

**I. ALL SERVICES**

The following terms and conditions apply to all Services being performed by COMPANY:

**1.0 GENERAL**

(a) Definitions.

- (i) "Cargo" will mean cargo, commodities, mail, letters, parcels, or any other items that COMPANY transports for PB under the Agreement.
- (ii) "Carrier" is a motor carrier that transports Cargo for PB under the Agreement.
- (iii) "Required Government Licenses" are collectively all government approvals, licenses, permits, inspection certificates, customs clearances, or other documentation required by the laws of the originating country, the destination country, and any other country through which the Cargo may transit prior to commencement of the Services.

(b) Non-exclusivity. COMPANY agrees and acknowledges that PB may retain other transportation providers to perform services substantially similar to those provided by COMPANY.

(c) Transition Services. Notwithstanding anything to the contrary in the Agreement, upon expiration or termination of the Agreement for any reason, COMPANY agrees to provide the Services transitionally, upon PB's written request, for a period not to exceed one hundred eighty (180) days under the terms of the Agreement ("Transition Services"). COMPANY shall charge PB for the Transition Services at the rates that were in effect at the termination or expiration of the Agreement. Upon cessation of the Transition Services (or the Services, if there are no Transition Services), COMPANY will immediately return to PB any proprietary and/or Confidential Information in COMPANY's possession and will return any Cargo, PB customer mail, documents and/or all other PB materials and equipment in COMPANY's possession, custody or control.

(d) Standards Of Performance. COMPANY and its Personnel will conduct themselves in a professional and businesslike manner in performing its obligations under the Agreement. COMPANY agrees that its Personnel will be properly attired with a uniform or clothing bearing a company insignia for the Services they perform.

(e) PB Policies. COMPANY's Personnel will not use, possess, transfer or sell any firearm, weapon, intoxicating beverage or illegal drug on PB's and/or PB's customer's property or while performing Services under the Agreement. COMPANY will not act in any manner that may endanger the safety of any PB and/or PB's customer's employee or anyone present at a PB and/or a PB's customer location or encountered while performing Services under the Agreement. COMPANY will observe all PB policies or PB customer policies of which COMPANY is advised, including non-smoking policies and policies prohibiting sexual harassment and discrimination against any person on the basis of gender, race, age, religion, ethnicity, disability, marital status, sexual orientation or any other legally protected category.

(f) Quarterly Business Reviews. At the request of PB, COMPANY agrees to participate in quarterly meetings as deemed necessary by PB to achieve the goals of the Agreement ("Quarterly Business Reviews"). Such Quarterly Business Reviews will involve general management team with functional mix as required. The meeting topics may include, but are not limited to, industry trends, potential problems, life of agreement, quality ratings, performance measures, opportunities for improvement and updates to any required documentation.

**2.0 PERSONNEL**

(a) Drug Test. COMPANY will ensure that its Personnel have passed an initial drug test, and are subject to on-going random drug testing (where lawful to do so, using an accredited laboratory).

(b) Background Check. COMPANY agrees to conduct on all its Personnel background checks for the previous seven (7) year period covering criminal convictions, employment verification, and any restrictions (e.g., a court order or restrictive covenant) that would prevent, limit, or restrict such person from providing the Services, including any restrictions that would cause such Personnel from being eligible to work in the applicable country in which the Services will be provided ("Background Checks"). COMPANY further agrees that no Personnel will perform Services for PB hereunder if such Personnel has been convicted of any crime involving theft, drugs, dishonesty or violence. Furthermore, COMPANY will maintain records and copies of its background checks conducted pursuant to this Section during the Term and for a minimum of three (3) years from the date of termination or expiration of the Ordering Document. COMPANY's records relating to such background checks will be subject to reasonable review at any reasonable time by PB, and COMPANY agrees to cause its Personnel to waive any privacy laws which would prevent PB from reviewing relevant data to the extent permitted by applicable law.

(c) Replacement Personnel. PB shall have the right to evaluate all Personnel assigned to perform Services under any Ordering Document and to accept or reject any Personnel. In the event that any Personnel is found to be unacceptable to PB at any time, PB shall notify COMPANY of such fact and COMPANY shall immediately remove such Personnel and, if requested by PB, provide replacement Personnel acceptable to PB, within five (5) days of such notice unless otherwise specifically addressed in the Ordering Document. PB is the sole judge as to performance capability of Personnel, provided that PB's request to remove such Personnel does not violate anti-discrimination laws, to the extent applicable.

## Logistics Services Terms and Conditions

(version – March 2019)

(d) Anticipated or Actual Delays. COMPANY understands that prompt performance of Services is required by PB. In the event that any anticipated or actual delays in meeting the deadlines or scheduled completion dates set forth in applicable Ordering Documents are caused by the unacceptable performance of any Personnel or any other cause within the reasonable control of COMPANY, COMPANY shall provide additional temporary Personnel, as requested by PB and at no charge to PB, in order to complete the Services in a timely manner. Neither Party, however, shall be responsible for any delays that are not due to such Party's fault or negligence or that could not have reasonably been foreseen.

(e) OSHA / EPA. COMPANY will, and will require its Personnel to, adhere to and comply with all applicable international and domestic environmental, health and safety laws, rulings, and regulations applicable to the performance of the Services under the Agreement, including but not limited to Occupational Safety and Health Administration, and Environmental Protection Agency regulations.

(f) USDOT. COMPANY will, and will require its Personnel to, adhere to and comply with all applicable USDOT regulations (and any comparable international regulations) regarding the handling, storage and/or delivery of Cargo.

### 3.0 FEES AND EXPENSES

(a) Fee Increases. COMPANY may only increase the fees specified in the applicable Ordering Document ("Fees") once each calendar year as follows: (i) COMPANY may propose one change in such Fees to PB in writing no later than October 1 of each calendar year, and such writing may be provided by mail or email (to the email address, if any, listed in applicable Agreement Order Form), but if provided by email, COMPANY will send a confirmatory letter to PB pursuant to the terms of Section 23 of the Standard Terms and Conditions within five (5) business days of sending such email; and (ii) any such Fee changes will become effective on January 1 of the next calendar year if PB and COMPANY agree to the Fee changes. If the parties cannot agree upon the Fee changes by December 31 of the then current year, then the Fees will remain at the then current levels, but either Party may terminate that part of the Services in the country or countries affected by the change of Fees upon written notice to the other Party no later than January 31 of the next calendar year. Such termination will be effective on March 31 of the next calendar year.

(b) Price Reductions. COMPANY agrees to cooperate and consult with PB and incorporate reasonable suggested changes to service techniques to improve the Services. COMPANY also understands that PB may request price reductions hereunder from time to time in order for PB to remain competitive. COMPANY agrees to evaluate and accept such requests if commercially reasonable. The parties will enter into appropriate amendments as may be required to effect the agreed changes.

(c) Service Levels and Service Level Credits. COMPANY will provide all Services in accordance with the level of performance required by the applicable Ordering Document (collectively, "Service Levels"). In the event that COMPANY fails to perform any portion of the Services in accordance with the applicable Service Levels, COMPANY will promptly take corrective action to remedy the problem, take measures to prevent the reoccurrence of the failure, and COMPANY will pay to PB the applicable amount of service level credits specified in the applicable Ordering Document ("Service Level Credits"). If at any time a Party reasonably disputes the other Party's determination of whether a Service Level Credit is due or the calculation of a Service Level Credit, then within ten (10) business days of receipt of written notice of such dispute, the parties will attempt to resolve the disputed Service Level Credit in good faith. In the event that the parties are unable to resolve the dispute within thirty (30) days of notice by either Party, PB may pursue any remedy available to it at law or in equity. Upon either Party's reasonable request, a Party will provide the requesting Party with all reasonable information and documentation necessary to verify or refute compliance by COMPANY with the Service Levels. COMPANY and PB each agree and acknowledge that Service Levels will be measured on a monthly, aggregate basis.

### 4.0 NON-SOLICITATION OF CUSTOMERS

COMPANY agrees that during the Term and for a period of one (1) year thereafter, it will not on its own behalf or on behalf of any third party promote, market, sell or solicit any services directly to any customer of PB, if such services are substantially similar to the Services provided to PB hereunder. The provisions of this Section will survive termination of the Agreement as necessary to affect its purpose.

