

**ENTERPRISE SAAS SOFTWARE/SERVICES LICENSE  
REQUIREMENTS AGREEMENT  
BETWEEN  
THE COMMONWEALTH OF PENNSYLVANIA,  
ACTING BY AND THROUGH THE GOVERNOR'S OFFICE OF ADMINISTRATION  
AND  
PITNEY BOWES, INC.**

---

This Enterprise SaaS Software/Services License Requirements Agreement ("Agreement") is entered into by and between Pitney Bowes, Inc. ("Licensor") and the **Commonwealth of Pennsylvania**, acting by and through the **Governor's Office of Administration** ("Commonwealth").

The parties intending to be legally bound, agree as follows:

- 1. Order of Precedence.** The terms and conditions of this Agreement, to the extent a conflict exists, supersede and take precedence over the terms and conditions of the Licensor On-Demand Subscription Services Agreement, which is attached to this Agreement as Exhibit A. The terms of this Agreement supersede and take precedence over the terms included in any quote, purchase order, terms of any shrink-wrap agreement included with the Licensed Products, terms of any click through agreement included with the Licensed Products or any other terms purported to apply to the Licensed Products. The products specified in Attachment 1, along with maintenance, support and services for said products, shall be referred to as "Licensed Products."
- 2. Effective Date.** The effective date of this Agreement shall be the date that it has been fully executed by the Licensor and by the Commonwealth and all approvals required by Commonwealth contracting procedures have been obtained.
- 3. Enterprise Language.**
  - (a) The parties agree that more than one agency of the Commonwealth ("Commonwealth Agency") may license products subject to this Agreement, provided that the procurement of any Licensed Products by any Commonwealth Agency must be made pursuant to one or more executed purchase orders or purchase documents submitted by each Commonwealth Agency seeking to use the Licensed Products.
  - (b) The parties agree that, if the licensee is a "Commonwealth Agency" as defined by Section 103 of the *Commonwealth Procurement Code*, 62 Pa. C. S. § 103, the terms and conditions of this Agreement apply to the procurement of any Licensed Products made by the Commonwealth, and that the terms and conditions of this

Agreement become part of the purchase order or other procurement document without further need for execution.

**4. List of Licensed Products.**

- (a) Attached hereto and made a part of this Agreement by reference is Attachment 1, which lists the Licensed Products that may be licensed under this Agreement. With the consent of the Commonwealth, the list of Licensed Products on Attachment 1 may be updated by the Licenser providing the Commonwealth with a revised Attachment 1 that adds the new product to the list. The Commonwealth, in its sole discretion, may consent either via written communication directly to the Licenser or, if applicable, providing the Commonwealth's reseller with a copy of Licenser's notification to update Attachment 1.
- (b) No amendment will be required to add a new Licensed Product to the list. If, however, the Licenser desires to add a new Licensed Product to the list that requires additional licensing terms or other requirements, either an amendment to this Agreement or a new agreement will be required.

**5. Applicable Law and Forum.** This Agreement is governed by and must be interpreted and enforced in accordance with the laws of the Commonwealth of Pennsylvania (without regard to any conflict of laws provisions) and the decisions of the Pennsylvania courts. The Licenser consents to the jurisdiction of any court of the Commonwealth of Pennsylvania and any federal courts in Pennsylvania, and waives any claim or defense that such forum is not convenient or proper. Any Pennsylvania court or tribunal has in personam jurisdiction over the Licenser, and the Licenser consents to service of process in any manner authorized by Pennsylvania law. This provision may not be interpreted as a waiver or limitation of the Commonwealth's rights or defenses.

**6. Indemnification.**

- (a) **Licenser Obligations.** The Licenser shall indemnify the Commonwealth against all third-party claims, suits, demands, losses, damages, costs, and expenses, including without limitation, litigation expenses, attorneys' fees, and liabilities, to the extent arising out of or in connection with any negligent or intentional act or omission of the activities performed by the Licenser or its employees and agents that are directly related to the use of the software that is provided under this Agreement.
- (b) **Commonwealth Attorneys Act.** The Commonwealth shall provide the Licenser with prompt notice of any claim or suit of which it learns. Pursuant to the Commonwealth Attorneys Act (71 P.S. Section 732-101, et seq.), the Office of Attorney General (OAG) has the sole authority to represent the Commonwealth in actions brought against the Commonwealth. The OAG may, however, in its sole discretion and under any terms as it deems appropriate, delegate its right of defense.

If OAG delegates the defense to the Licensor, the Commonwealth will cooperate with all reasonable requests of Licensor made in the defense of such suits.

- (c) **Settlement.** Notwithstanding the above, neither party may enter into a settlement of any claim or suit without the other party's written consent, which will not be unreasonably withheld. The Commonwealth may, in its sole discretion, allow the Licensor to control the defense and any related settlement negotiations.

## **7. Sovereign Immunity.**

No provisions of this Agreement may be construed to waive or limit the sovereign immunity of the Commonwealth of Pennsylvania or its governmental sub-units.

## **8. Patent, Copyright, Trademark and Trade Secret Protection.**

- (a) The Licensor shall, at its expense, defend, indemnify and hold the Commonwealth harmless from any suit or proceeding which may be brought by a third party against the Commonwealth, its departments, officers or employees for the alleged infringement of any United States patents, copyrights, trademarks or trade dress, or for a misappropriation of a United States trade secret arising out of performance of this Agreement ("Claim"), including all Licensed Products provided by the Licensor. For the purposes of this Agreement, "indemnify and hold harmless" shall mean the Licensor's obligation to (a) pay any judgments, fines and penalties finally awarded by a court of competent jurisdiction, governmental/administrative body or any settlements reached pursuant to a Claim and (b) reimburse the Commonwealth for its reasonable administrative costs or expenses, including without limitation reasonable attorney's fees, it necessarily incurs in handling the Claim. The Commonwealth shall give the Licensor prompt notice of any such claim of which it learns. Pursuant to the [Commonwealth Attorneys Act](#), Act of October 15, 1980, P.L. 950, No. 164, as amended, 71 P. S. §§ 732-101—732-506, the Office of Attorney General ("OAG") has the sole authority to represent the Commonwealth in actions brought against the Commonwealth. The OAG, however, in its sole discretion, and under the terms the OAG deems appropriate, may delegate its right of defense of a Claim. If the OAG delegates the defense to the Licensor, the Commonwealth will cooperate with all reasonable requests of the Licensor made in the defense of and/or settlement of a Claim. The Licensor shall not, without the Commonwealth's consent, enter into any settlement agreement which (a) states or implies that the Commonwealth has engaged in any wrongful or improper activity other than the innocent use of the material which is the subject of the Claim, (b) requires the Commonwealth to perform or cease to perform any act or relinquish any right, other than to cease use of the material which is the subject of the Claim, or (c) requires the Commonwealth to make a payment which the Licensor is not obligated by this Agreement to pay on behalf of the Commonwealth. In all events, the Commonwealth shall have the right to participate in the defense of any such suit or proceeding through counsel of its own choosing. It is expressly agreed by the Licensor that, in the event it requests that the Commonwealth provide support

