursuant to Section 5 of this Agreement, demonstrating that an independent third party that is a Qualified Security Assessor (QSA) company has performed security testing of the E-Hail App and related services to determine compliance with the security standards set forth in §19 of this Agreement, or as such standards may be waived or modified by the Commission pursuant to subdivision (g) of this section, and the successful results of the security testing;
 - (5) The E-Hail App Provider will notify the Chair of any material mistakes, errors, inadequacies or changes in and to any of the required documentation.

The Chair may order additional testing in his or her discretion whenever he or she believes that the E-Hail App may not meet the requirements of Section 19 of this Agreement.

- (c) *Components of Approval.* The parties agree that the following must be completed in connection with E-Hail App Authorization:
 - (1) The E-Hail App Provider has submitted an application with all required documentation.
 - (2) The E-Hail App Provider has completed an interview with TLC staff and provided all requested follow up materials and additional testing.
 - (3) The proposed E-Hail App has been examined and/or tested by TLC staff.

- (d) *Modification of E-Hail App.* If after the E-Hail App Provider Authorization is issued pursuant to this Agreement, the E-Hail App Provider wants to implement a Modification, the E-Hail App Provider shall submit an application for approval of a Modification of E-Hail App by submitting all documentation required by subdivision (b) of this section (as required) and by completing all other components in subdivision (c) of this section. The Commission will treat the submission as an application for a new E-Hail App Provider Authorization. If the Commission approves the Modification, the existing E-Hail App Provider Authorization will apply to the modified E-Hail App.

- (e) *Required Insurance.* The E-Hail App Provider has submitted to the Chair proof of the insurance required in this subdivision when the Commission requests it. The E-Hail App Provider shall submit further proof at any time required by the Chair. The E-Hail App Provider agrees that it will notify the Chair of any change, cancellation or modification affecting the insurance required herein for which proof has been submitted. The E-Hail App Provider understands that the E-Hail App Provider Authorization will be terminated unless the Chair has acceptable proof of required coverage at all times. Upon submission of an application to renew an E-Hail App Provider Authorization, if such is permitted, the E-Hail App Provider shall provide to the Commission proof of the insurance required in this subdivision.
 - (1) Commercial General Liability Insurance.
 - (i) The E-Hail App Provider shall maintain Commercial General Liability (“CGL”) Insurance covering the E-Hail App Provider as Named Insured and the City as an Additional Insured in the amount of at least Five Million Dollars (\$5,000,000) per occurrence. Such insurance shall protect the City and the E-Hail App Provider from claims for property damage and/or bodily injury, including death that may arise from any of the operations

performed or to be performed by or on behalf of the E-Hail App Provider in connection with any of the activities authorized under this Agreement. Coverage under this insurance will be at least as broad as that provided by the most recently issued Insurance Services Office (“ISO”) Form CG 0001, and shall be "occurrence" based rather than “claims-made.”

- (ii) If the E-Hail App Provider’s subcontractor(s) is/are performing or will perform operations in connection with any of the activities authorized under this Agreement, either the E-Hail App Provider’s CGL Insurance under subparagraph (i) of this paragraph shall cover the subcontractor(s) or such subcontractor(s) shall maintain its/their own CGL Insurance subject to all other requirements herein.
 - (iii) Such CGL Insurance shall name the City, together with its officials and employees, as an Additional Insured with coverage at least as broad as the most recently issued ISO Form CG20 10.
- (2) Professional Liability Insurance.
- (i) In the Commission’s discretion, if professional services will be performed by the E-Hail App Provider in connection with any of the activities authorized under this Agreement, the E-Hail App Provider shall maintain and submit evidence of Professional Liability (“PL”) Insurance appropriate to the type(s) of services performed by the E-Hail App Provider in the amount of at least One Million Dollars (\$1,000,000) per claim. The policy or policies shall include an endorsement to cover the liability assumed by the E-Hail App Provider under this Agreement arising out of the negligent performance of professional services or caused by an error, omission or negligent act of the E-Hail App Provider or anyone employed by the E-Hail App Provider.
 - (ii) If the E-Hail App Provider’s subcontractor(s) is/are performing or will perform professional services in connection with any of the activities authorized under this Agreement for which PL Insurance is reasonably commercially available, either the E-Hail App Provider’s PL Insurance under subparagraph (i) of this paragraph shall cover the subcontractor(s) or such subcontractor(s) shall maintain its/their own PL Insurance subject to all other requirements herein.
 - (iii) Claims-made policies will be accepted for Professional Liability Insurance. All such policies shall have an extended reporting period option or automatic coverage of not less than two (2) years. If available as an option, the E-Hail App Provider shall purchase

extended reporting period coverage effective on cancellation or termination of such insurance unless a new policy is secured with a retroactive date, including at least the last policy year.

(3) Crime Insurance.

- (i) The E-Hail App Provider shall maintain crime insurance to protect against employee dishonesty, covering tangible property or moneys against loss, damage or destruction resulting from larceny, theft, embezzlement, forgery, robbery, misappropriation, willful misapplication or other fraudulent or dishonest acts committed by the E-Hail App Provider's employees or agents. The liability limits under the policy shall be at least One Million Dollars (\$1,000,000) per occurrence.
- (ii) If the E-Hail App Provider's subcontractor(s) is/are performing or will perform operations in connection with any of the activities authorized under this Agreement, either the E-Hail App Provider's crime insurance under item (i) above shall cover the subcontractor(s) employees or agents or such subcontractor(s) shall maintain its/their own crime insurance subject to all other requirements herein.

(4) General Requirements for Insurance Coverage and Policies.

- (i) All required insurance policies shall be maintained with companies that may lawfully issue the required policy and have an A.M. Best rating of at least A- / "VII" or a Standard and Poor's rating of at least A, unless prior written approval is obtained from the Commission.
- (ii) All insurance policies shall be primary (and non-contributing) to any insurance or self-insurance maintained by the City.
- (iii) The E-Hail App Provider shall be solely responsible for the payment of all premiums for all required insurance policies and all deductibles or self-insured retentions to which such policies are subject, whether or not the City is an insured under the policy.
- (iv) There shall be no self-insurance program with regard to any insurance required under this subdivision unless approved in writing by the Commission. Any such self-insurance program shall provide the City with all rights that would be provided by traditional insurance required under this subdivision, including but not limited to the defense obligations that insurers are required to undertake in liability policies.

- (v) The City's limits of coverage for all types of insurance required under this subdivision shall be the greater of:
 - (A) the minimum limits set forth in this subdivision; or
 - (B) the limits provided to the E-Hail App Provider as Named Insured under all primary, excess, and umbrella policies of that type of coverage.

(5) Proof of Insurance.

- (i) For each policy required under this subdivision, the E-Hail App Provider shall file a Declarations Page issued by the Insurer with the Commission. All Declarations Pages shall be:
 - (A) in a form acceptable to the Commission and certify the issuance and effectiveness of such policies of insurance, each with the specified minimum limits;
 - (B) accompanied by the endorsement in the E-Hail App Provider's Commercial General Liability Insurance policy by which the City has been made an Additional Insured pursuant to subparagraph (iii) of paragraph (1) of this subdivision; and
 - (C) accompanied by either a duly executed Certification by Insurer in the form provided by the Commission or copies of all policies referenced in the Declarations Page. If complete policies have not yet been issued, binders are acceptable, until such time as the complete policies have been issued, at which time such policies will be submitted.
- (ii) The E-Hail App Provider shall provide the Commission with a copy of any policy required under this subdivision upon demand by the Commission or the New York City Law Department.
- (iii) Acceptance by the Commission of a Declarations Page or a policy does not excuse the E-Hail App Provider from maintaining policies consistent with all provisions of this subdivision (and ensuring that subcontractors maintain such policies) or from any liability arising from its failure to do so.
- (iv) If the E-Hail App Provider receives notice, from an insurance company or other person, that any insurance policy required under this subdivision will expire, be cancelled, or terminated for any reason, the E-Hail App Provider shall immediately forward a copy of the notice to the Commission and the New York City Comptroller at:

NYC Taxi and Limousine Commission
Attn: General Counsel
33 Beaver Street 22nd Floor
New York, New York 10004

New York City Comptroller
Attn: Office of Contract Administration
Municipal Building, One Centre Street, Room 1005

New York, New York 10007.

(6) Miscellaneous Insurance Provisions.

(i) Whenever notice of loss, damage, occurrence, accident, claim or suit is required under a Commercial General Liability policy maintained in accordance with this subdivision, the E-Hail App Provider shall provide the insurer with timely notice thereof on behalf of the City. Such notice shall be given even where the E-Hail App Provider may not have coverage under such policy (for example, where one of the E-Hail App Provider's employees was injured). Such notice shall expressly specify that "this notice is being given on behalf of the City of New York as Additional Insured" and contain the following information:

- the number of the insurance policy;
- the name of the named insured;
- the date and location of the damage, occurrence, or accident;
- the identity of the persons or things injured, damaged, or lost; and
- the title of the claim or suit, if applicable.