### 5.0 INDEMNITY

(a) Third Party Claims. COMPANY, on behalf of itself and its successors and assigns, agrees to defend, indemnify and hold harmless PB, its directors, officers and employees from all losses, claims of losses, damages and expenses (including without limitation court costs and reasonable attorneys' fees) asserted by third parties, including but not limited to PB customers, COMPANY Personnel and COMPANY's insurer resulting from or arising out of: (a) COMPANY's breach of the Agreement; (b) the loss, misplacement, or theft of, any Cargo resulting from the acts, omissions or misconduct of COMPANY or COMPANY's Personnel; (c) damage to personal or real property; (d) bodily injury or death caused by COMPANY or COMPANY's Personnel; (e) the destruction or damage to Cargo caused by the negligent acts, omissions or misconduct of COMPANY or COMPANY's Personnel; (f) violation of law or other applicable regulation by COMPANY or COMPANY's Personnel; and (g) infringement of any patent, copyright, trademark or other property right (including, but not limited to, misappropriation of trade secrets) based on the Services or the use thereof by PB. Without limiting the foregoing, COMPANY agrees it is solely responsible for any claims asserted by or against COMPANY's Personnel in its performance of obligations under the Agreement. If a claim for workers' compensation benefits or awards is asserted against PB by any Personnel of COMPANY or such Personnel's heirs, assigns or beneficiaries, COMPANY agrees to indemnify and hold harmless PB with respect to any liability imposed on PB in connection with such claims.

**Logistics Services Terms and Conditions**

(version – March 2019)

- (b) Refund of Charges. COMPANY shall fully refund any shipping, transportation and handling charges for Cargo that are subject to a claim in subsection (a) above.

**6.0 REPRESENTATIONS AND WARRANTIES**

COMPANY represents and warrants that COMPANY is legally able to provide the Services in each country the Services are provided under the Agreement and will comply with the Service Levels, if any, set forth in an applicable Ordering Document.

**7.0 C-TPAT.**

COMPANY represents and warrants that it is a party to a government supply chain security program, such as C-TPAT, PIP, AEO, or SAFE, (“Supply Chain Security Program”) or has otherwise verified that it complies with such Supply Chain Security Program standards, and that it will continue to be a party to such Supply Chain Security Program, or maintain such Supply Chain Security Program standards, during the Term of the Agreement. COMPANY shall at all times ensure that it maintains a verifiable documented security program consistent with such Supply Chain Security Program, and that, if applicable, COMPANY will only engage with business partners that are either parties to such Supply Chain Security Program, or which comply with all of such Supply Chain Security Program’s applicable security standards.

**8.0 OFAC.**

COMPANY further represents and warrants that it is not the subject of any sanctions administered or enforced by the U.S. Department of the Treasury’s Office of Foreign Assets Control (“OFAC”), the United Nations Security Council (“UNSC”), the European Union (“EU”), Her Majesty’s Treasury (“HMT”), or other relevant sanctions authority (collectively, “Sanctions”), nor is the COMPANY organized under or resident in a country or territory that is the subject of Sanctions. COMPANY represents and warrants that it has not and will not during the term of the Agreement violate any Sanctions. COMPANY will not use the Agreement to fund or engage in any activities with any individual or entity (“Person”) or in any country or territory that, at the time of such funding or activity, is the subject of Sanctions. COMPANY will not engage as an agent or subcontractor any entity or individual who is subject to Sanctions and will require that all Personnel not violate such Sanctions. If any COMPANY or its Personnel is found to be the subject of Sanctions or to have violated Sanctions, COMPANY will immediately cease using such agent or subcontractor to provide the Services and notify PB.

**9.0 THIRD PARTY MANDATORY FLOW DOWN PROVISIONS**

(a) Foreign Corrupt Practices Act Compliance. COMPANY will comply with and not violate any applicable anti-bribery laws, including but not limited to the Foreign Corrupt Practices Act of 1977, as amended from time to time, and any statute enacted to replace or supersede the Foreign Corrupt Practices Act of 1977 (the “FCPA”), in the performance of its obligations under this Agreement. In addition, COMPANY will at all times:

- (i) have in place policies and procedures with its subcontractors mandating compliance by its subcontractors with the FCPA and all other applicable anti-bribery laws;
- (ii) if applicable, require that all subcontractors include a provision in their subcontracts with their subcontractors to never pay bribes or facilitating payments or provide entertainment, gifts, or donations to customs and/or other government officials in connection with the Services;
- (iii) require that its subcontractors never utilize any other third party service providers that pay bribes or facilitating payments or provide entertainment, gifts, or donations to customs and/or other government officials in connection with the Services; and
- (iv) stop any conduct or activity and avoid any action or omission that may violate or be penalized under any applicable law.

(b) Anti-Boycott Clause. Nothing in this Agreement is intended to or will be effective to the extent that it constitutes or requires an action or inaction that would be prohibited or penalized under Section 999 of the U.S. Internal Revenue Code or the U.S. Export Administration Regulations.

(c) Audit Rights. During the Term of the Agreement and for seven (7) years thereafter, COMPANY will maintain records sufficient to demonstrate COMPANY’s compliance with the Agreement, if applicable, including those records for import and export, and Supply Chain Security Program standards. Upon reasonable request, and upon reasonable notice during normal business hours during the Term and for seven (7) years thereafter, PB or its agent will be permitted to examine COMPANY’s books and records that relate to the Agreement so as to ensure compliance under the Agreement and any applicable Ordering Document. PB will be responsible for the costs or expenses of any such examinations, provided however, that if such examination discloses any fraud, willful misconduct, or gross negligence, COMPANY will promptly reimburse PB for the cost of such examination. If such examination discloses any shortfall or discrepancy, which results in monies being owed to PB, COMPANY will make prompt payment of such amount to PB.

(d) Marketing Restrictions. COMPANY (and any of its subcontractors) will not at any time use any of PB’s Confidential Information obtained by COMPANY in providing the Services to send any marketing or other promotional communications to PB’s customers (whether individually or collectively), without PB’s prior written consent.

**10.0 LIMITATION OF LIABILITY.**

EXCEPT FOR CLAIMS RELATED TO (1) BREACHES OF CONFIDENTIALITY (INCLUDING SENSITIVE INFORMATION); (2) OBLIGATIONS OF INDEMNIFICATION SET FORTH IN THE AGREEMENT; (3) BODILY INJURY OR DEATH; (4) ANY GROSSLY NEGLIGENT ACT/OMISSION OR

**Logistics Services Terms and Conditions**

(version – March 2019)

WILLFUL MISCONDUCT; OR (5) VIOLATION OF ANY APPLICABLE LAW OR REGULATION, UNDER NO CIRCUMSTANCES WILL EITHER PARTY BE LIABLE TO THE OTHER PARTY FOR ANY SPECIAL OR PUNITIVE DAMAGES, OR CONSEQUENTIAL LOSS OR DAMAGE, OR ANY LOSS OF PROFITS, GOODWILL, BUSINESS OPPORTUNITY, BUSINESS, REVENUE OR ANTICIPATED SAVINGS, IN RELATION TO THIS AGREEMENT, WHETHER OR NOT THE RELEVANT LOSS WAS FORESEEABLE, OR THE PARTY WAS ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

**11.0 LOSS**

- (a) COMPANY will notify PB of any known loss that has resulted from theft (or other operational discrepancies), damage or destruction within seven (7) days of the incident(s). COMPANY will allow PB or one of its representative the ability to work directly with COMPANY management, Personnel or its subcontractors to investigate and resolve any issues that are related to such loss.
- (b) COMPANY accepts liability for all Cargo after the Cargo is tendered to COMPANY (or its Personnel). COMPANY shall be liable for any from theft (or other operational discrepancies), loss, damage or destruction to Cargo occurring while in the possession of COMPANY or under COMPANY's care, custody or control (for the avoidance of doubt, includes possession by COMPANY's Personnel), or resulting from COMPANY's performance of or failure to perform the Services provided herein ("**Loss Liability Claim**").
- (c) PB expressly reserves any other rights and remedies available under federal or state laws in the event of any such theft (or other operational discrepancies), loss, damage or destruction.
- (d) In order to pursue a Loss Liability Claim, PB must file a written intent to file claim ("Notice of Intent") with COMPANY (i) within thirty (30) days of the date that the Cargo was allegedly delivered by COMPANY or (ii) ninety (90) days from the expected delivery date. No later than nine (9) months from the date a Notice of Intent was filed, PB shall subsequently file a corresponding written claim notice with COMPANY identifying (i) the shipment and Cargo involved and (ii) the amount of COMPANY's liability for the Loss Liability Claim ("**Loss Liability Claim Notice**"). Upon receipt of a Loss Liability Claim Notice, COMPANY will acknowledge and respond to PB within five (5) business days. COMPANY will promptly investigate each Loss Liability Claim and pay, decline for reasonable cause, or settle the Loss Liability Claim within thirty (30) days after receipt of the Loss Liability Claim Notice. Past due Loss Liability Claim amounts shall bear interest at the highest rate allowed by law. PB will have the sole right to determine what constitutes reasonable cause, provided that in making such determination, PB will act in good faith and not act arbitrarily.
- (e) COMPANY shall fully refund any shipping, transportation and handling charges for Cargo that are subject to a Loss Liability Claim.