to the Licensor in defending any such Claim, the Licensor shall reimburse the Commonwealth for all necessary expenses (including attorneys' fees, if such are made necessary by the Licensor's request) incurred by the Commonwealth for such support. The Licensor, at its own expense, shall provide whatever cooperation the OAG requests in the defense of the Claim.

- (b) The Licensor shall exercise reasonable due diligence to prevent claims of infringement on the rights of third parties. The Licensor certifies that, in all respects applicable to this Agreement, it has exercised and will continue to exercise due diligence to ensure that all Licensed Products provided under this Agreement do not infringe on the patents, copyrights, trademarks, trade dress, trade secrets or other proprietary interests of any kind which may be held by third parties.
- (c) If the defense of a Claim and the authority to control any potential settlements of a Claim is delegated to the Licensor, the Licensor shall pay all damages and costs finally awarded against the Commonwealth or agreed to by the Licensor in any settlement. If information and assistance are furnished by the Commonwealth at the Licensor's written request, it shall be at the Licensor's sole expense.
- (d) If any Licensed Product furnished hereunder is likely to (in the Licensor's opinion) or does become subject to a claim of infringement of a United States patent, copyright, trade dress or trademark, or for a misappropriation of trade secret, or is held to constitute infringement and the use of the Licensed Product is enjoined, without diminishing the Licensor's obligation to satisfy any final award, the Licensor may, at its option and expense:
  - (i) Replace or substitute functional equivalents for the Licensed Product;
  - (ii) Modify the Licensed Product so that it is no longer infringing;
  - (iii) Re-perform the Services in a non-infringing manner; or
  - (iv) obtain the rights necessary for the Licensor to continue performance under this Agreement or obtain the rights for the Commonwealth to continue the use of the Licensed Product.
- (e) If the use of any Licensed Product is enjoined and the Licensor is unable to provide any remedy set forth in subsection (d) above, the Licensor, upon return of the Licensed Product, shall refund to the Commonwealth:
  - (i) the fee paid for the infringing Licensed Product, less the amount for the period of usage of the Licensed Product; and
  - (ii) the pro-rated portion of any maintenance fees representing the time remaining in any period of services for which payment was made.

- (f) The obligations of the Licensor under this section survive the termination of this Agreement.
- (g) Notwithstanding the above, the Licensor shall have no obligation under this section to the extent a Claim arises from:
  - (i) modification of any Licensed Products provided by the Commonwealth or Commonwealth Agency or a third party acting under the direction of the Commonwealth or Commonwealth Agency;
  - (ii) any material provided by the Commonwealth or Commonwealth Agency to the Licensor and incorporated into, or used to prepare any Licensed Products;
  - (iii) use of any Licensed Product after the Licensor recommends discontinuation because of possible or actual infringement and has provided one of the remedies under subsection (e) or subsection (f) above;
  - (iv) use of any Licensed Product in other than the specified operating environment;
  - (v) the combination, operation, or use of the Licensed Products with other products, services, or deliverables not provided by the Licensor as a system or the combination, operation, or use of the Licensed Products, service, or deliverable, with any products, data, or apparatus that the Licensor did not provide;
  - (vi) infringement of a non-Licensed Product alone;
  - (vii) the Commonwealth's or Commonwealth Agency's use of any Licensed Product beyond the scope contemplated by the Agreement; or
  - (viii) the Commonwealth's or Commonwealth Agency's failure to use the most current release of the Licensed Products corrections or enhancements made available to the Commonwealth or Commonwealth Agency by the Licensor at no charge.

**9. Virus, Malicious, Mischievous or Destructive Programming.**

- (a) The Licensor warrants that the Licensed Products as delivered by the Licensor does not contain any viruses, worms, Trojan Horses, or other malicious or destructive code to allow unauthorized intrusion upon, disabling of, or erasure of the Licensed Products (each a "Virus"). However, the Licensed Products may contain a key limiting use to the scope and quantity of the license(s) granted, and license keys issued by the Licensor for temporary use are time-sensitive.

- (b) The Licensor shall be liable to the Commonwealth for any damages, costs, fines, remedial measures incurred by the Commonwealth and shall indemnify the Commonwealth against any Third Party claims (in accordance with Section 6, Indemnification) if the Licensor or any of its employees, subcontractors or consultants introduces a virus or malicious, mischievous or destructive programming into the Licensed Product or the Commonwealth's or Third Party's software, data, systems or computer networks.

## **10. Limitation of Liability.**

- (a) Except as otherwise provided in this Agreement, the Licensor's liability to the Commonwealth under this Agreement shall be limited to the greater of \$500,000 or the total dollar amount of purchase orders issued for Licensed Products and services covered by this Agreement during the twelve (12)-month period prior to the event giving rise to the damage claim. This limitation does not apply to damages:
- (b)
  - (i) for bodily injury;
  - (ii) for death;
  - (iii) for gross negligence and willful or unlawful misconduct;
  - (iv) to real property or tangible personal property for which the Licensor is legally liable;
  - (v) under Section 8, [Patent, Copyright, Trade Secret and Trademark Protection](#);
  - (vi) resulting from a breach of the security of a system maintained or managed by the Licensor, including the costs for notification, mitigation and credit monitoring services required due to such breach;
  - (vii) resulting from a breach of confidentiality;
  - (viii) for which the Licensor is responsible pursuant to any indemnification obligations it has under this Agreement; or
  - (ix) under Section 9, [Virus, Malicious, Mischievous or Destructive Programming](#).
- (c) Except with respect to those damages enumerated in subsection 10(a)(i) through (ix) above, the Licensor shall not be liable for consequential, indirect, or incidental damages unless otherwise specified in the Agreement.