The E-Hail App Provider shall simultaneously send a copy of such notice to:

The City of New York c/o Insurance Claims Specialist,
Affirmative Litigation Division,

New York City Law Department,

100 Church Street, New York, New York 10007.

If the E-Hail App Provider fails to comply with the requirements of this subparagraph, the E-Hail App Provider shall indemnify the City for all losses, judgments, settlements and expenses, including reasonable attorneys' fees, arising from an insurer's disclaimer of coverage citing late notice by or on behalf of the City.

(ii) Insurance coverage in the minimum amounts required in this subdivision shall not relieve the E-Hail App Provider of any liability for indemnification under this Agreement.

(iii) The E-Hail App Provider waives all rights against the City, including its officers and employees, for any damages or losses that are covered under any insurance required under this subdivision (whether or not such insurance is actually procured or claims are paid under such insurance) or any other insurance

applicable to the activities of the E-Hail App Provider and/or its subcontractors required to be authorized under this Agreement.

- (iv) If the E-Hail App Provider requires any subcontractor to procure insurance in connection with any of the activities authorized under this Agreement and requires the subcontractor to name the E-Hail App Provider as an additional insured under such insurance, the E-Hail App Provider shall ensure that such entity also names the City, including its officials and employees, as an additional insured with coverage at least as broad as the most recently issued ISO form CG 20 26.
- (f) *Renewals of Required Insurance Policies.* The E-Hail App Provider will submit to the Commission Certificates of Insurance confirming renewals of insurance before coverage of insurance policies required under subdivision (e) of this section expires. Certificates of Insurance shall comply with the requirements of subparagraph (e)(5)(i) above.
- (g) *Waivers or Modifications.* Except where expressly prohibited by law, the Chair may, in his or her discretion, waive or modify any requirements for Authorization under this Agreement in the interests of public safety and convenience. Requests for waivers or modifications shall be submitted in writing to the Chair.

§4 Liquidated Damages/Bond Required

- (a) *Amount of Bond.* The E-Hail App Provider shall deposit or have deposited with the Commission a fifty thousand dollar (\$50,000) bond per E-Hail App, payable to the City of New York. The bond must be provided by one or more sureties approved by the Chair. The bond must be provided before this Agreement becomes effective and must remain valid and in force until one year after the earlier of the date on which the E-Hail Pilot terminates or the date on which the E-Hail App Provider's participation is terminated or ends.
- (b) *Bond Guarantees.* The bond must guarantee that the E-Hail App Provider will pay all liquidated damages due to the Commission under this Agreement.
- (c) *Payment of Damages..* The Commission may draw upon the bond for payment of liquidated damages.
- (d) *Liquidated Damages.* The E-Hail App Provider recognizes that its non-compliance with the provisions of this Agreement will have a material adverse impact on the City in that it impacts the Commission and its constituents, and that the loss or damage resulting from such non-compliance is not susceptible of precise determination. The E-Hail App Provider agrees to pay to the City liquidated damages as directed by the Chair of \$ 1,000 for each occurrence of any non-compliance with the provisions of Sections 7, 13, 14, 15, 19, 20, and/or Appendix A to this Agreement, and \$100 for each occurrence of any non-

compliance with any other provisions of this Agreement. Such amounts, in view of the difficulty of accurately ascertaining the loss or damage suffered by the City, are fixed as the liquidated damages that the City will suffer by reason of such non-compliance, and not as a penalty.

- (e) *Restitution.* The E-Hail App Provider agrees that it is responsible to pay Drivers, other TLC Licensees, and Passengers, restitution, as applicable, for any harm caused by unauthorized use of their E-Hail App or E-Payment during the duration of the Pilot Program.

§5 Authorization Term

- (a) The Authorization is valid for the shorter of one year from the effective date of this Agreement or the end of the E-Hail Pilot.
- (b) Should the Commission determine to extend the term of the E-Hail Pilot, the Chair may renew the Authorization, in his or her sole discretion. This Agreement will apply to any renewed Authorization unless the Chair requires that the renewal be subject to a different agreement.

§6 Grounds for Termination

- (a) The Chair may, in his or her discretion, terminate this Agreement without cause on ten days prior written notice to the E-Hail App Provider.
- (b) The Chair may terminate this Agreement for cause on ten days prior written notice to the E-Hail App Provider when the Chair determines that the E-Hail App Provider:
 - (1) no longer meets the requirements for the E-Hail App Provider Authorization; or
 - (2) has failed to comply, or is no longer complying, with any of the terms of this Agreement.
- (c) The Chair shall terminate this Agreement immediately upon the termination of the E-Hail Pilot, which may be based on corroborated evidence that an E-Hail App or E-Payment authorized for use in the E-Hail Pilot creates a security, safety or other unacceptable risk to Medallion owners, Passengers or Drivers.

§7 General Requirements – Unauthorized Activity

- (a) *E-Hail App Provider Authorization Required.* The E-Hail App Provider shall not make available for use, sell, or lease an E-Hail App for use in New York City, or enter into or renew a service agreement with a Licensee or Passenger for the use, sale, or lease of an E-Hail App for use in New York City, that has not been authorized by the Commission.

(b) *E-Payment Authorization Required.* The E-Hail App Provider shall not use or permit the use of an electronic payment system in connection with an E-Hail App for use in New York City unless that system is an E-Payment that is a component of or linked to an E-Hail App that has been authorized by the Commission.

§8 General Requirements – Compliance with Applicable Law

- (a) *Licenses and Permits.* The E-Hail App Provider shall obtain licenses and permits required by applicable local law, state or federal law.
- (b) *Occupational Safety & Health Administration.* The E-Hail App Provider shall comply with all applicable Occupational Safety and Health Administration (OSHA) standards and requirements at the E-Hail App Provider place of business, as well as all other federal, state, and local laws governing its business.
- (c) *Payment of All Fines and Fees.* The E-Hail App Provider shall pay all fines, fees, and taxes it owes to any federal, state, or local governmental jurisdiction when they are due.
- (d) *Workers' Compensation Laws.* The E-Hail App Provider shall comply with all laws regarding workers' compensation and disability benefits, as well as all federal laws regarding the withholding of taxes and payment of FICA and other withholding taxes.

§9 General Requirements – Indemnification

- (a) *General Indemnification.* The E-Hail App Provider shall defend, indemnify and hold the City, its officers and employees harmless from any and all third-party claims (even if the allegations of the lawsuit are without merit) or judgments for damages on account of any injuries or death to any person or damage to any property and from costs and expenses (including reasonable attorneys' fees) to which the City, its officers and employees may be subjected or which it may suffer or incur allegedly arising out of any operations of the E-Hail App Provider and/or its employees, agents or subcontractors in connection with any of the activities authorized under this Agreement to the extent resulting from any negligent act of commission or omission, any intentional tortious act, or failure to comply with any of the provisions of this Agreement. Insofar as the facts or law relating to any third-party claim would preclude the City from being completely indemnified by the E-Hail App Provider, the City shall be partially indemnified by the E-Hail App Provider to the fullest extent permitted by law.
- (b) *Infringement Indemnification.* The E-Hail App Provider shall defend, indemnify and hold the City harmless from any and all third-party claims (even if the allegations of the lawsuit are without merit) or judgments for damages and from costs and expenses (including reasonable attorneys' fees) to which the City may be subjected or which it may suffer or incur allegedly arising out of or in connection with any infringement by the E-Hail App Provider, its agents or

subcontractors of any copyright, trade secrets, trademark or patent rights or any other property or personal right of any third party in the conduct of the authorized activities. Insofar as the facts or law relating to any third-party claim would preclude the City from being completely indemnified by the E-Hail App Provider, the City shall be partially indemnified by the E-Hail App Provider to the fullest extent permitted by law.

- (c) *Not Limited by Insurance.* The indemnification obligations set forth in this section shall not be limited in any way by the E-Hail App Provider obligations to obtain and maintain insurance as provided in §3 of this Agreement.

§10 General Requirements – False Statements Prohibited

- (a) The E-Hail App Provider shall not file with the Commission any statement that he or she knows or reasonably should know to be false, misleading, deceptive, or materially incomplete.

§11 General Requirements – Notice to TLC

- (a) *Material Change in Information.* The E-Hail App Provider shall notify the Commission of any material change in the information contained in its current E-Hail App Provider Authorization application or renewal if such is permitted. Material changes include, but are not limited to, changes to officers, directors, or the identities of persons holding interests of 1% or more in the E-Hail App Provider.
- (b) *Suspension or Revocation of License.* The E-Hail App Provider shall immediately notify the Commission in writing of any suspension or revocation of any license granted to the E-Hail App Provider, or any other person acting on his or her behalf, by any agency of the City or State of New York, or the government of the United States.

§12 Business Requirements – Mailing and Email Address

- (a) The E-Hail App Provider shall designate and provide the Commission the street address of its primary E-Hail App Provider location as its mailing address.
- (b) The E-Hail App Provider shall have and provide the Commission a working email address and telephone number at all times.
- (c) The E-Hail App Provider shall report any change of mailing address, email address and telephone number to the Commission in person or by mail within ten days.
- (d) Any communication from the Commission is sufficient if sent to the last mailing address provided by the E-Hail App Provider.