**12.0 SURVIVING SECTIONS**

The following sections shall survive the termination or expiration of the Agreement:

- (a) Sections 2(b), 4, 5, 9(c), 9(d), 10, 11 and 12; and
- (b) any other section that, by its nature, would continue beyond the termination or expiration of the Agreement.

**II. CUSTOM BROKERAGE**

If COMPANY is providing custom brokerage Services, the following terms and conditions shall apply:

- 1.0 LICENSES, PERMITS AND CERTIFICATES.** COMPANY will have obtained, without any expense to PB, all Required Government Licenses. Upon request, copies of any such Required Government Licenses will be provided to PB. COMPANY will notify PB within thirty (30) days of any changes to such Required Government Licenses.
- 2.0 SPECIFICATIONS.** COMPANY will adhere to any specification (including but not limited to scheduling and/or tracking notification specifications) that PB may provide to COMPANY from time to time.
- 3.0 Surety Bonds.** COMPANY represents and warrants that it is authorized to submit any and all custom surety bonds to the applicable customs authorities and is in compliance with all government regulations and legislation. For all Cargo processed by COMPANY, COMPANY will fulfill all obligations between customs and an importer for any given transaction.

**4.0 SURVIVING SECTIONS**

The following sections shall survive the termination or expiration of the Agreement:

- (a) any section that, by its nature, would continue beyond the termination or expiration of the Agreement.

**III. TRANSPORTATION BROKERAGE**

If COMPANY is providing transportation brokerage Services, the following terms and conditions shall apply:

**1.0 BROKERING.**

(a) Carriers. PB acknowledges that COMPANY provides motor property brokering services and that certain Services may be provided by third party Carriers, who are contractually obligated by COMPANY to provide the Services in accordance with the Agreement ("Third Party Carrier"). All references in the Agreement that specify that COMPANY is responsible for performing any action or complying with any laws or requirements within a Third Party Carrier's control shall be read as also including COMPANY's requirement to contractually obligate such Third Party Carrier to agree to such compliance, performance or requirements, and to diligently enforce such contractual obligations. In addition, all references in the Agreement to "Personnel" shall be read as also including Third Party Carrier's employees and employees of any subcontractors of such Third Party Carriers.

(b) Carrier Contracts. COMPANY shall include a provision in its contracts with Third Party Carriers (or its Third Party Carrier rate confirmation) stating substantially as follows: "*Third Party Carrier agrees that it will look solely to COMPANY for the payment of its charges and that it will not contact or pursue COMPANY's customers or the shipper or consignee for payment of freight, accessorial or other charges owed to Third Party Carrier.*"

**2.0 CARRIERS.**

(a) Licenses, Permits and Certificates. COMPANY will verify that all Third Party Carriers have obtained, without any expense to PB, all Required Government Licenses. Upon request, copies of any such Required Government Licenses will be provided to PB. COMPANY will verify that all Personnel of such Third Party Carriers shall have a rating of "satisfactory" with the USDOT (or a comparable rating, as applicable, in the territory in which the Services are being performed).

(b) FMCSA. COMPANY agrees and warrants that, in the selection of Third Party Carriers to provide Services under the Agreement, it will observe and enforce the following procedures: (i) COMPANY shall verify that all Third Party Carriers are currently registered with the Federal Motor Carrier Safety Administration ("FMCSA") and/or state regulatory agencies as required by applicable federal and/or state law; and (ii) COMPANY shall not tender any shipment to a Third Party Carrier that has its operating authority revoked or suspended, or receives a "Conditional" or "Unsatisfactory" rating (as defined in 49 CFR 385.3) or is declared "Unfit" or "Out of Service" by the FMCSA.

(c) Carrier Claims. COMPANY shall be responsible for all claims against the responsible Third Party Carriers, including filing, communication with Third Party Carriers and collection of claims. COMPANY's liability under the Agreement shall not be dependent on its ability to recover from Third Party Carriers. PB will assist COMPANY in the processing of claims when requested by COMPANY. PB reserves the right to recover its claims for loss, damage, or delay directly from the responsible Third Party Carriers, provided that the exercise of PB's right to recover claims directly shall, under no circumstances, be deemed or construed as a waiver of PB's rights and remedies as against COMPANY.

**3.0 DOUBLE BROKERING.**

Unless prior written approval has been obtained from PB, COMPANY shall contract only with the actual Third-Party Carrier that will transport the Cargo and shall require that its Third Party Carrier does not subcontract or "double broker" the shipment to another Carrier.

**4.0 SURETY BOND & INSURANCE.**

COMPANY shall maintain a broker's surety bond that shall meet or exceed the requirements of the FMCSA as specified in 49 C.F.R. Sec. 387.307 and/or any state regulatory bodies having jurisdiction over broker operations, and COMPANY shall furnish PB with proof thereof during the Term of the Agreement.

**5.0 TRANSPORTATION EQUIPMENT AND VEHICLES, PROCEDURES AND PROCESSES.**

- (a) Transportation Equipment, Vehicles and Receipt Documentation. COMPANY shall verify that all Third Party Carriers have caused the following:
- (i) Third Party Carriers' drivers to complete and sign the appropriate receipt documentation (bill of lading or pickup slip) for each transaction.
  - (ii) Third Party Carriers or its Personnel to have exclusive control of the transportation equipment and vehicles, procedures and processes used in the performance of the Services pursuant to the applicable Ordering Document.
  - (iii) Third Party Carriers to maintain such transportation equipment and vehicles in good working order necessary to perform the Services in a safe and professional manner, including, but not limited to, maintaining trailers with a clean, odor free, dry and leak proof interior free of contamination, debris and infestation.
  - (iv) Third Party Carriers to pay all costs and expenses necessary or incidental to the maintenance and operation of equipment required to provide the Services unless otherwise specifically agreed to in writing by the Parties.

**Logistics Services Terms and Conditions**

(version – March 2019)

(b) Third Party Motor Carriers. COMPANY shall verify that all Third Party Carriers hold a rating of “satisfactory” with the USDOT (or a comparable rating, as applicable, in the territory in which the Services are being performed) in providing the Services to PB hereunder. PB further agrees to pay COMPANY directly pursuant to the terms and conditions of the Agreement for any and all Services performed by Third Party Carriers at the direction of COMPANY pursuant to this provision. Provided that PB has paid COMPANY for the Services provided hereunder, COMPANY agrees to hold PB harmless from any compensation due Third Party Carriers for Services performed at the direction of COMPANY on behalf of PB hereunder. Notwithstanding the fact that COMPANY may use Third Party Carriers in the performance of its obligations hereunder, COMPANY will remain responsible to PB for proper performance of the Agreement.

(c) Subcontractor – Drivers. For all drivers performing Services under the Agreement, COMPANY shall verify that all Third Party Carriers have caused the following:

- (i) Third Party Carriers have obtained written evidence that such drivers maintain and is in compliance with all Required Government Licenses.
- (ii) Third Party Carriers have obtained written evidence that a Background Check has been conducted on each driver and that each such driver passed an initial drug test, and is subject to on-going random drug testing (where lawful to do so, using an accredited laboratory).
- (iii) Third Party Carriers will provide to PB, upon request, evidence of compliance with each of these requirements.
- (iv) Third Party Carriers will require all drivers to have proper identification on their person while handling Cargo. Such identification can be a valid state driver’s license/identification card or a visible company identification card.

(d) Security. COMPANY shall verify that all Third Party Carriers’ facilities have a working burglar alarm system. The alarm system must be activated when the facility is shut down and must include key pad, man-door contacts, and interior motion detectors. The alarm system must also be monitored on a twenty-four (24) hour basis by a third-party alarm company. All former Personnel access must be terminated. COMPANY shall verify that all Third Party Carriers’ facilities possess a CCTV system that includes a DVR (Digital Video Recording) system with a capability of recording at least twenty-one (21) or more days of consecutive data. All cameras must be color and include adequate coverage of the interior and exterior of the facility. If Cargo or piece sort is taking place at a Third Party Carriers’ facility, there must be at least two (2) or more cameras at opposite angles directed on the sort area in order to view 100% of the area. If COMPANY has idle Cargo sitting overnight or on the weekends, there must be camera coverage on the Cargo. COMPANY shall verify that all Third Party Carriers facilities have adequate measure of access control to prohibit unauthorized entry into the facility or designated spaces. The facility must have adequate and working locks on all facility man and overhead doors. Key control must be in place to include a listing of all Personnel with keys and repossession of former Personnel’s keys.