## **11. Payment.**

The Commonwealth will make purchase and make payment through a reseller contract or another procurement document, which shall control with regard to payment amounts and provisions.

## **12. Termination.**

- (a) Licensors may suspend the services set forth in an Order entered into under this agreement if required by law or regulation or due to a security issue, where Security Issue is defined as: (i) use of the services which causes disruption to the Commonwealth's use of the services, other customers' use of the services, or the network or servers used to provide the services; or (ii) unauthorized use or access of the services.
- (b) Upon termination or expiry of this Agreement, Licensee will stop using the Licensed Products and Licensee will irretrievably delete and/or remove them from Licensee's Computer systems and, if not deleted and/or removed, return the Licensed Products and Documentation together with all copies to Licensors; and upon request, Licensee will certify compliance with this Section in writing.
- (c) The Commonwealth may terminate this Agreement without cause by giving the Licensors **30 calendar days'** prior written notice ("Notice of Termination") whenever the Commonwealth shall determine that such termination is in the best interest of the Commonwealth ("Termination for Convenience"). Notwithstanding the foregoing, any purchase orders or other procurement document issued during the term of a current procurement vehicle shall continue for the duration of the specific purchase order or other procurement document, unless the purchase order or other procurement document is terminated in accordance with the terms of the applicable procurement document.
- (d) A party may terminate this Agreement if the other party commits a material breach of this Agreement and fails to cure the breach within 30 days after receipt of written notice of the breach, or if either party becomes insolvent or files for bankruptcy.

## **13. Background Checks.**

- (a) Upon prior written request by the Commonwealth, the Licensors must, at its expense, arrange for a background check for each of its employees, as well as for the employees of its subcontractors, who will have access to Commonwealth Confidential Information or Commonwealth facilities, either through on site or remote access. Licensors perform the following pre-employment screenings:
  - Drug Screening
  - Social Security Number trace

- Verification of previous employment
  - Review of academic qualifications
  - Review of professional qualifications
  - Checking Criminal-background
  - Credit reports
- (b) The background check shall be conducted prior to initial access by the Licensor employee.
- (c) Before the Commonwealth permits an employee access to the Commonwealth Confidential Information or Commonwealth facilities, the Licensor must provide written confirmation to the office designated by the applicable Commonwealth Agency that the background check has been conducted. If, at any time, it is discovered that an employee has a criminal record that includes a felony or misdemeanor involving terrorist threats, violence, use of a lethal weapon, or breach of trust/fiduciary responsibility; or which raises concerns about building, system, or personal security, or is otherwise job-related, the Licensor shall not assign that employee to any Commonwealth facilities, shall remove any access privileges already given to the employee, and shall not permit that employee remote access to Commonwealth facilities, systems or Confidential Information, unless the Commonwealth Agency consents, in writing, prior to the access being provided. The Commonwealth Agency may withhold its consent at its sole discretion. Failure of the Licensor to comply with the terms of this subsection may result in the default of the Licensor under its Agreement with the Commonwealth.
- (d) The Commonwealth specifically reserves the right to conduct background checks over and above that described herein.

#### **14. Confidentiality.**

- (a) Definition. “Confidential Information:”
- (i) For the Commonwealth: Information, whether oral or written or via computer disk or electronic media, to which the Licensor is given access, or which is made available by the Commonwealth, whether directly or through a third party, is defined as "Confidential Information." Confidential Information shall include, without limitation, all technology, know-how, processes, software, databases, Trade Secrets (as defined by the Pennsylvania Uniform Trade Secret Act found at 12 Pa. Cons. Stats Secs. 5392 et. seq.), proprietary information, product and business requirements, and information about or from the Commonwealth’s vendors or employees whether received before or after the Effective Date of this Agreement.



Confidential Information shall also include information and documentation that is not permitted to be disclosed to third parties under local, Commonwealth or federal laws and regulations or pursuant to any policy adopted by the Commonwealth or pursuant to the terms of any third-party agreement to which the Commonwealth is a party. Sensitive information, as define in Section 15 below, shall be a subset of Confidential Information of the Commonwealth, and shall be subject to additional protections as set forth in Section 15 below.

(ii) For the Licensor: All information identified in writing by the Licensor as confidential or proprietary to the Licensor or its subcontractors.

(b) Confidential Information. All Confidential Information of or relating to the disclosing party shall be held in confidence by the receiving party to the same extent and in at least the same manner as the receiving party protects its own confidential or proprietary information, using no less than commercially reasonable standards or higher or more stringent standards required by law, including those laws governing Sensitive Information, and those standard specified in this Agreement. The receiving party shall not disclose, publish, release, transfer or otherwise make available any Confidential Information of the disclosing party in any form to, or for the use or benefit of, any person or entity without the disclosing party's consent. Subject to the other provisions of this Agreement, receiving party shall be permitted to disclose relevant aspects of the disclosing party's Confidential Information to the receiving party's officers, agents, subcontractors and personnel and to the officers, agents, subcontractors and personnel of the receiving party's corporate affiliates or subsidiaries to the extent that such disclosure is reasonably necessary for the performance of the receiving party's duties and obligations under this Agreement; provided, however, that the receiving party shall take all reasonable measures to ensure that Confidential Information of the disclosing party is not disclosed or duplicated in violation of the provisions of this Agreement by such officers, agents, subcontractors and personnel and that the receiving party shall be responsible for any unauthorized disclosure of the Confidential Information by the receiving party's officers, agents, subcontractors or personnel; and further provided, that if the disclosure is by the Commonwealth to another contractor or sub-contractor, such disclosure is subject to a suitable non-disclosure agreement imposing equally or more stringent requirements for data privacy and security. Except for Sensitive Information (which shall be protected in all circumstances), and except to the extent provided otherwise by any applicable law, the obligations of this subsection (b) shall not apply with respect to information that:

- (i) is developed by the other party without violating the disclosing party's proprietary rights;
- (ii) is or becomes publicly known,