- (e) Any communication from the Commission is sufficient if sent by email to the last Email Address provided by the E-Hail App Provider.

§13 Business Requirements – Fees, Charges and Terms

(a) *Tips and Gratuities.*

- (1) The E-Hail App Provider shall not charge a Passenger a fee for a tip or gratuity unless:

- (i) The Driver receives the full amount of such tip or gratuity, without any withholding or sharing, and
- (ii) The Passenger can elect to change or withhold payment of such tip or gratuity.

- (2) The E-Hail App Provider cannot charge as a tip or gratuity (or using the words “tip” or “gratuity” or something similar) any fee that the Provider will retain.

(b) *Fares.* The E-Hail App and the E-Hail App Provider shall NOT charge any Passenger a fare for a trip that exceeds the fare as calculated by the Taximeter, permitted in §58-26 of the Rules of the TLC. The E-Hail App and the E-Hail App Provider may charge additional fees to a Passenger above the fare for the trip in accordance with subdivision (c) below so long as such fees are clearly delineated and not called a “fare”. NOTE: If an E-Hail App Provider charges a per-trip fee for use of the E-Hail App and if such fee is assessed on a per-trip basis and bundled into the same credit card transaction as the payment of the fare, the Provider is required to have the written agreement of a merchant of record permitting remittance of such fee to the E-Hail App Provider.

(c) *Notice of Fees.* The E-Hail App Provider shall provide Passengers and/or Drivers with reasonable notice of all Passenger and Driver fees and rates charged by the E-Hail App Provider for use of the E-Hail App, as applicable, including any variable or surge pricing policies, prior to Drivers’ or Passengers’ use of the E-Hail App for request of a trip. Additionally, the E-Hail App Provider shall provide Drivers and/or Passengers with reasonable notice of any modifications of such fees or rates, as applicable, prior to the effective date of the modifications.

(d) *File Fee Schedule.* The E-Hail App Provider shall file with the Commission a complete schedule of fees and rates charged to Passengers and/or Drivers for use of the E-Hail App, including any variable or surge pricing policies, and the fee structure (such as whether it is based on per-trip usage, or a monthly fee). The E-Hail App Provider shall also file with the Commission all updates of such schedule.

(e) *File User Agreement Terms.* The E-Hail App Provider shall file with the Commission all forms of the user agreements, use contracts and terms it requires for use, sale, and lease of the E-Hail App, both as to Passengers and Drivers. The E-Hail App Provider

must file with the Commission all updates of such documents and/or terms reflecting changes thereto.

§14 Business Requirements – Use of E-Hail App

All of the following conditions apply with regard to the E-Hail App Provider's making an E-Hail App available for use, sale or lease:

- (a) The E-Hail App Provider shall not make an E-Hail App available for use, sale or lease for use in New York City unless the E-Hail App has been authorized by the Chair pursuant to this Agreement and the E-Hail App to be used is identical to and is the E-Hail App that was authorized;
- (b) No modification shall be made to any Licensee's Vehicle to install a device on which the E-Hail App is to be used without the permission of the Chair.
- (c) The E-Hail App Provider shall not permit a Licensee to use and will block the use of the E-Hail App when the Chair has notified the E-Hail Provider to block a Licensee's use of the E-Hail App, until further notice by the Chair .
- (d) The E-Hail App Provider must provide written or electronic notification to Drivers who have registered to use the E-Hail App that a Driver must only use one device to access the E-Hail App and that that device must be mounted in a way that does not interfere with the Driver's view of the road or the Driver's or Passenger's view of the taximeter.

§15 Business Requirements –Payments

- (a) *Credit, Debit, and Prepaid Card Payment.* In addition to the requirements of §19(a) of this Agreement:
 - (1) An E-Hail App shall not provide a Driver compensation for a trip that exceeds the fare for the trip plus tolls and tip if any.
 - (2) An E-Hail App can permit Passengers to split a fare if this feature is provided by the T-PEP processing the fare payment.

§16 Business Requirements – Cooperation with the TLC

- (a) Upon request of the Chair, the E-Hail App Provider shall provide at no charge a fully operable demonstration of the E-Hail App and access by the Commission staff to the full range of features of the E-Hail App.

- (b) *Inspection by TLC.* The E-Hail App Provider shall ensure that an E-Hail App can be inspected and accessed by Commission personnel including for testing, including but not limited to testing of Driver and Passenger usage and functionality. For testing of Driver and Passenger usage, the E-Hail App Provider shall provide to TLC personnel appropriate IDs for Driver and Passenger credentials.
- (c) *Commission Ordered Testing.* In any instance where the E-Hail App Provider has failed to comply with any of the subdivisions above or any provision of Section 19 of this Agreement, the Chair may order the E-Hail App Provider to provide, within sixty (60) days:
- documentation demonstrating that subsequent to the non-compliance an independent third party with relevant expertise, acceptable to the Chair, has performed testing of the E-Hail App and related services to determine that the condition giving rise to the non-compliance has been corrected, and
 - certification by such third party of the successful results of such testing.

§17 Business Requirements – E-Hail App Provider Liability for Conduct of Employees

- (a) *Liability for Employee Conduct.* The E-Hail App Provider shall supervise and be responsible for the conduct of all of its employees, contractors, and agents for activities performed to carry out the requirements of this Agreement.
- (b) *Familiarizing Employees with Rules and Regulations.* The E-Hail App Provider shall ensure that all of its employees, contractors, and agents are fully familiar with all relevant regulatory agency rules and regulations.
- (c) *Compliance with Laws.* The E-Hail App Provider will ensure that all of its employees, contractors, and agents perform their duties in compliance with the Provider's obligations under this Agreement and all relevant federal, state, and city laws, rules, and regulations.

§18 Comply with Laws – Conduct Rules

- (a) *Acceptance of Gift or Gratuity.* The E-Hail App Provider or any person acting on his or her behalf shall not accept any gift, gratuity, or thing of value from an owner or driver of any vehicle licensed by the TLC or from anyone acting on behalf of an owner or driver for the purpose of not complying with any of the provisions of this Agreement or violating any of the rules of the TLC through acts of commission or omission.
- (b) *Reporting Requests for Gift or Gratuity.* The E-Hail App Provider, any person acting on the E-Hail App Provider's behalf, or any of the E-Hail App Provider's

employees shall immediately report to the Chair and the NYC Department of Investigation any request or demand for a gift, gratuity, or thing of value by any employee, representative, or member of the Commission or by any public servant.

- (c) *Offer of Gifts and Gratuities.* The E-Hail App Provider or any person acting on his or her behalf shall not offer or give any gift, gratuity, or thing of value to any employee, representative, or member of the Commission or to any other public servant.
- (d) *Reporting Offers of Gift or Gratuity.* The E-Hail App Provider shall notify the Chair immediately by telephone and in writing or email within 24 hours after receiving any offer of a gift or gratuity prohibited by subdivision (a) above.
- (e) *Fraud, Misrepresentation & Larceny.* The E-Hail App Provider, while performing his or her duties and responsibilities as an E-Hail App Provider, shall not commit or attempt to commit, alone or in concert with another, any act of fraud, misrepresentation, or larceny. Examples of fraud, larceny, or misrepresentation include, but are not limited to:
 - calibration of a fare other than that set by the Commission;
 - falsification of Trip Data.
- (f) *Willful Acts of Omission and Commission.*
 - (1) *Omission.* While performing the duties and responsibilities of an E-Hail App Provider, the E-Hail App Provider shall not deliberately fail to perform, alone or with another, any act where this failure is against the best interests of the public, although not specifically mentioned in this Agreement.
 - (2) *Commission.* While performing the duties and responsibilities of an E-Hail App Provider, the E-Hail App Provider shall not deliberately perform, alone or with another, any act that is against the best interests of the public, although not specifically mentioned in this Agreement.
- (g) *Notice of Criminal Conviction.*
 - (1) The E-Hail App Provider shall notify the Chair in writing within two (2) days after any criminal conviction of the Provider or any of the E-Hail App Provider's Business Entity Persons.
 - (2) Notification shall be in writing and shall be accompanied by a certified copy of the certificate of disposition of the conviction issued by the clerk of the court.

- (h) *Threats, Harassment, Abuse.* The E-Hail App Provider shall not threaten, harass, or abuse any governmental or TLC representative, public servant, or other person while performing his or her duties and responsibilities as an E-Hail App Provider.
- (i) *Use or Threat of Physical Force.* The E-Hail App Provider shall not use or attempt to use any physical force against a TLC representative, public servant, or other person while performing his or her duties and responsibilities as an E-Hail App Provider.
- (j) *Failure to Cooperate with Law Enforcement.* The E-Hail App Provider shall cooperate with all law enforcement officers and representatives of the TLC at all times.
- (k) *Failure to Cooperate with the Commission.* The E-Hail App Provider shall answer and comply as directed with all questions, communications, notices, directives, and summonses from the TLC or its representatives. The E-Hail App Provider shall produce his or her E-Hail App Provider Authorization and other documents whenever the TLC requires.