**6.0 SURVIVING SECTIONS**

The following sections shall survive the termination or expiration of the Agreement:

- (a) Sections 2(c) and 5(b); and
- (b) any other section that, by its nature, would continue beyond the termination or expiration of the Agreement.

**IV. TRANSPORTATION PROVIDER**

If COMPANY is providing transportation provider Services, the following terms and conditions shall apply:

**1.0 COMPLIANCE WITH LAWS.**

(a) Licenses, Permits and Certificates. COMPANY will, at its sole expense, obtain all government approvals, licenses, permits, inspection certificates, customs clearances, or other documentation required by the laws of the originating country, the destination country, and any other country through which the Cargo may transit prior to commencement of the Services (collectively, “Required Government Licenses”). Upon request, copies of any such Required Government Licenses will be provided to PB. All Personnel shall have a rating of “satisfactory” with the USDOT (or a comparable rating, as applicable, in the territory in which the Services are being performed).

(b) FMCSA. COMPANY agrees and warrants that it will observe and enforce the following procedures: (i) COMPANY shall be registered with the Federal Motor Carrier Safety Administration (“FMCSA”) and/or state regulatory agencies as required by applicable federal and/or state law; and (ii) COMPANY shall not accept a shipment if its operating authority is revoked or suspended, or it receives a “Conditional” or “Unsatisfactory” rating (as defined in 49 CFR 385.3) or is declared “Unfit” or “Out of Service” by the FMCSA.

**2.0 TRANSPORTATION EQUIPMENT AND VEHICLES, PROCEDURES AND PROCESSES.**

(a) Transportation Equipment, Vehicles and Receipt Documentation. COMPANY will cause its drivers to complete and sign the appropriate receipt documentation (bill of lading or pickup slip) for each transaction. COMPANY or its Personnel will have exclusive control of the transportation equipment and vehicles, procedures and processes used in the performance of the Services pursuant to the applicable Ordering Document. COMPANY will maintain such transportation equipment and vehicles in good working order necessary to perform the Services in a safe and professional manner, including, but not limited to, maintaining trailers with a clean, odor free, dry and leak proof interior free of contamination, debris and infestation.

## Logistics Services Terms and Conditions

(version – March 2019)

COMPANY will pay all costs and expenses necessary or incidental to the maintenance and operation of equipment required to provide the Services unless otherwise specifically agreed to in writing by the Parties.

(b) Carriers. COMPANY shall hold a rating of “satisfactory” with the USDOT (or a comparable rating, as applicable, in the territory in which the Services are being performed) in providing the Services to PB hereunder.

(c) Drivers. For any drivers performing Services under the Agreement with COMPANY, COMPANY agrees to:

- i. Provide written evidence that each driver maintains and is in compliance with all Required Government Licenses.
- ii. Provide written evidence that a Background Check has been conducted on each driver and that each such driver passed an initial drug test, and is subject to on-going random drug testing (where lawful to do so, using an accredited laboratory).
- iii. Provide to PB, upon request, evidence of compliance with each of these requirements.
- iv. Require all drivers to have proper identification on their person while handling Cargo. Such identification can be a valid state driver’s license/identification card or a visible company identification card.

(d) Security. COMPANY’s facilities must have a working burglar alarm system. The alarm system must be activated when the facility is shut down and must include key pad, man-door contacts, and interior motion detectors. The alarm system must also be monitored on a twenty-four (24) hour basis by a third-party alarm company. All former Personnel access must be terminated. COMPANY’s facilities must possess a CCTV system that includes a DVR (Digital Video Recording) system with a capability of recording at least twenty-one (21) or more days of consecutive data. All cameras must be color and include adequate coverage of the interior and exterior of the facility. If Cargo or piece sort is taking place at the COMPANY’s facility, there must be at least two (2) or more cameras at opposite angles directed on the sort area in order to view 100% of the area. If COMPANY has idle Cargo sitting overnight or on the weekends, there must be camera coverage on the Cargo. . COMPANY’s facilities must have adequate measure of access control to prohibit unauthorized entry into the facility or designated spaces. The facility must have adequate and working locks on all facility man and overhead doors. Key control must be in place to include a listing of all Personnel with keys and repossession of former Personnel’s keys.

### 3.0 SURVIVING SECTIONS

The following sections shall survive the termination or expiration of the Agreement:

- (a) any section that, by its nature, would continue beyond the termination or expiration of the Agreement.

## V. AIR TRANSPORTATION SERVICES

If COMPANY is providing air transportation Services, the following terms and conditions shall apply:

### 1.0 INDIRECT AIR CARRIER.

If applicable, COMPANY represents and warrants that it is authorized to act as an Indirect Air Carrier (“IAC”) pursuant to U.S. Department of Transportation rules and regulations. COMPANY further agrees to remain an authorized IAC throughout the Term of the Agreement. COMPANY shall be the IAC for all air transportation of the Cargo or shall receive the Cargo from an IAC of PB’s choosing. As IAC, PB grants COMPANY the authority to open, inspect, and/or repackage Packages for purposes of proving chain of custody, auditing suspicious or damaged items, or other requirements according to Transportation Security Administration (“TSA”) guidelines. COMPANY shall re-weigh any Cargo that has been opened and/or repackaged.

### 2.0 KNOWN SHIPPER.

COMPANY shall establish processes and procedures to accept Cargo from Known Shipper locations for the purposes of TSA chain of custody requirements and to allow air transportation by both commercial and cargo airlines.

### 3.0 HAZARDOUS MATERIALS / DANGEROUS GOODS.

PB will not tender, and COMPANY will not accept, Cargo, which is prohibited by law or regulation, or any hazardous materials, dangerous goods or other items which are subject to regulation by Title 49 of the U.S. Code of Federal Regulations, the International Air Transport Association (“IATA”) dangerous goods regulations, the International Maritime Dangerous Good (“IMDG”) code or the European Agreement concerning the international carriage of Dangerous goods by Road (“ADR”) regulations.

### 4.0 SURVIVING SECTIONS

The following sections shall survive the termination or expiration of the Agreement:

- (a) Any section that, by its nature, would continue beyond the termination or expiration of the Agreement.

**VI. PRESORT**

If COMPANY is providing Presort Services, the following terms and conditions shall apply:

**1.0 DEFINITIONS**

- (a) Access Device. The term “Access Device” shall mean a method of access to a PB premises or facility (including, but not limited to, keys, codes, or access cards).
- (b) Confidential Information. The term “Confidential Information” shall include, but not be limited to, PB Customer Mail, the identity of any PB client submitting mail to PB, security measures and business continuity.
- (c) Cross-Dock Services. The term “Cross-Dock Services” shall mean Company’s handling of Customer Mail in any of Company’s facilities that are used to hold and secure such Customer Mail until such time that PB or another PB approved transportation provider picks up such Customer Mail and transports it to the destination designated by PB.
- (d) Customer Mail. The term “Customer Mail” shall mean all mail provided by PB to Company for PB’s customers including all envelopes, postcards, packages or other containers, whether bearing postage meter mark or other indicia, and whether or not received by the USPS.
- (e) Personnel. The term “Personnel” shall mean Company’s full time or part time employees, and employees of its subcontractors and shall include, but not be limited to, all drivers, authorized representatives, third party motor carriers, agents, contracted labor and independent contractors, performing the Transportation Services and/or Cross-Dock Services under the Agreement.
- (f) Personnel with Mail Access. The term “Personnel with Mail Access” shall mean Personnel that will have access to Customer Mail.
- (g) Transportation Services. The term “Transportation Services” shall mean any or all freight broker, freight forwarding and/or physical transportation services as may be provided by Company or engaged by Company on behalf of PB under the Agreement, including but not limited to transporting or arranging for the transport of Customer Mail in compliance with the requirements, terms and conditions of the Agreement for such routes as PB may request from time to time upon reasonable advance notice or for such recurring routes as the Parties may agree upon from time to time.