- (iii) is disclosed by the owner of such information to a third party free of any obligation of confidentiality;
  - (iv) is already known by the receiving party without an obligation of confidentiality other than pursuant to this Agreement or any confidentiality contract entered into before the Effective Date of the Agreement between the Commonwealth and the Licensor; or
  - (v) is rightfully received by the receiving party free of any obligation of confidentiality.
- (c) Obligations. Each party shall:
- (i) notify the other party promptly of any known unauthorized possession, use or knowledge of the other party's Confidential Information by any person or entity;
  - (ii) promptly furnish to the other party full details known by such party relating to the unauthorized possession, use or knowledge thereof and shall use reasonable efforts to assist the other party in investigating or preventing the recurrence of any unauthorized possession, use or knowledge of the other party's Confidential Information;
  - (iii) use reasonable efforts to cooperate with the other party in any litigation and investigation against third parties deemed necessary by the other party to protect its proprietary rights; and
  - (iv) promptly use all reasonable efforts to prevent a recurrence of any such unauthorized possession, use or knowledge of the other party's Confidential Information.
- (d) Cost of compliance; required disclosure. Each party shall bear the cost it incurs as a result of compliance with this section. The obligations in this section shall not restrict any disclosure by either party pursuant to any applicable law or pursuant to the order of any court or other legal process or government agency of competent jurisdiction (provided that the receiving party shall give prompt notice to the non-disclosing party of such disclosure or order in a timeframe to allow the disclosing party to resist the disclosure or order).
- (e) Submitting Confidential Information to the Commonwealth. The Licensor shall use the following process when submitting information to the Commonwealth that it believes to be confidential and/or proprietary information or trade secrets:
- (i) prepare an un-redacted version of the appropriate document;

- (ii) prepare a redacted version of the document that redacts the information that is asserted to be confidential or proprietary information or a trade secret;
- (iii) prepare a signed written statement that states:
  - (1) the attached document contains confidential or proprietary information or trade secrets;
  - (2) the Licensor is submitting the document in both redacted and un-redacted format in accordance with Section 707(b) of the *Right-to-Know Law*, 65 P.S. § 67.707(b); and
  - (3) the Licensor is requesting that the document be considered exempt under Section 708(b)(11) of the *Right-to-Know Law*, 65 P.S. § 67.708(b)(11) from public records requests; and
- (iv) submit the **two (2)** documents with the signed written statement to the Commonwealth.
- (f) Confidential Information at termination. Upon expiration or termination of this Agreement, or a purchase order or other procurement document for Licensed Products governed by the terms of this Agreement, and at any other time at the written request of a party, the receiving party must promptly return to the disclosing party all of the disclosing party's Confidential Information and Data (and all copies of this information) that is in the receiving party's possession or control, regardless of form.
- (g) Not confidential. Additionally, neither this Agreement, nor purchase orders issued pursuant to this Agreement, will be deemed confidential.

## **15. Sensitive Information.**

- (a) "Sensitive Information" is a subcategory of Confidential Information of the Commonwealth and shall include, regardless of whether marked or identified by the Commonwealth as confidential:
  - (i) Information related to the design or implementation of the Commonwealth's technology and security infrastructure and architecture,

including, but not limited to, Protected Critical Infrastructure Information (PCII) under the Cybersecurity Information Sharing Act (CISA) of 2015;

- (ii) Information identified as Sensitive Security Information, Protected Information or Privileged Information as defined in the Commonwealth's *Data Classification Policy*;
  - (iii) Passwords, encryption keys, and other cyber security control design information;
  - (iv) Consumer and citizen information;
  - (v) Employee information;
  - (vi) Information that is either nonpublic personal information or personally identifiable information, including, without limitation, names, addresses, telephone numbers, fax numbers, electronic mail addresses, web universal resource locators (URLs), Internet Protocol (IP) addresses, vehicle identifiers, account numbers, birthdates, social security numbers, individual likeness or images, fingerprint or biometric data, genetic information, demographic, information contained in, relating to or deriving from medical or personal health records, criminal justice information and records, information relating to drivers licenses or other identification cards, financial and transactional information, tax information and any other information that is deemed to be nonpublic or protected under federal and state law, regulation, order or standard including, but not limited to, the Criminal History Record Information Act, the Family Education Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), Confidentiality of HIV-Related Information Act, the Omnibus Reconciliation Act of 1990, Real ID Act of 2005, Tax Reform Act of 1976 the Internal Revenue Code and IRS Publication 1075, the Affordable Care Act, federal and state notification laws, The Driver's Privacy Protection Act of 1994, Title V of the *Gramm-Leach-Bliley Act*, Section 628 of the *Fair Credit Reporting Act*, Section 216 of the Fair and Accurate Credit Transactions Act, the *Children's Online Privacy Protection Act*, and any implementing regulations, guidelines and Commonwealth policies adopted under any of these or other related laws; and
  - (vii) Payment Card Industry Information (PCI).
- (b) The Licensor understands that its level of access may allow or require it to view or access Sensitive Information and Confidential Information. The Licensor shall hold all Commonwealth Sensitive Information in the strictest of confidence and shall use all protective measures to protect the Sensitive Information as prescribed by law, regulation and/or Commonwealth policies and standards. In addition, the Licensor shall only permit staff located in the United States to access Sensitive

Information, Confidential Information and Commonwealth systems, data and services.

- (c) Sensitive Information and Confidential Information may be subject to and governed by specific state and federal laws, regulations and policies that must be followed. If applicable, prior to deployment of the Products or Services, the Licensor may be required to sign off on particular instructions, restrictions and limitations as dictated by the Commonwealth, including, but not limited to, as necessary, HIPAA Business Associate Agreements. The Commonwealth's use of any sign off sheet shall create specificity in the Licensor's obligations with respect to certain Confidential Information, and this Section and the instructions within the sign-off sheet shall not, in any way, diminish the obligations of the Licensor under this Agreement with respect to Confidential Information generally and Sensitive Information specifically. The sign-off sheet shall be signed by at least one authorized signatory for the Licensor and incorporated into this Agreement.