§19 Technical Requirements – E-Hail App

The E-Hail App Provider shall not permit an E-Hail App to be used in New York City unless it has been authorized by the Chair and it complies at all times with all of the requirements set forth in this section or as such requirements may be waived or modified by the Commission pursuant to §3(f) of this Agreement or this section.

- (a) *Payment*
 - (1) *Credit, Debit, and Prepaid Card Payment.* An E-Hail App that performs E-Payment shall conform to the following specifications:
 - (i) The E-Hail App shall offer the Passenger a receipt in accordance with paragraph (2) below; the receipt can be an electronic receipt.
 - (ii) Payment can be initiated at the beginning or made at the end of the trip, in accordance with §75-25(a)(2)(iv) of the Rules of the TLC.
 - (iii) An E-Hail App can offer pre-set payment options, including pre-set tip percentages, provided that the Passenger is permitted to change a pre-set tip percentage.
 - (iv) An E-Hail App cannot require a Passenger to pay a tip to the Driver.

- (2) The E-Hail App shall be able to generate an accurate receipt for payment of fare, regardless of the means of payment, and such receipt shall be offered to the Passenger. Upon the Passenger's request, a receipt either in hard copy form or in electronic form shall be transmitted to the Passenger. The receipt shall contain all the following information:
 - (i) All items required by §75-25(a)(2)(v) of the Rules of the TLC; and
 - (ii) Any extra fee paid by the Passenger to the E-Hail App Provider if paid directly to such Provider if such fee is assessed on a per-trip basis and bundled into the same credit card transaction as the payment of the fare. NOTE: §13(a) of this Agreement limits what can be considered a tip or gratuity.
 - (3) Any E-Payment technology used with any E-Hail App shall be integrated into the T-PEP used by any Licensee using the E-Hail App as required by § 19(b) of this Agreement including, but not limited to, ensuring the following: (i) that the fare charged for any trip is calculated by the taximeter and is processed by the T-PEP Provider through the T-PEP Provider's payment gateway; and (ii) that the E-Hail App provides to the T-PEP Provider relevant payment information necessary to process the transaction, display total charges including fare, tip, extras and service fees on the Passenger Information Monitor and on the printed receipts, and submit to the Chair a complete electronic trip record for the fare as further described in §19(c) of this Agreement.
 - (4) The E-Hail App which includes E-Payment shall comply with all applicable PCI Standards for E-Hail Payments. Credit, debit, and prepaid card information made through the E-Hail App will not be stored in the E-Hail App after the Driver has received authorization for use of the card.
- (b) *T-PEP Integration.* An E-Hail App which performs E-Payment shall integrate with T-PEP as follows:
- (1) The E-Hail App shall receive fare and Trip Data automatically from T-PEP and shall not permit a Driver or anybody else to enter any information manually. The E-Hail App also shall provide the T-PEP Provider with the following:
 - (i) Credit, debit, or prepaid card and payment information necessary to allow T-PEP Providers to process the transaction through their payment gateways, display total charges, including fare, tip and extras on the Passenger Information Monitor and on printed receipts, and allow submission to the Chair of a complete

electronic trip record for the fare as further described in §19(c) of this Agreement.

- (ii) Any other functionality but only if agreed to by the Commission, the E-Hail App Provider, and the T-PEP Provider.
- (2) All fares shall be calculated by the Taximeter and in accordance with the Rules of the Commission. An E-Hail App is NOT permitted to make a fare calculation independent of the Taximeter and must NOT permit a Driver to manually enter a fare.
 - (3) An E-Hail App must not provide a fee to the T-PEP Provider when the Passenger is using an E-Hail App which provides the Passenger's credit, debit or prepaid card and payment information to the T-PEP Provider for payment processing. In such instance, the E-Hail App Provider will not process payments for the trips.
 - (4) Any E-Hail App which performs E-Payment shall integrate (as described in subparagraph (b)(1)(i) above) with all T-PEP and the systems offered by all Authorized T-PEP Providers in use by Licensees using such E-Hail App. For purposes of §75-24 of the Rules of the TLC, an E-Hail App Provider whose E-Hail App performs E-Payment is a designee of the Commission.
 - (5) Notwithstanding the requirement of this subdivision (b) to integrate with T-PEP, the Chair, in his or her sole discretion, may waive this integration requirement in whole or in part if T-PEP cannot adequately support integration and the E-Hail App Provider has developed alternative means to:
 - protect Passengers against overcharging;
 - ensure that all trip related data is reported to the TLC; and
 - ensure that all trip based taxes and fees are collected.

Any waiver will be subject to an amendment to this Agreement, which may include provisions requiring payment of a service fee to T-PEP Providers to compensate for lost revenue.

- (c) *Trip Data Collection and Transmission.* An E-Hail App shall be capable of automatically collecting and transmitting to the Licensee's T-PEP the Trip Data as described below when E-Payment is used. The E-Hail App shall conform to the following specifications:

- (1) The E-Hail App shall be capable of automatically collecting and transmitting to T-PEP Trip Data as required in paragraph (2) below for all trips using E-Payment made during a shift.

(2) The Trip Data to be collected and transmitted shall include:

- (i) E-Hail App identifying number;
- (ii) E-Hail App-issued unique Passenger identifier
- (iii) credit/debit/pre-paid card type;
- (iv) first two and last four digits of the credit, debit, or prepaid card used for paying fares;
- (v) total itemized fare;
- (vi) tip amount;
- (vii) any Passenger service fee charged to the Passenger by the E-Hail App Provider if such fee is assessed on a per-trip basis and bundled into the same credit card transaction as the payment of the fare ;
- (viii) the number of Passengers that payment of the fare was split among if the E-Hail App permits the fare to be split.

The information specified in subparagraphs (ii) through (vi) must be reported for each passenger if there is a split fare.

(d) *Use Restrictions.* An E-Hail App shall conform to the following specifications:

- (1) The E-Hail App shall not operate:
 - (i) At John F. Kennedy International Airport;
 - (ii) At LaGuardia Airport; and
 - (iii) In any other geographic area specified by the Chair, including, as appropriate, areas with taxi lines or taxi staging areas.
- (2) The E-Hail App and the E-Hail App Provider shall ensure that:
 - An E-Hail request submitted from a location within the Manhattan Central Business District (defined as Manhattan south of 59th Street) can only be accepted by a Driver who is within 0.5 miles of such location.
 - An E-Hail request submitted from a location outside of the Manhattan Central Business District can only be accepted by a Driver who is within 1.5 miles of such location.
- (3) The E-Hail App shall only transmit requests for transportation or hails to a Driver who possesses a current and Valid Taxicab Driver's License and is operating a Vehicle currently and Validly licensed as a Taxicab.

- (4) The E-Hail App shall be available to a Licensee *ONLY* in compliance with §54-14 (e)(1) of the TLC's Rules or when the Vehicle is standing or stopped except that an E-Hail App can permit a Driver to accept an E-Hail request with a single touch.
- (5) The E-Hail App Provider must ensure that an E-Hail request transmitted to a Driver does not reveal the Passenger's desired destination.
- (6) The E-Hail App must ensure that no information about the Passenger is transmitted to a Driver, except that a Passenger's trip identification number or E-Hail App user name may be transmitted to the Driver after the Driver has accepted the Passenger's E-Hail request.
- (7) The E-Hail App Provider shall, upon receipt of notice from the Chair, prevent any Driver from using the E-Hail App at the time and for the period specified by the Chair.
- (8) The E-Hail App Provider's E-Hail App shall not remit to a Driver payment for a fare for a trip arranged by the E-Hail App.

(e) *Security.*

- (1) All features of the E-Hail App required by this section, including the collection, transmission and maintenance of data by the E-Hail App Provider, shall conform to applicable PCI Standards. Until the point at which PCI Standards are formally adopted for mobile payments, an E-Hail App which contains E-Hail Payment shall comply with all guidelines dictated by the PCI Security Standards Council.
- (2) An E-Hail App shall comply with TLC security standards attached to this Agreement as Appendix A.
- (3) The E-Hail App Provider shall not store credit, debit and prepaid card information received or processed through the E-Hail App after the Driver has received authorization for use of the card.
- (4) The E-Hail App Provider shall inform the TLC if it is required to make disclosures under State or Federal law regarding security breaches, including the New York State Information Security Breach and Notification Act (General Business Law section 899-aa).
- (5) The E-Hail App Provider shall immediately notify the TLC if it makes any Modifications to its TLC authorized E-Hail App or E-Payment service and shall not use the modified service in New York City until such Modification has been approved by the TLC.

§20 Reporting

(a) Every report required by this Agreement shall be submitted by the E-Hail App Provider in the form and format, and at the times and for the periods required by this Agreement or as instructed by the Chair if this Agreement does not specify a form, format and timing. All information in the report submitted must include a field indicating the name of the E-Hail App to permit the TLC to identify the origin of the information. Before submission of reports to TLC, the information contained in the report must be cleaned and validated to assess accuracy in accordance with an industry standard that is acceptable to the Chair.