**2.0 TRANSPORTATION SERVICES AND CROSS-DOCK SERVICES**

- (a) Vehicles and Receipt Documentation. Personnel shall lock all vehicles (including tractor and trailer compartments) when transporting or holding Customer Mail and complete and sign the appropriate receipt documentation (bill of lading or pickup slip) for each transaction.
- (b) Cross-Dock Services. In the event that Company provides Cross-Dock Services, Company shall comply with the following Cross-Dock Services security requirements at any Company facility where Cross-Dock Services are provided:
  - (i) Cross-Dock Services may only be provided in a facility that maintains an interior and exterior camera system with video recordings which are retained for a period of ninety (90) calendar days.
  - (ii) Video equipment must be maintained in an area that is restricted from unauthorized persons.
  - (iii) Exterior cameras must cover all entrances and exits, including bay docks.
  - (iv) Interior cameras must cover all areas where Customer Mail is processed or held.
  - (v) All exterior doors must remain closed and locked from the inside and may only be accessed from the outside with an Access Device.
  - (vi) Dock doors are required to be kept closed at all times, except when in use for normal loading dock activities.
  - (vii) Exterior windows, doors and other openings must be protected against intrusion by mechanisms such as intruder resistant glass, glass break detection, or magnetic contact detectors.
  - (viii) Third party security system vendors must monitor alarm systems which are activated during non-production times.
  - (ix) Visitors must access the building through a designated visitor entrance. All visitors are required to show a government issued identification, sign a visitor’s log, receive a numbered badge that contains no access credentials, be bound by a non-disclosure agreement with requirements substantially similar to those set out in the Agreement, and be escorted at all times during their visit.
  - (x) Access for Personnel must be granted according to the Personnel’s access level. Access levels are determined by the Personnel’s



## Logistics Services Terms and Conditions

(version – March 2019)

responsibilities within the Company.

- (xi) Access badge log information must be retained for at least ninety (90) days.
- (xii) A procedure must be in place to promptly revoke access for separated Personnel.
- (xiii) Personnel with Mail Access must receive annual security and confidentiality training.

(c) Employment Eligibility. Company shall only assign Personnel to perform Transportation Services and Cross-Dock Services that are legally eligible for employment in the U.S. and the state where the Transportation Services and Cross-Dock Services are being performed and shall maintain all government required documentation.

(d) Access Device or Unescorted Access. If any Personnel will have an Access Device or will have unescorted access to Customer Mail or a PB facility, Company shall conduct, or cause to be conducted, a background check (as prescribed below in subsection (e) below). All such Personnel must meet the requirements in subsection 2.0 (f) below. All Access Devices issued to Company's Personnel shall be kept in a secured location when not in use for the performance of Services. Company or its Personnel shall immediately notify PB if there is any loss or misuse of such Access Device.

(e) Background Check. All background checks must include:

- (i) Criminal history check for the previous seven years in all jurisdictions where the Personnel has resided during that time.
- (ii) National Sex Offender Registry (NSOR)
- (iii) FACIS Level I - Security Watch List (which includes: ATF Most Wanted, Australian Consolidated List, Consolidated List of Financial Sanctions Targets, Politically Exposed Persons (PEP) List, DEA Fugitives, US Marshals 15 Most Wanted, European Union Consolidated List, FBI 10 Most Wanted, FBI's Most Wanted Terrorists, FBI Fugitives/Cyber Crimes, FBI Fugitives/Violent Murders, FBI Fugitives/Add'l Violent Crimes, FBI Fugitives/Criminal Enterprise, FBI Fugitives/Domestic Terrorism, FBI Fugitives/White Collar Crimes, Excluded Parties List, FBI Fugitives/Crimes Against Children, Health & Human Services Exclusions List, INTERPOL, NCUA Administrative Orders, Specially Designated Nationals List, Palestinian Legislative Council (PLC) List, OCC Enforcement Actions List, OTS Enforcement Actions List, Canadian Sanctions List, US Secret Service Most Wanted, Air Force Fugitives, Denied Persons List, Entity List, Debarred Parties List, USPS Most Wanted, World Bank Listing of Ineligible firms/individuals), Terrorism Knowledge Base, Unverified List
- (iv) If the Personnel will be operating a PB motor vehicle, the seven- year check must include the MVR for states in which the applicant is licensed to drive.

(f) Background Check Requirements. As a result of the confidential nature of Customer Mail and associated security requirements, Personnel shall be presumed to be unqualified for certain positions if they do not successfully meet the background check requirements below. Therefore, to the extent permitted by law (including any applicable EEOC requirements), Company shall not assign or allow any Personnel to provide Transportation Services or Cross-Dock Services with access to Customer Mail, PB Confidential Information or to have unescorted access to Customer Mail or PB facilities, under the following conditions:

- (i) The Personnel has ANY felony convictions.
- (ii) The Personnel has any misdemeanor convictions (including deferments and diversions) related to theft; check or credit card fraud; securities trade, banking or insurance violations; or any drug related offense.
- (iii) The Personnel has a history of violent behavior, drug use/distribution, securities trade, banking or insurance regulatory violations, or any kind of theft or job-related dishonesty, (regardless of convictions or dismissals).
- (iv) The Personnel has been named on the NSOR or the FACIS Level 1 lists.
- (v) The Social Security Number of the Personnel does not match the Social Security Administration database and the matter cannot be resolved within the legal time limit.
- (vi) In addition, if for a driving position, the Personnel has any alcohol or drug-related violations or other serious or multiple driving infractions indicating a security or safety risk.
- (vii) The Personnel fails or refuses the pre-employment/pre-assignment drug screen or any random or periodic drug screens required by the USDOT or by Company's own lawful policies.
- (viii) The Personnel does not have a rating of "satisfactory" with the USDOT (or a comparable rating, as applicable, in the territory in which the Services are being performed).

(g) Cell Phone Use. Personnel shall not use cell phones in any PB production area or customer facility.

(h) Confidentiality and Security Training. Company shall provide confidentiality and security training that addresses the requirements of this Addendum to all Personnel who provide Transportation Services or Cross-Dock Services with access to Customer Mail or PB Confidential Information or have unescorted access to Customer Mail or a PB facility. Upon request, Personnel shall complete any PB required security training, confidentiality

**Logistics Services Terms and Conditions**

(version – March 2019)

training, or driver’s training that is applicable to the Transportation Services or Cross-Dock Services to be provided under the Agreement.

**3.0 SURVIVING SECTIONS**

The following sections shall survive the termination or expiration of the Agreement:

- (a) Any section that, by its nature, would continue beyond the termination or expiration of the Agreement.

**VII. FDR**

If COMPANY is providing FDR Services, the following terms and conditions shall apply:

There are no additional terms and conditions that are applicable to FDR Services.

**VIII. SMB**

If COMPANY is providing SMB Services, the following terms and conditions shall apply:

There are no additional terms and conditions that are applicable to SMB Services.

**IX. Cross Border**

If COMPANY is providing cross border Services, the following terms and conditions shall apply:

**1.0 CONFIDENTIALITY AND INFORMATION SECURITY**

COMPANY will also comply with the privacy and information security terms and conditions contained in Exhibit A, which is attached hereto.

**2.0 THIRD PARTY MANDATORY FLOW DOWN PROVISIONS**

- (a) “PB Data” means:

- (i) any and all data and information that are provided by PB and/or its service providers, in connection with the Agreement;
- (ii) any and all data and information regarding sellers, buyers, and/or consignees that are collected or obtained by PB and/or its service providers in connection with the Agreement;
- (iii) any and all data regarding Cargo that are provided by PB and/or its service providers in connection with the Agreement; and
- (iv) any and all reports, analyses, compilations, studies, or other documents which contain or otherwise reflect any of the data or information in (i)-(iii) above, including without limitation the reports produced by COMPANY pursuant to the Agreement.

- (b) COMPANY acknowledges and agrees that:

- (i) PB will own all right, title, and interest and any and all intellectual property rights in and to the PB Data, which, as between PB and COMPANY, will at all times remain the sole and exclusive property and Confidential Information of PB.
- (ii) PB does not in any way assign, transfer, or convey title of the PB Data to COMPANY, and, except as expressly provided in the Agreement or as necessary to perform the Services. COMPANY will have no rights to copy, access, use, reproduce, display, perform, modify, collect, store, transmit or transfer the PB Data or any derivative works thereof other than as necessary to perform the Services.
- (iii) COMPANY warrants that it will only share PB Data with COMPANY’s subcontractors who have entered into an agreement with COMPANY and then only as necessary to perform the Services.
- (iv) COMPANY agrees not to challenge the validity of PB’s ownership in the PB Data or to alter, modify, combine, reproduce, sell, license, rent, or distribute the PB Data or PB’s customer information, disclose or assign the PB Data or PB’s customer information to any third party, or use the PB Data or PB’s customer information to solicit or cause the solicitation of the names and/or addresses of those individuals contained in the PB Data or PB’s customer information.
- (v) COMPANY agrees to delete all (or such portion requested) of the PB Data and PB’s customer information from COMPANY’s computer and storage systems and media and destroy any and all tangible copies of all (or such portion requested) of the PB Data or PB’s customer information in accordance with Section 5.2-5.3 of Exhibit A, except for any data that COMPANY is expressly required to retain under applicable law.

**3.0 SURVIVING SECTIONS**

The following sections shall survive the termination or expiration of the Agreement:

- (a) Any section that, by its nature, would continue beyond the termination or expiration of the Agreement.