## 16. Data Breach or Loss.

- (a) Compliance with Laws. The Licensor shall comply with all applicable data protection, data security, data privacy and data breach notification laws, including, but not limited to, the *Breach of Personal Information Notification Act*, as amended November 2, 2022, P.L. 2139, No. 151, 73 P.S. §§ 2301—2330. Further, to the extent the Licensor maintains, stores, or manages computerized data on behalf of the Commonwealth that constitutes personal information, as defined in the *Breach of Personal Information Notification Act*, the Licensor shall comply with the then current version of the following IT Policies (ITPs): *Data Classification Policy*, *IT Incident Reporting Policy*, and *Encryption Policy*.
- (b) Control of Licensor. For Data and Confidential Information in the possession, custody, and control of the Licensor or its employees, agents, and/or subcontractors:
  - (i) The Licensor shall report unauthorized access, acquisition, use, release, loss, destruction or disclosure of Data or Confidential Information ("Incident") to the Commonwealth within twenty-four (24) hours of when the Licensor knows of such Incident, and the Licensor must immediately take all reasonable steps to mitigate any potential harm or further access, acquisition, use, release, loss, destruction or disclosure of such Data or Confidential Information.
  - (ii) The Licensor shall provide timely notice to all individuals that may require notice under any applicable law or regulation as a result of an Incident. The notice must be pre-approved by the Commonwealth. At the Commonwealth's request, the Licensor shall, at its sole expense, provide credit monitoring services to all individuals that were impacted by any Incident requiring notice and such individuals opt-in to such credit monitoring services.

- (iii) The Licensor shall be solely responsible for any costs, losses, fines, or damages incurred by the Commonwealth due to Incidents, which shall be reimbursed upon invoice received from the Commonwealth.
  - (iv) The Licensor shall indemnify the Commonwealth against any third party claims arising out of an Incident.
  - (c) Security Breach. Licensor agrees that it shall not inform any third party (other than any third party that is employed by Licensor to help remediate the Security Breach) of any Security Breach specific to Commonwealth's data without first obtaining the Commonwealth's prior, written consent, other than to inform a complainant that the matter has been forwarded to the Commonwealth's legal counsel unless required by law or regulation to do so. Further, the Licensor agrees that the Commonwealth shall have the sole right to determine: the contents of such notice, whether any type or remediation may be offered to affected persons, and the nature and extent of any such remediation unless required by law or regulation for the Licensor to do so.
  - (d) Diligent Performance and Cooperation. The Licensor shall diligently perform all of the duties required in this Section in cooperation with the Commonwealth.
  - (e) The requirements of this section are in addition to and not in lieu of other requirements of this Agreement and its Attachments and Exhibits having to do with data privacy and security, including but not limited to the requirement that the Licensor comply with Attachment 2, *Requirements for Non-Commonwealth Hosting Applications/Services*, and all applicable Commonwealth Information Technology Policies (ITPs), which can be found at: <http://www.oa.pa.gov/Policies/Pages/itp.aspx>.
17. **Hyperlink Content.** Any terms and conditions contained in any hyperlink content referenced in this Agreement ("Hyperlink Content") shall not apply to the extent such terms and conditions are expressly prohibited by applicable law. In addition, no financial obligation of the Commonwealth to Licensor shall be affected by any change to information contained in a hyperlink, nor will any additional material obligations be placed on the Commonwealth as a result of any such changes to Hyperlink Content. Terms and conditions in the Hyperlink Content that are materially inconsistent with the Agreement are rejected, unenforceable by the Licensor, and shall not become part of this Agreement unless such terms and conditions are to the benefit of the Commonwealth.
18. **Publicity/Advertisement.** The Licensor must obtain written Commonwealth approval prior to mentioning the Commonwealth or a Commonwealth Agency in an advertisement, endorsement, or any other type of publicity. This includes the use of any trademark or logo.

**19. Portability.** The parties agree that a Commonwealth Agency may move a Licensed Product from machine to machine, whether physical or virtual, and to other locations, where those machines and locations are internal to the Commonwealth or to a Commonwealth contractor, as long as such relocation and the use being made of the Licensed Product comports with the license grant and restrictions. Notwithstanding the foregoing, a Commonwealth Agency may move the machine or appliance provided by the Licensor upon which the Licensed Product is installed.

**20. Taxes-Federal, State and Local; Interest.**

- (a) The Commonwealth is exempt from all excise taxes imposed by the Internal Revenue Service and has accordingly registered with the Internal Revenue Service to make tax-free purchases under registration No. 23-23740001-K. With the exception of purchases of the following items, no exemption certificates are required and none will be issued: undyed diesel fuel, tires, trucks, gas-guzzler emergency vehicles, and sports fishing equipment. The Commonwealth is also exempt from Pennsylvania sales tax, local sales tax, public transportation assistance taxes, and fees and vehicle rental tax. The Department of Revenue regulations provide that exemption certificates are not required for sales made to governmental entities and none will be issued. Nothing in this section is meant to exempt a construction contractor from the payment of any of these taxes or fees which are required to be paid with respect to the purchase, use, rental or lease of tangible personal property or taxable services used or transferred in connection with the performance of a construction contract.
- (b) The only interest the Commonwealth is authorized to pay is in accordance with Act of December 13, 1982, P.L. 1155, No. 266, as amended, [72 P. S. § 1507](#), (relating to Interest Penalties on Commonwealth Accounts) and accompanying regulations [4 Pa. Code §§ 2.31—2.40](#) (relating to Interest Penalties for Late Payments).

**21. Commonwealth Audit Responsibilities.**

- (a) The Commonwealth shall maintain, and promptly provide to the Licensor upon request, accurate records regarding use of the Licensed Products by or for the Commonwealth. If the Commonwealth becomes aware of any unauthorized use of all or any part of the Licensed Products, the Commonwealth shall notify the Licensor promptly, providing reasonable details. The limit of the Commonwealth's responsibility for use of the Licensed Products by more individuals than are permitted by the licensing terms applicable to the Licensed Products shall be to purchase additional licenses and Maintenance and Support (if applicable) for such Licensed Products through a reseller contract or another procurement document.
- (b) The Commonwealth shall perform a self-audit upon the request of the Licensor, which request may not occur more often than annually, and report any change in user count (hereinafter "True up number"). The Commonwealth shall notify the Licensor of the True up number no later than **45 calendar days** after the request

that the Commonwealth perform a self-audit. If the user count has increased, the Commonwealth shall make an additional purchase of the Licensed Products through a reseller contract or another procurement document, which is equivalent to the additional users. This section sets out the sole software license audit right under this Agreement.