(b) To enable the TLC to evaluate the E-Hail Pilot, the E-Hail App Provider shall submit a report to the TLC every week containing the following information for the prior week as required below. Such reports shall be in a standardized format and layout prescribed by the Chair that is open and non-proprietary, and shall be transmitted by secure transfer protocol in accordance with a format, layout, and procedure prescribed by the Chair. This information should be provided ONLY for trips provided by TLC-licensed Drivers in TLC-licensed Taxicabs and which occur within the New York City metropolitan area:

(1) Passenger Request Information

(i) The E-Hail App Provider shall provide a unique, anonymous identifier for a Passenger that can be used to link multiple trips requested by that Passenger.

(ii) For each Passenger trip request, the E-Hail App Provider shall provide:

- A unique request identifier
- date/timestamp and latitude, longitude and human-readable address for the location of the request
- number of Passengers (if recorded)
- type of vehicle requested (if this is an option)
- yes/no indicator for whether the trip request was ever accepted by a Driver (except broadcast models)

(iii) If using a “broadcast” model in the E-Hail App, the E-Hail App Provider shall provide the date/timestamp and latitude, longitude and human-readable address for the location when a broadcast is ended (if applicable).

(2) Driver E-Hail Acceptance Information (not relevant for broadcast-only model)

(i) For each Passenger trip request, the E-Hail App Provider shall provide an indicator of final trip status (e.g., not accepted, accepted and completed, accepted and cancelled by the Passenger or Driver, accepted and Passenger no-show, accepted and Driver does not show)

(ii) For each Passenger trip request accepted by a Driver, the E-Hail App Provider shall provide:

- number of Drivers that did not accept the request before it was accepted
- Medallion number of Vehicle and TLC License number of Driver who accepted the request
- date/timestamp and latitude, longitude and human-readable address for the location of Driver acceptance

(iii) For each Driver offered the trip by the E-Hail App who does not accept, the E-Hail App Provider shall provide:

- indicator of whether the trip was not accepted through active or passive action
- date/timestamp and latitude, longitude for the location of each Driver at time of non-acceptance
- Medallion number of Vehicle and TLC license number of each non-accepting Driver

(iv) When a Passenger cancels a trip request, the E-Hail App Provider shall provide:

- an indicator that the trip request was cancelled by the Passenger
- date/timestamp and latitude, longitude, and human readable address for the location of cancellation

(v) When a Driver cancels a trip that has been accepted, the E-Hail App Provider shall provide:

- an indicator that the trip was cancelled by the Driver
- date/timestamp and latitude, longitude, and human readable address for the location of cancellation

(3) Trip Information (not relevant for broadcast-only model)

For each Taxi trip initiated by use of the E-Hail App, the E-Hail App Provider shall provide:

- -date/timestamp and latitude, longitude and human-readable address for the location of actual pickup

- -date/timestamp and latitude, longitude and human-readable address for the location of actual drop-off
- trip time and trip distance

(4) Payment Information (applies only to E-Hail Apps that include E-Payment; not relevant for broadcast-only model)

(i) For each fare, the E-Hail App Provider shall provide:

- base metered fare (sum of \$2.50 drop plus \$0.50 increments), TLC time-based surcharges, itemized tolls, MTA tax, and tip amount.
- indicator for how Passenger selected tip amount (e.g., an automatic amount from the E-Hail App, mid-trip pre-set amount, manual selection at end of trip, cash/no tip).

(ii) For trip-associated E-Hail App fees for each trip, the E-Hail App Provider shall provide:

- the amount of the fee charged to Passenger and Drivers
- an indicator (or flag) if surge pricing was used for that trip
- fee structure indicator for Driver and Passenger (i.e., per trip, monthly, pre-paid, etc)

(iii) For each fare payment recorded by the E-Hail App, the E-Hail App Provider shall provide:

- an indicator of method of payment, such as cash, credit/debit/prepaid card, E-Hail App or other application, if applicable
- an indicator whether payment was auto-paid, paid during trip or after meter was disengaged
- indicator for whether the Passenger received a receipt from the E-Hail App.

(5) Passenger and Driver Download and Logon Data

(i)The E-Hail App Provider shall provide, on a weekly basis:

- Number of registrations for NYC market (by Drivers and by Passengers)
- Number of inactive (not accessed in past 60 days) accounts (by Drivers and by Passengers)

- Number of active (accessed in the past 60 days) accounts for the E-Hail App (by Drivers and by Passengers)

(ii) For each Driver authorized to use the E-Hail App, the E-Hail App Provider shall provide:

- Driver ID assigned by the E-Hail App
- TLC Driver license number for Driver
- date and timestamp of initial registration

- the number of weekly views of the E-Hail App by the Driver (that is, when the E-Hail App is not in the background on the access equipment)

(iii) For each Passenger authorized to use the E-Hail App, the E-Hail App Provider shall provide:

- unique Passenger ID assigned by the E-Hail App
- date and timestamp of initial registration by the Passenger
- the number of weekly views of the E-Hail App by the Passenger (that is, when the E-Hail App is not in the background on the access equipment)

(iv) For each Driver logon to the E-Hail App or “on duty” event recorded, the E-Hail App Provider shall provide:

- Medallion number of the Vehicle being operated by the Driver
- date/timestamp and latitude, longitude, and human-readable address for the location of logon

(v) For each Driver logoff from the E-Hail App, the E-Hail App Provider shall provide:

- date/timestamp and latitude, longitude, and human-readable address for the location of logoff

(vi) When a Driver or Passenger deregisters or otherwise terminates usage of the E-Hail App, the E-Hail App Provider shall provide

- date and timestamp
- reason for deregistration (if provided)

(6) Subscription Plan Data

For each E-Hail App user (Drivers and Passengers) and for each change in subscription plan, the E-Hail App Provider shall submit:

- user type (Passenger or Driver)
- unique Passenger identifier (for Passengers)
- TLC Driver License Number (for Drivers)
- subscription plan type (e.g., monthly, weekly, pay-as-you-go) determined by the E-Hail App Provider
- date/timestamp for start of subscription plan
- date/timestamp for end of subscription plan

(c) The E-Hail App Provider shall submit to the TLC each month a summary of all Passenger and Driver complaints received in the prior month in a form and format as prescribed by the Chair, which summary includes the following:

- date and timestamp for filing of each consumer complaint
- complainant type (e.g., Driver, Passenger or other)
- indicators describing nature of consumer complaint (e.g., driver no-show, suspected overcharge, etc.)
- raw text describing consumer complaint
- unique, anonymous identifier for customer who complained (should be Passenger ID assigned by Provider if Passenger complaint)
- date and timestamp for when incident occurred (if complaint relates to particular event)
- Medallion number of Vehicle involved with the complaint (if complaint related to a particular trip)
- TLC License number of Driver against whom complaint was filed (if complaint related to a Driver or particular trip)
- unique identifier for Passenger trip request (should be trip ID assigned by the Provider if complaint is related to a particular trip request)

(d) The E-Hail App Provider shall submit to the TLC each month a report for activity for the prior month with the following information, in a form and format, and including such fields, as prescribed by the Chair:

- Itemized total revenue from usage of the E-Hail App in New York City, including revenue generated from usage fees paid by Passengers or Drivers and revenues generated from third parties, such as advertising.
- For an E-Hail App for which Drivers or users are charged on a non-per-trip basis (e.g., monthly or weekly fee), information on how much is being charged.

(e) Upon request of the Chair, the E-Hail App Provider shall conduct Passenger Surveys through use of the E-Hail App, shall provide access to the E-Hail App to the Chair to conduct Passenger surveys, and shall provide survey responses to the Chair.

(f) No later than two months after the E-Hail App Provider ceases to operate under the E-Hail Pilot, it must submit to the Chair a program summary report including a summary of the data required to be submitted by this Agreement. The report should also include the results of the use of the E-Hail App, any recommendations by the Provider as to the use of electronic applications for Taxicabs and other vehicles for hire, and any suggestions for possible rule-making.

(g) Use of Data. All reports and data transmitted to the TLC under this Agreement may be used by the TLC for any internal purpose and the TLC may make the data and reports publicly available for use by the general public and by third parties and as required by applicable law.

(h) The E-Hail App Provider shall maintain all of the data required by this Agreement for at least three years after the date on which the Provider commences providing E-Hail App services pursuant to the E-Hail Pilot.

§21 Miscellaneous Provisions

(a) **Modifications.** All modifications to this Agreement must be in writing signed by both parties.

(b) **Merger.** This Agreement shall constitute the entire agreement between the parties and any prior understanding or representation, oral or written, relating to the subject matter hereof preceding the date of this Agreement shall not be binding upon either party and is superseded hereby.

(c) **Counterparts.** This Agreement may be executed in as many counterparts as may be required, each of which when delivered is an original but all of which taken together constitute one and the same instrument.