## Logistics Services Terms and Conditions

(version – March 2019)

### EXHIBIT A

#### PRIVACY AND INFORMATION SECURITY TERMS AND CONDITIONS

#### 1. Definitions

- 1.1 "Aggregate" means to combine or store PB Data with any data or information of COMPANY or any third party.
- 1.2 "Anonymize" means to use, collect, store, transmit or transform any data or information (including PB Data) in a manner or form that does not identify, permit identification of, and is not otherwise attributable to any user, device identifier, source, product, service, context, brand, or PB or its Affiliates.
- 1.3 "Applicable Laws and Regulations" means any applicable data protection, privacy or information security laws, codes and regulations or other binding restrictions governing the processing of PB Data, that are applicable to or required by (i) any location identified in an Ordering Document; (ii) the jurisdiction(s) in which COMPANY or its Personnel are located; or (iii) the jurisdiction(s) in which the Data Subjects are located.
- 1.4 "Data Centers" means locations at which COMPANY provides data processing or transmission functions in support of the Agreement. Data Centers can be COMPANY-owned or third party service model-based.
- 1.5 "Data Controller" means PB, who is the party that determines the purposes of the processing of PB Personal Data.
- 1.6 "Data Protection Authority" or "Data Protection Authorities" means the competent body (or bodies) in the jurisdiction charged with enforcement of Applicable Laws and Regulations.
- 1.7 "Data Subject" means the identified or identifiable natural person who is the subject of Personal Data and is protected under Applicable Laws and Regulations.
- 1.8 "Incident" means any impairment to the security of Sensitive Information including any (i) act that violates any law or any COMPANY or PB security policy; (ii) unplanned service disruption that prevents the normal operation of Services to PB; or (iii) unauthorized access, or attempt to access, to Sensitive Information.
- 1.9 "Industry Standard Encryption Algorithms and Key Strengths" means encryption that meets at least the following standard encryption algorithm (Note: The algorithm and key strengths may change depending upon the new and most up-to-date industry standard encryption practice):
  - 1.9.1 Symmetric encryption: 3DES (≥ 168-bit, CBC mode); RC4 (≥ 128-bit, CBC mode); AES (≥ 128-bit, CBC mode);
  - 1.9.2 Asymmetric encryption: RSA (≥ 2048-bit); ECC (≥ 160-bit); El Gamel (≥ 1024-bit); and
  - 1.9.3 Hashing: SHA2 (≥ 224-bit) with "salt" will be added to the input string prior to encoding to ensure that the same password text chosen by different users will yield different encodings.
- 1.10 "In Storage" means information stored in databases, in file systems, and on various forms of online and offline media (DASD, tape, etc.) and is also commonly referred to as "at rest."
- 1.11 "Personal Data" means any PB Data relating to a Data Subject. For the avoidance of doubt, an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.
- 1.12 "Processing Location" means the location(s) in which PB, or any Affiliate, in the Agreement is established, and any countries where COMPANY or its subcontractors process PB Data.
- 1.13 "Restricted Information" will mean highly sensitive or regulated information that is intended only for a limited audience within COMPANY or whose release would likely have a material adverse financial or reputational effect on PB, PB employees, or PB customers. All information in this category will be restricted to a limited group with authorized need to know access. Examples include but are not limited to:
  - 1.13.1 Passwords, challenge/response answers, personal identification numbers (PIN), biometric data, and any other codes that provide access to systems or networks that store, transmit or process Sensitive Information;
  - 1.13.2 Government issued identification numbers (e.g. tax identification number, Social Security number; passport number; driver's license number; state identification number, and Russian internal passport information);
  - 1.13.3 Financial and Payment Information (e.g., bank account numbers, credit card or debit card numbers, including Cadastro de Pessoas Físicas in the Federal Republic of Brazil); and
  - 1.13.4 other information that is specially categorized by Applicable Laws and Regulations.
- 1.14 "Sensitive Information" will mean Confidential Information or Restricted Information.

#### 2. Security Incidents, Incident Response and Notification Procedures

- 2.1 Incident Response Function. COMPANY will maintain an Incident response function capable of identifying, mitigating the effects of, and preventing the recurrence of Incidents. If an Incident occurs (or if PB reasonably suspects and notifies COMPANY that an Incident may have occurred), COMPANY will (i) promptly take all

(version – March 2019)

necessary steps to prevent any further compromise of Sensitive Information or any future Incidents; (ii) notify PB within twenty-four (24) hours of the Incident being identified and provide a written report within three (3) days thereafter; (iii) if a security deficiency has been identified within any information system, coordinate the conduct of an investigation with PB within twenty-four (24) hours; and (iv) respond promptly to any reasonable request from PB for detailed information pertaining to the Incident.

COMPANY's notice to PB may be delayed to the extent that COMPANY has been specifically instructed in writing by a law enforcement or regulatory agency to postpone notice in order to avoid jeopardizing an investigation of the cause of the Incident; provided, however, that COMPANY must present such notice to PB within twenty four (24) hours after the law enforcement agency no longer requires such notice to be delayed. COMPANY agrees not to notify any regulatory authority, nor any customer, on behalf of PB unless PB specifically requests in writing that COMPANY do so. COMPANY will also provide immediate feedback to PB about any impact this possible or actual Incident may or will have on PB or any parties related to the processing described in the Agreement. COMPANY hereby authorizes PB to disclose all information relating to the Incident and compromise of Sensitive Information to PB's affected customers. PB controls the means and timing of all notifications to such affected customers. COMPANY agrees to pay the costs of such notifications.

- 2.2 **Notification Format.** Pursuant to this Exhibit, COMPANY's notification of an Incident will take the form of a phone call to the PB number to be provided or such other PB phone number as is designated in writing by PB.

COMPANY will provide the following information during such notification phone call:

- a. Problem statement including a description of the nature of the Incident, its impact, extent of the Incident, possible systems or databases compromised, any known information about how the Incident occurred;
- b. Investigative, corrective or remedial action that has been taken and any planned investigative, corrective or remedial action. If the corrective action is unknown at the time of the phone call, COMPANY will state this; and
- c. The name and phone number of the COMPANY representative that PB can contact to obtain Incident updates.

- 2.3 **PB Security Resources.** PB may, upon mutual agreement with COMPANY, provide resources from its security group to assist with an identified Incident.

- 2.4 **Incident Logs.** At PB's request, COMPANY will permit PB or its third party auditor to review and verify relevant logs, video surveillance records and data pertaining to any Incident investigation. Upon conclusion of investigative, corrective, and remedial actions with respect to an Incident, COMPANY will prepare and deliver to PB a final report that describes in detail (i) the extent of the Incident; (ii) the Sensitive Information disclosed, destroyed, or otherwise compromised or altered; (iii) all supporting evidence, including system, network, and application logs; (iv) all corrective and remedial actions completed; (v) all efforts taken to mitigate the risks of further Incidents; and (vi) an assessment of the security impact to PB.

- 2.5 **Annual logs.** COMPANY will provide to PB, on an annual basis or more frequently upon PB's request, (1) log data about all use (both authorized and unauthorized) of PB's accounts or credentials provided to COMPANY for use on behalf of PB (e.g., social media account credentials), and (2) detailed log data about any impersonation of, or attempt to impersonate, PB employees or subcontractors or COMPANY Personnel with access to PB Data.

- 2.6 **Reviews.** PB reserves the right to periodically request COMPANY to complete a PB risk assessment questionnaire. Upon PB's written request, COMPANY will certify in writing to PB that it is in compliance with this Exhibit. PB reserves the right to periodically review the security of systems that COMPANY uses to process PB Data. COMPANY will cooperate and provide PB with all required information within a reasonable time frame but no more than twenty (20) calendar days from the date of PB's request. If any security review identifies any deficiencies, COMPANY will, at its sole cost and expense, take all actions necessary to remediate those deficiencies within an agreed upon timeframe.

### **3. Subcontractors**

- 3.1 **Due Diligence over Subcontractors.** As applicable to the Services, COMPANY will maintain a security process to conduct appropriate due diligence prior to utilizing subcontractors to provide any of the Services. COMPANY will monitor the security capabilities of any such subcontractors to ensure COMPANY's ability to comply with this Exhibit and the terms of the Agreement. The due diligence and monitoring elements of this process will provide for (i) the identification and resolution of significant security issues prior to engaging a subcontractor, (ii) written information security requirements within all agreements with such subcontractors, and for (iii) the identification and resolution of any security issues during the Term.