22. **Right-to-Know Law.** The Pennsylvania *Right-to-Know Law*, Act of February 14, 2008, P.L. 6, No. 3, 65 P.S. §§ 67.101—3104 (“RTKL”), applies to this Agreement.
23. **Third-Party Software.** If a Licensed Product utilizes or includes third party software and other copyrighted material, any additional licensing terms, acknowledgements or disclaimers associated with the third-party software and materials shall not be applicable to the Commonwealth unless agreed to in writing. The parties agree that the Commonwealth, by acknowledging third-party software, does not agree to any terms and conditions of the third-party software agreements.
24. **Attorneys’ Fees.** The Commonwealth is not responsible for and shall not pay attorneys’ fees incurred by or paid by the Licensors.
25. **Controversies.**
  - (a) Pursuant to Section 1712.1 of the *Commonwealth Procurement Code*, 62 Pa. C.S. § 1712.1, in the event of a claim arising from the Agreement or a purchase order, the Licensors, within **six (6) months** after the claim accrues, must file a written claim with the contracting officer for a determination. The claim shall state all grounds upon which the Licensors asserts a controversy exists. If the Licensors fails to file a claim or files an untimely claim, the Licensors is deemed to have waived its right to assert a claim in any forum. At the time the claim is filed, or within **60 days** thereafter, either party may request mediation through the Commonwealth Office of General Counsel Dispute Resolution Program, <http://www.ogc.pa.gov/Services%20to%20Agencies/Mediation%20Procedures/Pages/default.aspx>.
  - (b) If the Licensors or the contracting officer requests mediation and the other party agrees, the contracting officer shall promptly make arrangements for mediation. Mediation shall be scheduled so as to not delay the issuance of the final determination beyond the required **120 days** after receipt of the claim if mediation is unsuccessful. If mediation is not agreed to or if resolution is not reached through mediation, the contracting officer shall review timely-filed claims and issue a final determination, in writing, regarding the claim. The final determination shall be issued within **120 days** of the receipt of the claim, unless extended by consent of the contracting officer and the Licensors. The contracting officer shall send his/her written determination to the Licensors. If the contracting officer fails to issue a final determination within the **120 days** (unless extended by consent of the parties), the claim shall be deemed denied. The contracting officer’s determination shall be the final order of the purchasing agency.



- (c) Within **15 days** of the mailing date of the determination denying a claim or within **135 days** of filing a claim if, no extension is agreed to by the parties, whichever occurs first, the Licensor may file a statement of claim with the Commonwealth Board of Claims. Pending a final judicial resolution of a controversy or claim, the Licensor shall proceed diligently with the performance of the Agreement or purchase order in a manner consistent with the determination of the contracting officer and the Commonwealth shall compensate the Licensor pursuant to the terms of the Agreement, purchase order or other procurement document.

## **26. Insurance.**

- (a) The Licensor shall maintain at its expense, and require its agents, contractors and subcontractors to procure and maintain, as appropriate, the following types and amounts of insurance issued by companies acceptable to the Commonwealth and authorized to conduct such business under the laws of the Commonwealth:
  - (i) Workers' Compensation Insurance for all of the employees engaged in performing Services in accordance with the *Worker's Compensation Act*, the Act of June 2, 1915, P.L. 736, No. 338, reenacted and amended June 21, 1939, P.L. 520, No. 281, as amended, 77 P.S. §§ 101—2708.
  - (ii) Commercial general liability insurance providing coverage from claims for damages for personal injury, death (including bodily injury), sickness or disease, accidental death and damage to and property of others, including loss of use resulting from any property damage which may arise from the Licensor's operations under this Agreement, whether such operation be by the Licensor, its agent, contractor or subcontractor, or by anyone directly or indirectly employed by either. The limits of such insurance shall be in an amount not less than \$500,000 per person and \$2,000,000 per occurrence, personal injury and property damage combined. Such policies shall be occurrence based rather than claims-made policies and shall name the Commonwealth of Pennsylvania as an additional insured, as its interests may appear. The insurance shall not contain any endorsements or any other form designed to limit and restrict any action by the Commonwealth as an additional insured against the insurance coverages in regard to the Services performed for or supplies provided to the Commonwealth.
  - (iii) Professional and Technology-Based Services Liability Insurance (insuring against damages and claim expenses as a result of claims arising from any actual or alleged wrongful acts in performing cyber and technology activities) in the amount of \$2,000,000, per claim/annual aggregate.
  - (iv) Technology Products Liability/Professional Liability/Errors & Omissions Insurance in the amount of \$2,000,000, per claim/annual aggregate,

covering the Licensor, its employees, agents, contractors, and subcontractors in the performance of all services.

- (v) Comprehensive crime insurance in an amount of not less than \$5,000,000 per occurrence.
  - (vi) Information Security and Privacy Liability Insurance including Privacy Notification Costs (including coverage for Technology Professional Liability if not covered under Licensor's Professional Liability/Errors and Omissions Insurance referenced above) in the amount of \$3,000,000, per claim/annual aggregate, covering the Licensor, its employees, agents, contractors, and subcontractors in the performance of all services.
- (b) Certificate of Insurance. Prior to providing Licensed Products under this Agreement, and annually thereafter, the Licensor shall provide the Commonwealth with a copy of each current certificate of insurance required by this section. These certificates shall contain a provision that coverages afforded under the policies will not be canceled or materially changed in such a way to cause the coverage to fail to comply with the requirements of this section until at least **15 days'** prior written notice has been received by the Commonwealth. Such cancellation or change shall not relieve the Licensor of its continuing obligation to maintain insurance coverage in accordance with this section.
- (c) Insurance coverage length. The Licensor shall maintain such insurance for the life of any applicable purchase order issued pursuant to the Agreement.