- (d) **Further Assurances.** The parties will execute and deliver all such further endorsements, instruments, agreements, and other documents and take all such further actions as the other party may reasonably request from time to time in order to effectuate the terms, purposes, and intent of this Agreement.
- (e) **Interpretation.** Whenever the context requires, the singular includes the plural and vice versa and each gender includes the other gender. The headings of the sections of this Agreement are for convenience only and do not limit their provisions.
- (f) **Assignment.** Neither party may assign this Agreement or any of the rights hereunder or delegate any of its obligations hereunder, without the prior written consent of the other party, and any such attempted assignment shall be void.
- (g) **Third Party Beneficiary.** Except as expressly set forth in this Agreement, the parties do not intend the benefits of this Agreement to inure to any third party, and nothing contained herein shall be construed as creating any right, claim or cause of action in favor of any such third party, against either of the parties hereto.
- (h) **Severability.** In the event that any covenant, provision or restriction contained in this Agreement is found to be void or unenforceable (in whole or in part) by a court of competent jurisdiction, it shall not affect or impair the validity of any other covenant, provisions or restrictions contained herein, nor shall it affect the validity or enforceability of such provisions in any other jurisdiction or in regard to other circumstances. Any covenants, provisions or restrictions found to be void or unenforceable are declared to be separate and distinct, and the remaining covenants, provisions and restrictions shall remain in full force and effect.
- (i) **Waiver.** The failure of either party to insist upon strict compliance with any of the terms, covenants or conditions of this Agreement shall not be deemed a waiver by that party of that term, covenant or condition or of any other term, covenant or condition of this Agreement.
- (j) **Governing Law.** This Agreement shall be governed by the laws of the State of New York without reference to its principles of conflict of laws. E-Hail Pilot Participant and the Commission irrevocably consent and submit to personal jurisdiction in the courts of the State of New York located in the City and County of New York for all matters arising under this Agreement.
- (k) **Notices.** Any notice provided for or concerning this Agreement shall be in writing and deemed received when sent by overnight delivery service or certified or registered mail, return receipt requested, if sent to the address below:

For E-Hail Pilot Participant:

The New York City Taxi and Limousine Commission:
33 Beaver St., 22nd Floor
New York, NY 10004
c/o David Yassky, Chair/Commissioner

IN WITNESS WHEREOF, the parties hereto have executed these Terms and Conditions and consent to the provisions contained herein on the date indicated.

By:
Title:

Date

Meera Joshi
Deputy Commissioner for Legal Affairs
New York City Taxi & Limousine Commission

Date

Approved by the NYCTLC on the ____ this day of _____.

Approved as to Form:

Acting Corporation Counsel

Appendix A

Table of Contents

§1	Scope of Appendix A	34
§2	Definitions Specific to Appendix A	34
§3	Information Security Requirements	35

§1 Scope of Appendix A

- (a) To establish the Commission's information security requirements for the collection, transmission, processing, maintenance, and storage of E-Hail App Data and TPEP Data by E-Hail App Providers, their employees, agents and subcontractors.
- (b) The information security requirements set forth in this Appendix apply to E-Hail Apps, all Information System Components, E-Hail App Data and TPEP Data, and all related services provided by E-Hail App Providers, their employees, agents and subcontractors to carry out the activities authorized under this Agreement.

§2 Definitions Specific to Appendix A

- (a) *Application.* A computer program designed for a specific use or task and includes all software applications whether custom or off-the-shelf, including internal and external (web) applications.
- (b) *Database.* An organized collection of data, typically in digital form.
- (c) *Database Management System.* A software package with computer programs that control the creation, maintenance and use of a database.
- (d) *DOITT Standards.* The Department of Information Technology and Telecommunications Citywide Information Security Policy for Service Providers and Encryption Standards, found at <http://www.nyc.gov/html/doitt/html/business/security.shtml>.
- (e) *E-Hail App Data.* All data required to be collected, transmitted and maintained pursuant to this Agreement. E-Hail App Data includes, but is not limited to, Trip Data as described in §19(c) of this Agreement, data related to credit, debit, and prepaid card transactions, and data relating to E-Hail App usage as described in §20 of this Agreement. Any data that is transferred to the E-Hail App by TPEPs become E-Hail App Data once received by the E-Hail App.
- (f) *Information System* means the same as the same term in §75-03 of Commission Rules.
- (g) *Information System Component* includes any Network Component, Server, Agent, or Application included in, or connected to, the E-Hail App and/or E-Hail App Data and TPEP Data environment.
- (h) *TPEP Data.* All data required to be collected, transmitted and maintained pursuant to §75-25 of Commission Rules and other information assets related to the TPEP Data. TPEP Data includes, but is not limited to, Trip Data, data related to credit, debit and prepaid card transactions, and text messages and the date and time such messages were sent and received. Any data that is transferred to the

TPEP by E-Hail Apps that provide E-Payment become TPEP Data once received by the TPEP.

- (i) *Network Component* includes all firewalls, switches, routers, wireless access points, network appliances, and other security appliances.
- (j) *Non-consumer User*. Any individual, excluding a cardholder, who accesses Database Management System components, including, but not limited to employees, administrators and third parties.
- (k) *Personal Information* means the same as the same term in §75-03 of Commission rules.
- (l) *Security Incident or Incident* means the same as the same term in §75-03 of Commission Rules.
- (m) *Security Policy*. The information security policy and procedures established by an E-Hail App Provider that comply with the requirements in §3 of this Appendix.
- (n) *Server*. A physical computer hardware system dedicated to running one or more services at the requests of other programs or agents including but not limited to web, database, authentication, Domain Name System, mail proxy, and Network Time Protocol.
- (o) *Trip Data* means the same as the same term in §51-03 of these Rules.

§3 Information Security Requirements

- (a) *Information Security Policy*.
 - (1) *Establish Information Security Policy (Security Policy)*. Prior to system design, the E-Hail App Provider must establish, maintain, and disseminate to its employees and relevant third parties such as agents and subcontractors, their information security policy and procedures that comply with all of the requirements in this section. The E-Hail App Provider must require employees to acknowledge in writing they have read and understood the Security Policy.
 - (2) *Responsibilities of E-Hail App Providers and Employees*. The Security Policy must clearly define the information security responsibilities of the E-Hail App Provider, its employees, and related third parties such as agents and subcontractors.
 - (3) *Management Responsibilities*. The E-Hail App Provider must assign to an individual or team the following information security management responsibilities:

- (i) Establish, document, and distribute the Security Policy;
 - (ii) Monitor and analyze security alerts and information, and distribute to appropriate personnel;
 - (iii) Establish, document, and distribute Security Incident response and escalation procedures to ensure timely and effective handling of all situations;
 - (iv) Administer user accounts, including additions, deletions, and modifications; and
 - (v) Monitor and control all access to data.
- (4) *Screen Employees.* The E-Hail App Provider must screen potential employees to minimize the risk of attacks from internal sources.
 - (5) *Requirements for Third Party Access.* The E-Hail App Provider must require all third parties, such as agents and subcontractors (other than individuals who are solely users of the E-Hail App), with access to the E-Hail App, TPEP, Information System Components, E-Hail App Data, or TPEP Data, or who are involved in any related services provided by the E-Hail App Provider in carrying out the activities authorized under this Agreement, to agree in writing and demonstrate compliance with the Security Policy and all security requirements in this section.
 - (6) *Incident Response Plan.* The E-Hail App Provider must implement a Security Incident response plan that, at a minimum, requires the E-Hail App Provider to respond immediately to a system breach. The plan must:
 - (i) Contain specific Incident response procedures, business recovery and continuity procedures, data backup processes, roles and responsibilities, and communication and contact strategies;
 - (ii) Be tested at least annually;
 - (iii) Designate specific personnel to be available on a 24/7 basis to respond to alerts;
 - (iv) Provide appropriate training to staff with Security Incident response responsibilities;
 - (v) Include alerts from intrusion detection, intrusion prevention, system logs, and file integrity monitoring systems;
 - (vi) Contain a process to modify and evolve the Incident response plan according to lessons learned and to incorporate industry developments; and
 - (vii) Require notification to the Commission of Security Incidents within 2 hours of occurrence.