- 3.2 COMPANY shall not subcontract any of its rights or obligations under this Exhibit without the prior written consent of PB. If COMPANY subcontracts its obligations under this Exhibit, COMPANY shall enter into a written agreement with its subcontractor that (i) imposes in all materials respects the same obligations on the subcontractor that are imposed on COMPANY under this Exhibit ("Subcontractor Obligations"), and (ii) does not allow further subcontracting of its obligations. In all events, COMPANY shall remain fully liable to PB for the fulfillment of its obligations under this Exhibit, including any misuse or mishandling of PB Data by its subcontractors. COMPANY acknowledges and agrees that any breach of a Subcontractor Obligation by a subcontractor shall be considered a breach of this Exhibit by COMPANY.

### **4. Physical and Technical Security**

- 4.1 **Secure Facility.** COMPANY will provide proper security, at a minimum to be in accordance with the then-current industry standards and practices, but ultimately as required to ensure reasonable security of the Cargo.

- 4.2 **Administrative, Technical and Physical Safeguards.** COMPANY shall (consistent with the then current industry standards and all Applicable Laws and Regulations) maintain administrative, technical and physical safeguards to protect the security, integrity and confidentiality of PB Data, including the protection of PB Data against any unauthorized or unlawful access to, use of, or disclosure of PB Data. At a minimum, COMPANY shall use (i) install and maintain a working network firewall to protect data accessible via the Internet; (ii) keep its systems and software up-to-date with the latest upgrades, updates, bug fixes, new versions

(version – March 2019)

and other modifications necessary to ensure security of the PB Data; and (iii) use up to date malware software. COMPANY shall provide details of any major changes to its administrative, technical and physical safeguards that may adversely affect the security of any PB Data. Such changes must be communicated in writing to the PB within ten (10) business days prior to the effectiveness of such changes.

4.3 Policies and Training. COMPANY will maintain and enforce information and network policies and will conduct security awareness and training programs covering its policies and practices for all Personnel that will have access to PB Data. Upon request by PB, COMPANY will provide PB with information on violations of COMPANY's information and network policies, even if it does not constitute an Incident.

4.4 Access Controls. COMPANY will secure PB Data by complying with the following requirements:

4.4.1 COMPANY will assign a unique ID to each Personnel with computer access to PB Data.

4.4.2 COMPANY will restrict access to PB Data to only Personnel with a "need-to-know."

4.4.3 COMPANY will follow principle of least privilege allowing access to only the information and resources that are necessary under the terms of the Agreement.

4.4.4 All COMPANY Personnel will have an individual account that authenticates that individual's access to PB Data. COMPANY will not allow sharing of accounts. Access controls and passwords must be configured in accordance with industry standards and best practices.

4.4.5 COMPANY will regularly review, at least once every ninety (90) days, the list of Personnel and services with access to PB Data, and remove accounts that no longer require access.

4.4.6 COMPANY will not use manufacturer-supplied defaults for system passwords and other security parameters on any operating systems, software or other systems that store or process PB Data. COMPANY will mandate and ensure the use of system-enforced "strong passwords" in accordance with the best practices (described below) on all systems hosting, storing, processing, or that have or control access to, PB Data and will require that all passwords and access credentials are kept confidential and not shared among Personnel.

4.4.7 Passwords must meet the following criteria:

4.4.7.1 contain at least eight (8) characters;

4.4.7.2 not match previous passwords, the user's login, or common name;

4.4.7.3 must be changed whenever an account compromise is suspected or assumed; and

4.4.7.4 are regularly replaced after no more than ninety (90) days.

4.4.8 COMPANY will maintain and enforce "account lockout" by disabling accounts with access to PB Data when an account exceeds more than three (3) consecutive incorrect password attempts.

4.4.9 COMPANY will regularly review access logs for signs of malicious behavior or unauthorized access.

4.4.10 COMPANY will deploy an intrusion detection or prevention system (NIDS/NIPS) to generate, monitor and respond to alerts that could indicate an Incident.

4.5 Remote Access. COMPANY will ensure that any access from outside protected corporate or production environments to systems holding PB Data requires multi-factor authentication (e.g., requires at least two separate factors for identifying users).

4.6 Patch Management. COMPANY will patch all workstations and servers with all current operating system, database and application patches deployed in COMPANY's computing environment according to a schedule predicated on the criticality of the patch. COMPANY must perform appropriate steps to help ensure patches do not compromise the security of the information resources being patched. All emergency or critical rated patches must be applied as soon as possible according to provider's critical patch management policy and procedures.

4.7 Physical Security. To the extent COMPANY is operating a Data Center or utilizing a third party Data Center, COMPANY will comply with physical security controls outlined in one or more of the following industry standards: ISO 27001, SSAE 16 or ISAE 3402, or PCI-DSS.

## 5. Data Security

5.1 Transfer of Data. When Sensitive Information or PB Data is transferred between networks pursuant to the Agreement, stored (including on mobile devices/backups) and processed in a non-production environment, it will be encrypted as specified in Section 6 or secured on private networks. Personal Data will be encrypted during transmission on any public network.

5.2 Expiration or Termination. Unless otherwise required by applicable law, upon the later to occur of either the date (i) of expiration or termination of the Agreement plus any Transition Services, (ii) when Sensitive Information and PB Data are no longer required for the purposes of the Agreement or (iii) at any time upon written request from PB, COMPANY will provide a full backup of all data to PB within seventy-two (72) hours. After verification that PB has received and restored the backup data, then COMPANY will (a) promptly remove all Sensitive Information and PB Data from COMPANY's environment and destroy it within a reasonable timeframe, but in no case longer than twenty one (21) days after the above date, (b) clean or destroy all media used to store Sensitive Information and PB Data using information security best practices based on the classification and sensitivity of the Sensitive Information or PB Data, and (c) upon written request from PB, provide PB with a written certification regarding such removal, destruction, and cleaning within thirty (30) days of such occurrence.

5.3 Destruction of Data. COMPANY will dispose of PB Data (including Sensitive Information) when information is deemed no longer necessary to preserve, or has exceeded the time/duration/age utilizing industry best practices for shredding of physical documents and wiping of electronic media (i.e. DoD 5220.22). All

(version – March 2019)

Sensitive Information must be rendered unreadable and unrecoverable regardless of the form (physical or electronic). If COMPANY cannot promptly return, delete or destroy Sensitive Information, COMPANY will protect such Sensitive Information in accordance with the Agreement and this Exhibit for so long as COMPANY retains such Sensitive Information. COMPANY will cause its hosting provider(s) to destroy any equipment containing PB Data that is damaged or non-functional. If COMPANY is required by law to retain archival copies of PB Data for tax or similar regulatory purposes, this archived PB Data must be stored in one of the following ways: (i) as a “cold” or offline (i.e., not available for immediate or interactive use) backup stored in a physically secure facility; or (ii) encrypted, where the system hosting or storing the encrypted file(s) does not have access to a copy of the key(s) used for encryption.

### 6. Cryptography

6.1 COMPANY will utilize Industry Standard Encryption Algorithms and Key Strengths to encrypt the following:

6.1.1 All Sensitive Information that is in electronic form while in transit over all public wired networks (i.e. Internet) and all wireless networks.

6.1.2 All PB Data and Sensitive Information while In Storage in accordance with industry best practices.

6.2 Passwords will be hashed with industry standard algorithms as defined by OWASP (i.e. SHA256) with randomly generated “salt” added to the input string prior to encoding to ensure that the same password text chosen by different users will yield different encodings. The randomly generated salt should be at least as long as the output of the hash function.

6.3 Where encryption is utilized, COMPANY will maintain a key management process that includes appropriate access controls to limit access to private keys (both synchronous and asynchronous) and a key revocation process when COMPANY has reason to believe that encryption keys are compromised. Private keys must not be stored on the same media as the data they protect.

### 7. Vulnerability Management

7.1 COMPANY will run internal and external network vulnerability scans quarterly and after any material change in the network configuration (e.g., new system component installations, changes in network topology, firewall rule modifications, or product upgrades).

7.2 For all internet-facing applications that collect, transmit or display Sensitive Information, COMPANY agrees to conduct an application security assessment review to identify common security vulnerabilities as identified by industry-recognized organizations (i.e. OWASP Top 10 Vulnerabilities; CWE/SANS Top 25 vulnerabilities) annually or for all major releases, whichever occurs first. The scope of the security assessment will primarily focus on application security including a penetration test of the application, as well as a code review.