## **27. Signatures.**

- (a) The parties agree that: (1) a record or signature may not be denied legal effect or enforceability solely because it is in electronic form; (2) a contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation; (3) if a law requires a record to be in writing, an electronic record satisfies the law; and (4) if law requires a signature, an electronic signature satisfies the law.
- (b) The fully executed Agreement may not contain ink signatures by the Commonwealth. If this Agreement does not contain ink signatures by the Commonwealth, the Licensor understands and agrees that the receipt of an electronically-printed Agreement with the printed name of the Commonwealth purchasing agent constitutes a valid, binding contract with the Commonwealth. The printed name of the purchasing agent represents the signature of that individual who is authorized to bind the Commonwealth to the obligations contained in this Agreement. The printed name also indicates that all approvals required by Commonwealth contracting procedures have been obtained.

28. **Independent Contractor.** The parties are independent contractors, and this Agreement does not create an agency, partnership or joint venture.
29. **Travel.** The Licensor shall not be allowed or paid travel or per diem expenses except as specifically set forth in this Agreement or Statement of Work. If not otherwise specified in the Agreement or Statement of Work, travel and related expenses shall be reimbursed in accordance with [Management Directive 230.10 Amended](#), [Commonwealth Travel Policy](#), and [Manual 230.1](#), [Commonwealth Travel Procedures Manual](#).
30. **Entire Agreement.** This Agreement, together with Exhibit A, constitutes the entire agreement between the parties pertaining to the subject matter hereof, and supersedes and integrates all prior discussions, agreements and understandings pertaining thereto. No modification of this Agreement will be effective unless in writing and signed by both Parties. Other terms and conditions or additional terms and conditions included or referenced in the Licensor's quotations, invoices, business forms, or other documentation shall not become part of the parties' agreement and shall be disregarded by the parties, unenforceable by the Licensor and not binding on the Commonwealth. No modification of this Agreement will be effective unless in writing and signed by both Parties.
31. **Assignment.** Either party may assign this Agreement in its entirety, but not in parts, on written notice to the other party to its parent company, affiliate or subsidiary, in connection with a merger, consolidation, or sale or other disposition of all or substantially all of its assets, or in the case of the Commonwealth to another Commonwealth entity. Any other assignment shall be null and void, except with the other party's prior written consent, which shall not be unreasonably withheld. This Agreement and all obligations shall be binding upon and inure to the benefit of the parties' successors and lawful assignees.
32. **Notice.** Any written notice to either party under this Agreement shall be deemed sufficient if delivered personally, or by facsimile, telecopy, electronic or digital transmission (provided such delivery is confirmed), or by a recognized overnight courier service (e.g., DHL, Federal Express, etc.), with confirmed receipt, or by certified or registered United States mail, postage prepaid, return receipt requested, sent to the address such party may designate by notice given pursuant to this section.
33. **Survival.** The termination or expiration of this Agreement will not affect any provisions of this Agreement which by their nature survive termination or expiration, including the provisions that deal with the following subject matters: definitions, confidentiality, term and termination, effect of termination, intellectual property, license compliance, limitation of liability, indemnification and privacy.
34. **Waiver.** Failure to enforce any provision will not constitute a waiver.
35. **Severability.** If any provision is found unenforceable, it and any related provisions will be interpreted to best accomplish the unenforceable provision's essential purpose.

36. **Nonexclusive Remedy.** Except as expressly set forth in this Agreement, the exercise by either party of any of its remedies under this Agreement will be without prejudice to its other remedies under this Agreement or otherwise.
37. **Integration.** This Agreement, including all exhibits and referenced documents, and any Purchase Orders referencing this Agreement, constitutes the entire agreement between the parties. No agent, representative, employee or officer of the Commonwealth or of Licensor has authority to make any statement, agreement, or representation, oral or written, in connection with this Agreement, which in any way can be deemed to modify, add to, or detract from, or otherwise change or alter its terms and conditions. No negotiations between the parties, nor any custom or usage, shall be permitted to modify or contradict any of the terms and conditions of this Agreement. No modifications, alterations, changes, or waiver to this Agreement or any of its terms shall be valid or binding unless accomplished by a written amendment executed by the parties.

[Reminder of Page Intentionally Left Blank]

The parties to this Agreement have executed it, through their respective duly authorized representatives.

**Witness:**

Amy R. Hare 1/27/2025  
\_\_\_\_\_  
Signature Date  
Amy Hare  
\_\_\_\_\_  
Printed Name  
Director, Government Contracts & Compliance  
\_\_\_\_\_  
Title

**Licensors:**

Bill Walter 1/27/2025  
\_\_\_\_\_  
Signature Date  
Bill Walter  
\_\_\_\_\_  
Printed Name  
VP, State and Local Govt  
\_\_\_\_\_  
Title

*If a corporation, the Chairman, President, Vice-President, Senior Vice-President, Executive Vice-President, Assistant Vice-President, Chief Executive Officer or Chief Operating Officer must sign; if a sole proprietor, then the owner must sign; if a general or limited partnership, a general partner must sign; if a limited liability company, then a member must sign, unless it is a managed by a manager, then the manager must sign; otherwise a resolution indicating authority to bind the corporation must be attached to this Agreement.*

---

**COMMONWEALTH OF PENNSYLVANIA  
GOVERNOR'S OFFICE OF ADMINISTRATION**

**Electronically signed per Section 27**

Agency Head or Designee

**APPROVED AS TO FORM AND LEGALITY:**

**Electronically signed per Section 27**

Office of Chief Counsel

**Electronically signed per Section 27**

Office of General Counsel

**Electronically signed per Section 27**

Office of Attorney General

**APPROVED:**

**Electronically signed per Section 27**

Comptroller

## ATTACHMENT 1

### **LIST OF LICENSED PRODUCTS**

With the consent of the Commonwealth, additional Licensed Products may be added to this attachment by Licensor providing the Commonwealth with a new copy of this Attachment 1.

#### **Licensed Products:**

The Licensed Products include (list all titles covered by this Agreement):

- SendPro® 360 Locker Management
- ParcelPoint™ Smart Locker Management
- SendPro® 360 Receiving
- PitneyTrack™ Inbound
- PitneyShip®
- SendPro® 360 Sending
- PitneyShip® Pro
- PitneyShip® Enterprise
- SendPro® Enterprise Subscription
- Pitney Analytics

**ATTACHMENT 2**  
**Requirements for Non-Commonwealth Hosted Applications/Services**

The purpose of this Attachment is to define requirements for business or technology solutions and services procured by the Commonwealth that are hosted within the Service Organization (Licensor's) or its Subservice Organization(s) (subcontractors) managed infrastructure. Any reference to Licensor below applies to Licensor and its subcontractors.