- (b) *Authentication.* The E-Hail App Provider must provide a process that verifies a user's identity to ensure that the person requesting access to a system is the person to whom entry is authorized.
- (c) *Copyright Compliance.* The E-Hail App Provider must comply with the terms of all software licenses and may not use any software in any form that has not been legally purchased or otherwise legitimately obtained.
- (d) *Database Management Systems.* The E-Hail App Provider must develop and implement appropriate controls and procedures to ensure that the Database Management Systems are adequately protected.
- (e) *Access to E-Hail App Data, TPEP Data and Computing Resources.*
 - (1) *Limit Access.* The E-Hail App Provider must limit access to E-Hail App Data and TPEP Data and related computing resources to only those individuals and processes (i) whose responsibilities are described by the Commission, and (ii) required to have access by the E-Hail App Provider.
 - (2) *Restrict Access.* The E-Hail App Provider must establish a mechanism for systems with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.
 - (3) *Account Management.* To ensure proper user authentication and password management for Non-consumer Users and administrators on all system components, the E-Hail App Provider must:
 - (i) Control the addition, deletion, and modification of user IDs, credentials, and other identifier objects;
 - (ii) Immediately revoke accesses of terminated users;
 - (iii) Remove inactive user accounts at least every ninety (90) days;
 - (iv) Enable accounts used by vendors for remote maintenance only during the time needed;
 - (v) Distribute and enforce password procedures and policies to all users who have access to E-Hail App Data or TPEP Data and related computing resources;
 - (vi) Authenticate all access to any database containing E-Hail App Data or TPEP Data, including access by applications, administrators, and all other users.
 - (4) *Restrict Physical Access.* The E-Hail App Provider must restrict physical access to E-Hail App Data and TPEP Data and related computing resources as follows:

- (i) Any physical access to data or systems that house E-Hail App Data or TPEP Data, allows the opportunity to access devices or data, and/or removes systems or hardcopies, must be appropriately restricted.
- (ii) The E-Hail App Provider must ensure that employees and visitors are authorized before entering areas where E-Hail App Data or TPEP Data is collected, transmitted, processed, maintained or stored.
- (iii) The E-Hail App Provider must use a visitor log to retain a physical audit trail of visitor activity, and retain this log for a minimum of three (3) months, unless otherwise restricted by law.
- (iv) The E-Hail App Provider and any subcontractor(s) who is/are performing or will perform services in connection with any of the activities required under this Agreement must physically secure all paper and electronic media (e.g., computers, electronic media, networking and communications hardware, telecommunication lines, paper receipts, paper reports, and faxes) that contain E-Hail App Data or TPEP Data.
- (v) The E-Hail App Provider must maintain strict control over the internal or external distribution of any kind of media that contains E-Hail App Data or TPEP Data, including:
 - (A) Labeling the media so it can be identified as confidential; and
 - (B) Sending the media via secured courier or a delivery mechanism that can be accurately tracked and is not accessible during transit.
- (vi) The E-Hail App Provider must maintain strict control over the storage and accessibility of media that contains E-Hail App Data or TPEP Data including properly inventorying all media and making sure it is securely stored.
- (vii) The E-Hail App Provider must destroy media containing E-Hail App Data or TPEP Data when it is no longer needed for business or legal reasons including:
 - (A) Cross-cut shredding, incinerating, or pulping hardcopy materials; and
 - (B) Purging, degaussing, shredding, or otherwise destroying electronic media so that E-Hail App Data or TPEP Data cannot be reconstructed.

(f) *Firewalls.*

- (1) *Firewall Configuration.* A firewall must control access between internal networks and external networks. All firewalls used in the E-Hail App Provider's systems must be configured by the E-Hail App Provider to:
 - (i) Block all data traffic (subject to the protocol limitations of the firewall) except that traffic which is explicitly allowed; direct incoming traffic to trusted internal systems; and protect vulnerable systems;
 - (ii) Prevent disclosure of information such as system names, network topology, and network device types; and
 - (iii) Support network layer authentication, with both the firewall and the network layer authentication to be used in conjunction with standard application authentication methods.
- (2) *External Firewall Connections and Changes.* The E-Hail App Provider must establish a formal process for approving and testing all external network connections and changes to the firewall configuration.
- (3) *Periodic Review.* The E-Hail App Provider must conduct a periodic review of firewall/router rule sets.
- (4) *Exceptions to Denial of Untrusted Networks/Hosts.* The E-Hail App Provider must build a firewall configuration that denies all traffic from "untrusted" networks/hosts, except for:
 - (i) Web protocols - Secure Sockets Layer (SSL) (port 443);
 - (ii) System administration protocols (e.g., Secure Shell (SSH) or Virtual Private Network); and
 - (iii) Other protocols required by the business (e.g., for ISO 8583).
- (5) *Restricting Connections between Publicly Accessible Servers and E-Hail App Data or TPEP Data.* The E-Hail App Provider must build a firewall configuration that restricts connections between publicly accessible servers and any system component storing E-Hail App Data or TPEP Data, including any connections from wireless networks. This firewall configuration must include:
 - (i) Restricting inbound and outbound Internet traffic to ports 22 and 443;
 - (ii) Securing and synchronizing router configuration files (e.g., running configuration files which are used for normal running of

the routers, and start-up configuration files which are used when machines are re-booted, must have the same, secure configuration);

- (iii) Denying all other inbound and outbound traffic not specifically allowed;
- (iv) Installation of personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (e.g., laptops used by employees), which are used to access the organization's network;
- (v) Prohibiting direct public access between external networks and any system component that stores E-Hail App Data or TPEP Data (e.g., databases);
- (vi) Filtering and screening all traffic to prohibit direct routes for inbound and outbound Internet traffic;
- (vii) Restricting outbound traffic from sensitive applications to authorized IP addresses; and
- (viii) Implementing IP masquerading to prevent internal addresses from being translated and revealed on the Internet. The E-Hail App Provider must use technologies that implement RFC 1918 address space, such as Port Address Translation or Network Address Translation.

(g) *Host and Server Systems.* The E-Hail App Provider must configure host and server systems with sufficient security features to ensure that E-Hail App Data and TPEP Data are adequately protected from unauthorized use, disclosure, modification, destruction, and denial of service.

(h) *Local Area Networks.* The E-Hail App Provider must configure local area networks ("LANs") with sufficient security features to ensure that E-Hail App and TPEP Data are adequately protected from unauthorized use, disclosure, modification, destruction, and denial of service.

(i) *Network Management.*

- (1) *Appropriate Access.* The E-Hail App Provider must implement controls over all such devices and platforms so that only appropriate resources, agents, and individuals may access the network. The E-Hail App Provider must also implement appropriate architectures, procedures, management assignments, and back-up and recovery plans to provide such controls.
- (2) *Monitor All Access.* The E-Hail App Provider must track and monitor all access to network resources and E-Hail App Data and TPEP Data.

- (3) *Linking Access to System Components.* The E-Hail App Provider must establish a process for linking all access to system components (especially those done with administrative privileges such as root) to an individual user.
 - (4) *Automated Audit Trails.* The E-Hail App Provider must implement automated audit trails to reconstruct the following events for all system components:
 - (i) All individual user access to E-Hail App Data or TPEP Data;
 - (ii) All actions taken by any individual with root or administrative privileges;
 - (iii) Access to all audit trails;
 - (iv) Invalid logical access attempts;
 - (v) Use of identification and authentication mechanisms;
 - (vi) Initialization of the audit logs; and
 - (vii) Creation and deletion of system-level objects.
 - (5) *Synchronize Times.* The E-Hail App Provider must synchronize all critical system clocks and times.
 - (6) *Secure Audit Trails.* The E-Hail App Provider must secure audit trails so they cannot be altered.
 - (7) *Review Logs.* The E-Hail App Provider must review logs for all system components. Log reviews must include those servers that perform security functions (like intrusion detection systems) and authentication, authorization and accounting servers (e.g., Diameter).
 - (8) *Retain Audit Trail History.* The E-Hail App Provider must retain audit trail history for a period that is consistent with its effective use, as well as all applicable law, rules and regulations.
- (j) *Wireless Networks.* At a minimum, dynamic Wi-Fi Protected Access must be used by the E-Hail App Provider for any portion of the network or system that includes 802.11x, or similar technology.
- (k) *Personal Information.* All E-Hail App Provider employees, agents or subcontractors or employees of such agents or subcontractors with access to Personal Information are required to maintain the confidentiality of Personal Information.
Personal Information:

- (1) Must only be used for the stated purpose for which it was gathered, and
- (2) May not be shared or disclosed, except for lawful purposes.

(l) *Fraud Prevention.* The E-Hail App Provider must ensure that controls are developed and implemented into the E-Hail App, Information System Components and any software contained therein to prevent the possibility of fraud, and to ensure that the E-Hail App and TPEP Data are adequately protected. This protection must address and prevent both malicious and inadvertent damage by the general user community, as well as authorized users.

(m) *Security Incident Management.*

(1) *Reporting Security Incidents.* The E-Hail App Provider must develop a procedure for reporting observed or suspected Security Incidents, threats, weaknesses, or malfunctions that may have an impact on the security of the E-Hail App, Information System Components and any software contained therein, and E-Hail App Data and TPEP Data. All such observed or suspected Security Incidents, threats, weaknesses, or malfunctions must be reported to the Commission within two (2) hours of when the E-Hail App Provider knows of or should have known of such Security Incidents, threats, weaknesses or malfunctions.

(2) *Security Incident Management Procedures.* The E-Hail App Provider's Security Incident management responsibilities and procedures must be clearly defined and documented to ensure an immediate, effective, and orderly response to Incidents. At a minimum, these procedures must address:

- (i) Information system failures and loss of service;
- (ii) Denial of service;
- (iii) Errors resulting from incomplete or inaccurate data;
- (iv) Breaches of confidentiality; and
- (v) Loss of integrity of the E-Hail App, E-Hail App Data, TPEP Data, Information System Components or any software contained therein.