7.3 At a minimum, the security assessment will cover the OWASP Top 10 Vulnerabilities (<https://www.owasp.org>) and the following common security vulnerabilities:

- Injection
- Cross Site Scripting (XSS)
- Broken Authentication and Session Management
- Insecure Direct Object References
- Cross Site Request Forgery (CSRF)
- Security Misconfiguration
- Insecure Cryptographic Storage
- Failure to Restrict URL Access
- Insufficient Transport Layer Protection
- Unvalidated Redirects and Forwards
- Clickjacking
- Insufficient Authorization (TCv2)
- Embedded 3rd-party content

7.4 For all mobile applications (i.e. running on Android, Blackberry, iOS, Windows Phone) that collect, transmit or display PB Data, COMPANY shall conduct an application security assessment review to identify and remediate industry-recognized vulnerabilities specific to mobile applications.

7.5 COMPANY should utilize a qualified third-party to conduct the application security assessments. COMPANY may conduct the security assessment review themselves, provided that COMPANY Personnel are sufficiently trained, follow industry standard best practices, and the assessment process is reviewed and approved by PB. Vulnerabilities identified and rated as high risk by COMPANY will be remediated within ninety (90) days of discovery.

### 8. Business Continuity and Disaster Recovery

8.1 COMPANY represents and warrants that it has a documented business continuity plan, which includes advance arrangements and procedures to access tracking data (including, but not limited to, proof of delivery data) at all times including during an event or occurrence that could suspend, delay, inhibit or prevent COMPANY’s performance under the Agreement.

8.2 If COMPANY performs a “recovery” (i.e., reverting to a backup) for the purpose of disaster recovery, COMPANY will have and maintain a process that ensures that all PB Data that is required to be deleted pursuant to this Exhibit will be re-deleted or overwritten from the recovered data in accordance with this Exhibit

## Logistics Services Terms and Conditions

(version – March 2019)

within twenty-four (24) hours after recovery occurs. If COMPANY performs a recovery for any purpose, no PB Data may be recovered to any third party system or network without PB's prior written approval.

### 9. Data Storage

- 9.1 Except as expressly authorized under the Agreement, COMPANY (i) will isolate PB Data at all times (including in storage, processing or transmission) from COMPANY's and any third party information; and (ii) will not Aggregate any PB Data, even if Anonymized.
- 9.2 COMPANY shall establish and maintain appropriate network segmentation, including the use of virtual local area networks (VLANS) where appropriate, to restrict network access to systems storing PB Data. COMPANY will proxy all connections from public networks into the COMPANY's internal network using DMZ or equivalent. COMPANY will not allow direct connections from public networks into any network segment storing PB Data.

### 10. Access

- 10.1 Extranet. As applicable, PB may grant COMPANY access to PB Data via web portals or other non-public websites or extranet services on PB's or a third party's website or system (each, an "Extranet"). If PB permits COMPANY to access any PB Data using an Extranet, COMPANY must comply with the following requirements:
  - 10.1.1 Permitted Purpose. COMPANY and its Personnel will access, collect, use, view, retrieve, download or store PB Data from the Extranet solely for the purposes of the Agreement.
  - 10.1.2 Accounts. COMPANY will ensure that COMPANY Personnel use only the Extranet account(s) designated for each individual by PB and will require COMPANY Personnel to keep their access credentials confidential.
  - 10.1.3 Systems. COMPANY will access the Extranet only through computing or processing systems or applications that are (i) running operating systems managed by COMPANY; and (ii) in compliance with this Exhibit, including Section 4.2. Portable devices shall use full disk encryption.
  - 10.1.4 Restrictions. Except if approved in advance in a writing by PB, COMPANY will not download, mirror or permanently store any PB Data from any Extranet on any medium, including any machines, devices or servers.
  - 10.1.5 Account Termination. COMPANY will terminate the account of each of COMPANY Personnel and notify PB no later than twenty-four (24) hours after any specific COMPANY Personnel, who has been authorized to access any Extranet, (a) no longer needs access to PB Data or (b) no longer qualifies as COMPANY Personnel.
  - 10.1.6 Third Party Systems. COMPANY will give PB prior notice and obtain PB's prior written approval before it uses any third party system that stores or may otherwise have access to PB Data, unless a) the PB Data is encrypted in accordance with this Exhibit, and b) the third party system will not have access to the decryption key or unencrypted "plain text" versions of the PB Data. If COMPANY uses any third party systems that store or otherwise may access unencrypted PB Data, COMPANY must perform a security review of the third party systems and their security controls and will provide PB periodic reporting about the third party system's security controls in the format requested by PB (e.g., SAS 70 or its successor report), or other recognized industry-standard report approved by PB).

### 11. Personal Data

- 11.1 COMPANY warrants and agrees to cooperate with and promptly assist PB, through appropriate organizational, technical, and physical measures, insofar as this is possible and at no charge to PB, in meeting its obligations to Data Subjects and regulatory authorities, including Data Protection Authorities.
- 11.2 COMPANY shall not disclose PB Personal Data to any third party in any circumstances other than in compliance with PB's processing instructions (and only to the extent permitted by the disclosure notice provided to the Data Subject at the time of collection of such Personal Data). To the extent legally permitted, COMPANY shall immediately notify PB in writing upon receipt of an order, demand, or document purporting to request, demand or compel the production of PB Personal Data to any third party. To the extent legally permitted, COMPANY shall not disclose PB Personal Data to the third party without providing PB at least twenty-four (24) hours' notice, so that PB may, at its own expense, exercise such rights as it may have under Applicable Laws and Regulations to prevent or limit such disclosure. Notwithstanding the foregoing, COMPANY will exercise commercially reasonable efforts to prevent and limit any such disclosure and to otherwise preserve the confidentiality of PB Personal Data; additionally, COMPANY will cooperate with PB with respect to any action taken pursuant to such order, demand, or other document request, including to obtain an appropriate protective order or other reliable assurance that confidential treatment will be accorded to PB Personal Data.
- 11.3 Where applicable, COMPANY represents and warrants that it has notified the relevant Data Protection Authorities of COMPANY's data processing activities and will provide PB with the registration number upon request. COMPANY further warrants that it will maintain this registration and where necessary renew it during the term of the applicable Ordering Document. Any changes to COMPANY's status in this respect shall be notified to PB immediately.

### 12. Operations

- 12.1 In the event COMPANY is assigned PB equipment for use (including, without limitation, laptop computer, desktop computer, thin client terminal, VPN token, mobile phone, tablet, or other equipment) and/or permitted remote access (e.g., VPN, direct connection, etc.) to any internal PB (or its client's) systems (including, without limitation, hardware, software, data, servers, personal computer or control devices, software or other systems directly owned by PB or by third parties in which PB has provisioned the use of through contractual agreement), services, or networks (collectively, "PB Systems"), Service Provider shall:
  - 12.1.1 Not connect to, access or use (nor attempt to do any of the foregoing) any PB Systems without the prior authorization of PB;



**Logistics Services Terms and Conditions**

(version – March 2019)

- 12.1.2 Not enable bridging of any PB network (e.g., PB intranet, etc.) with any other network;
- 12.1.3 Not use shared personal accounts;
- 12.1.4 Not attempt to gain unauthorized access to any systems, infrastructure, or other user's account;
- 12.1.5 Not store the PIN or password in the VPN client configuration when using two-factor authentication to the PB network; and
- 12.1.6 Not physically store hardware-based authenticators for remote access with the device used to connect to the PB network when not in use.
- 12.2 COMPANY shall be responsible for all assigned PB equipment issued or in their possession or control. Such equipment must be secured against removal or theft. COMPANY shall report to PB, within twenty-four (24) hours when such equipment is lost, stolen, or otherwise compromised. Information and classification of the information contained on the computer/computer equipment must be identified.
- 12.3 COMPANY shall return any assigned PB equipment when no longer required to complete the Services, if the Agreement is terminated, or immediately upon PB's request. PB equipment will be returned to PB within twenty-four (24) hours when COMPANY Personnel no longer require access. PB may take all action deemed appropriate to recover or protect its property.
- 12.4 If COMPANY is sending emails to PB customers or employees, appropriate email identity solutions, including but not limited to DKIM, SPF, and DMARC, will be utilized. If PB utilizes PB-owned (or a PB customer owned) domain names to send emails, COMPANY will adhere to the PB Email Security requirements, provided upon request.
- 13. **Hub Operations.** If PB provides COMPANY with an "Advanced Search App" that enables COMPANY Personnel and agents at the COMPANY parcel processing hub to identify unknown parcels, the Advanced Search App will store PB user order information for a limited number of days in an unencrypted format, and will be published to an unencrypted in-memory cache. COMPANY shall limit order information that is stored and published to that information which is necessary to identify a parcel and in no event shall such information include Restricted Information. Users of the Advanced Search App will be required to furnish application security credentials to utilize the Advanced Search App, and access will be limited to only certain IP addresses.
- 14. **Survival Rights.** These terms and conditions in this Exhibit shall survive as long as COMPANY and/or its Personnel retains any PB Data.