(3) *Security Incident Response Procedures.* In addition to normal contingency plans designed to recover systems or services, the Security Incident response procedures must also cover:

- (i) Analysis and identification of the cause of the Incident;

- (ii) Planning and implementation of corrective actions to prevent reoccurrence;
- (iii) Collection of audit log information;
- (iv) Communication with those affected by or involved in the recovery from the Incident; and
- (v) Reporting and escalation (as appropriate) of Incidents.

(n) *Security Staffing.* The E-Hail App Providers and their agents or subcontractors must employ staff familiar with generally accepted baseline security practices and methodologies in connection with their performance under this section. These resources must have oversight responsibilities for compliance with this section and be able to articulate and direct secure solutions to protect the infrastructure and the underlying data.

(o) *Criminal Activity.* The E-Hail App Provider must report all instances of suspected criminal activity to the Commission and the Agency Inspector General Office at the New York City Department of Investigation within twelve (12) hours of when the E-Hail App Provider knows of or should have known of such instances of suspected criminal activity.

(p) *Logging and Administration.* All E-Hail App, Information System Components and any software contained therein provided by or for the E-Hail App Provider must enable appropriate logging and auditing capabilities.

(q) *Anti-Virus Security Policy.*

- (1) *Commercial Anti-virus Software.* Servers, desktops, and laptops must have current commercial anti-virus software installed, properly configured and running at all times.
- (2) *Remove the Virus.* Anti-virus software must be configured to automatically remove the virus.
- (3) *Users Not to Disable Anti-virus Software.* Users must not disable automatic virus scanning on their local machines.
- (4) *Administrators Not to Disable Anti-virus Software.* Server administrators must not disable anti-virus software on server machines.
- (5) *Signature Updates.* When possible, signature updates must be installed without user intervention.
- (6) *Virus Signature Files.* New versions of the virus signature files must be loaded within forty-eight (48) hours.

- (7) *Affected Devices.* All virus alerts must be followed by an immediate full scan of affected devices performed by appropriate IT personnel.
 - (8) *Root Cause Investigation.* The E-Hail App Provider's administrators must perform a root cause investigation when a virus is identified to ensure proper containment.
- (r) *Application Development Security Policy.*
- (1) *Security Requirements Analysis.* A comprehensive security requirements analysis must be performed for all new systems and for significant upgrades to existing systems.
 - (2) *Best Practice Standards.* System security requirements and specifications must be compliant with industry best practice standards for technologies and system configuration.
 - (3) *Interoperability.* System security requirements and specifications must ensure secure interoperability with all information sources and services with which it must interface.
 - (4) *Integration.* System security requirements and specifications must ensure integration with existing security services where applicable.
 - (5) *Production Environment.* The production environment must not be used for development or testing activities.
 - (6) *Functionality.* All security functionality must be operational during formal acceptance and operational testing.
 - (7) *Testing of New Application.* Prior to production release of any new application, testing must be done to ensure the new application will not adversely affect any existing systems.
 - (8) *Back Out Plan.* Each application must have a defined back out plan in the unlikely event that its migration to the production environment causes service degradation.
 - (9) *Disaster Recovery Program.* Each new application must create a business continuity and disaster recovery program in accordance with the business significance of the application.
- (s) *Digital Media Re-use and Disposal Policy.*
- (1) *Rendering Information Permanently Unreadable.* Where any equipment containing digital media is to be discarded, donated, sold or otherwise transferred to an external person, organization or vendor (e.g. at the end of a lease or as an RMA (returned merchandise), the E-Hail App Provider

must use one of the following approved methods appropriate for rendering all information on the media permanently unreadable:

- (i) A data wiping program that will securely delete all data by methods that irreversibly wipe the physical area of storage (rather than simply removing the disk-directory reference to that information). The program should overwrite all addressable locations with a character, its complement, then a random character;
 - (ii) Any full disk encryption method which is compliant with the DOITT Standards and in which it can be reasonably expected that no unauthorized person has the ability to decrypt the data; or
 - (iii) Degaussing and/or physical media shredding technology which meets NIST standard 800-88 (or its successor). See http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf
- (2) *Transfer of Asset for Disposal.* An asset can be securely transferred for disposal to a vendor who has contractually committed to following one or more of the above methods.
- (t) *Encryption Policy.*
- (1) *Approved Algorithms.* Only approved cryptographic algorithms and supporting processes as described in the DOITT Standards found at <http://www.nyc.gov/html/doitt/html/business/security.shtml> must be used to protect business critical information.
 - (2) *Confidential Data at Rest.* Where technology permits, private or confidential data at rest must be protected by encryption. The use of password protection instead of encryption is not an acceptable alternative to protecting sensitive information.
 - (3) *Private or Confidential Data.* Data categorized as private or confidential must not be transitioned to removable media without Commission approval.
 - (4) *Removable Media.* Removable media including CDs, backup tapes, and USB memory drives that contain private or confidential data must be encrypted and stored in a secure location.
 - (5) *Transfer of Removable Media.* When transferring removable media, the receiver must be identified to ensure the person requesting the data is a valid recipient.
 - (6) *Emails.* All emails containing data classified as private or confidential must be encrypted.

- (7) *Unencrypted Transmission.* Unencrypted transmission of private or confidential data in any way (e.g. through the use of web applications or File Transfer Protocol) is not allowed.
 - (8) *Wireless Networks.* Wireless networks must be encrypted in accordance with DOITT Standards.
 - (9) *Storage of Private or Confidential Data.* Private or confidential data may only be stored on portable devices such as laptops, smart phones and personal digital assistants (PDAs) when encrypted.
 - (10) *Portable Devices.* Portable devices must not be used for long-term storage of private or confidential data.
 - (11) *Remote Wipe.* Where it is technologically feasible, portable devices must have the capability to be remotely wiped in the event of theft or accidental loss.
 - (12) *Protections for Portable Devices.* Portable devices must have proper protections in place.
 - (13) *Approved Encryption Algorithms.* Approved encryption algorithms must be a minimum key length of 128 bits.
 - (14) *Private Keys.* Private keys must be kept confidential.
 - (15) *Key Management.* Key lifecycle management must be implemented.
 - (16) *Keys in Storage and Transit.* Keys in storage and transit must be encrypted.
 - (17) *Key Choice.* Keys must be chosen randomly from the entire key space, and weak keys must never be used.
 - (18) *Encryption Keys.* Encryption keys must allow for retrieval for administrative or forensic use.
- (u) *Password Policy.*
- (1) *Passwords and PINs.* Passwords and PINs:
 - (i) Must never be shared or displayed on screen;
 - (ii) Must be classified; and
 - (iii) Must be changed when there is any indication of system or password compromise.

- (2) *Encryption of Passwords and PINs.* Passwords and PINs must comply with all DOITT Standards and:
 - (i) Must be encrypted when transmitted electronically with a protocol which complies with the DOITT Standards; and
 - (ii) Must be encrypted or hashed when held in storage. When embedded in configuration files, source code or scripts, passwords and PINs must be either encrypted or secured with compensating controls which provide a comparable level of protection.
 - (3) *Change Password.* A user wishing to change his or her password/PIN must be positively identified by demonstrating knowledge of the current password/PIN or by other comparable methods. Passwords must be changed every ninety (90) days. Passwords cannot be changed more than once a day.
 - (4) *Password Delivery.* Passwords must be delivered securely to the recipient (authorized user) with an approved transmission method. Although passwords and PINS must never be shared, initial passwords may be delivered to the recipient's manager. In all cases, the recipient or manager must be positively identified before the password is delivered.
 - (5) *Use of PINS.* PINs may only be used where a numeric method for authentication is required, such as a telephone keypad. In all other cases, passwords or pass-phrases must be used for authentication.
- (v) *Access Policy.*
- (1) *Authenticated Users.* Users must be positively and individually identified and authenticated prior to being permitted access to any E-Hail App Data or TPEP Data or related networking and computing resource.
 - (2) *Disconnect from Remote Access.* Users must disconnect from the remote access connection when not actively in use.
 - (3) *Confidentiality of Passwords and Authentication Mechanisms.* Users are responsible for maintaining the confidentiality of passwords or other authentication mechanisms that are assigned in conjunction with the remote access service. A user's credentials must be classified as restricted information. Individual passwords must never be shared.
 - (4) *Confidentiality of Data Remotely Accessed.* Users must protect the confidentiality and integrity of data that is accessed remotely. This includes, but is not limited to ensuring that E-Hail App Data and TPEP Data is either erased from the remote device after use or appropriately protected based on the level of sensitivity of the information.

(w) *User Responsibilities Policy.*

- (1) *Safeguard.* The E-Hail App Provider is responsible and accountable for safeguarding E-Hail App and TPEP Data from unauthorized modification, disclosure, and destruction.
- (2) *Protect Critical Data.* Critical data and removable data devices (USB drives, CDs, external drives, etc.) must be protected by appropriate physical means from modification, theft, or unauthorized access.