**A. Hosting Requirements**

1. The Licensor shall supply and maintain all hosting equipment (hardware and software) required for the delivery of the computing services.
2. The Licensor shall provide secure access to users leveraging the principle of least privilege and delegating administration to the Commonwealth where possible.
3. The Licensor shall use commercially reasonable resources and efforts to maintain adequate network bandwidth and server capacity to meet expected service levels.
4. The Licensor shall maintain all components of the Licensor hosted solution with commercially reasonable support and replace as necessary to maintain compliance.
5. The Licensor shall monitor, prevent, and deter unauthorized system access. The Licensor shall use all commercially reasonable methods to confirm suspected breaches. In the event of any impermissible disclosure, unauthorized loss or destruction of Confidential Information, the receiving Party must immediately notify the disclosing Party and take all reasonable steps to mitigate any potential harm or further disclosure of such Confidential Information. The Licensor shall provide the Commonwealth with any requested Commonwealth-specific logs, reports, and other information concerning unauthorized access or disclosure of Commonwealth data, including any mitigation efforts by Licensor. Any such information provided by Licensor shall be treated as confidential. In addition, pertaining to the unauthorized access, use, release, or disclosure of data, the Licensor shall comply with state and federal data breach notification statutes and regulations, and shall report security incidents to the Commonwealth as soon as possible, within twenty four (24) hours of when the Licensor has reasonable confirmation of such unauthorized access, use, release, or disclosure of data.
6. In the event the Licensor is not in compliance with **Section B System and Organization Controls (SOC) Reporting Requirements** relating to the hosted system's data center locations and security architecture, the Licensor shall allow the Commonwealth or its delegate, at times chosen by the Commonwealth, and with

*Requirements for Non-Commonwealth Hosted Applications and/or Services*

Page 1 of 9

Updated 11/03/2023

at least **ten (10) business days'** notice, to review the hosted system's data center locations and security architecture.

7. The Licensor's employees or subcontractors, who are directly responsible for day-to-day monitoring and maintenance of the hosted system, shall have industry standard certifications applicable to the environment and system architecture used.
8. The Licensor shall house all servers and equipment in an operational environment that meets industry standards including, but not limited to, climate control, fire and security hazard detection and response, electrical needs, and physical security.
9. The Licensor shall examine applicable system and error logs, which should include, but not be limited to, security events. Such logs shall be examined on a continual basis, at least daily, to minimize and predict system problems and initiate appropriate action.
10. The Licensor shall update and patch all applicable systems and third-party software security configurations to reduce security risk in alignment with industry best practices beginning prior to service release and on an ongoing basis.
11. During the term of the contract, the Licensor shall provide or make available all Commonwealth data to the Commonwealth, at no cost and upon request in a format and method agreeable to both parties. If the parties are unable to reach an agreement regarding format or method, data shall be provided in an industry standard format and method.

#### **B. System and Organization Controls (SOC) Reporting Requirements**

1. Subject to this section and unless otherwise agreed to in writing by the Commonwealth, the Licensor shall, and shall require its subcontractors to, engage, on an annual basis, a CPA certified third-party auditing firm to conduct the following, as applicable:
  - (i) RESERVED.
  - (ii) a SOC 2 Type II report with respect to controls used by the Licensor relevant to internal and external procedures and systems that access, process, host or contain Commonwealth Data designated as Class "C" Classified Records or Closed Records, as defined in in the Commonwealth's [Data Classification Policy](#), or in compliance with mandates by federal or state audit requirements and/or policy.



The Licensor shall receive and review their subcontractor's relevant SOC reports, if applicable, and the Licensor shall provide the Commonwealth with a Letter of Attestation that confirms its analysis of their subcontractor's SOC report.

2. Unless otherwise agreed to in writing by the Commonwealth, the Licensor's SOC Report(s) shall be provided upon contract execution and annually thereafter upon request of the Commonwealth. While it is preferable that SOC Reports coincide with Pennsylvania's fiscal year (July 1 through June 30), SOC Reports, at the very least, must cover at least **6 consecutive months** of Pennsylvania's fiscal year.
3. SOC 2 Type II reports shall address the following:
  - (i) Security of Information and Systems;
  - (ii) Availability of Information and Systems;
  - (iii) Processing Integrity;
  - (iv) Confidentiality; and
  - (v) Privacy.
4. At the request of the Commonwealth and at Licensor's expense, the Licensor shall, and shall require its subcontractors, as applicable, to provide a SOC for Cybersecurity audit in the event:
  - (i) Reoccurring findings in any SOC report required by subsection 1 above; or
  - (ii) A cybersecurity incident or breach that impacts the Commonwealth has occurred, the Commonwealth has requested a copy of Licensor's SOC 2 Type 2 Report and the incident or breach was not handled in accordance with Licensor's Incident Response Plan (IRP) including, but not limited to, providing timely notice to the Commonwealth as required by Contract or applicable law; or
  - (iii) Licensor shall provide the following information in the event of an incident or breach:
    - a forensic report and periodic updates
    - a description of what happened
    - type of protected or Personal Information involved
    - actions being taken to protect data from further unauthorized access
    - what the Contractor will do to assist affected persons
    - what such affected persons can do to assist themselves
  - (iv) As agreed upon by the parties.

The SOC for Cybersecurity report shall detail the controls used by the Licensor or its subcontractor setting forth the description and effectiveness of the Licensor's or

*Requirements for Non-Commonwealth Hosted Applications and/or Services*

Page 3 of 9

Updated 11/03/2023

subcontractor's cybersecurity risk management program and the policies, processes and controls enacted to achieve each cybersecurity objective.

The Licensor shall provide to the Commonwealth a report of the SOC for Cybersecurity audit findings upon request of the Commonwealth.

5. Additional standards, certifications or audits as required by law shall be supported by Licensor as mutually agreed upon in writing by the parties.
6. The Licensor shall adhere to the then current American Institute of Certified Public Accountants (AICPA) audit standards. The Licensor acknowledges that the AICPA guidance may be updated during the Term of this Contract, and the Licensor shall comply with such updates, which shall be reflected in the next annual SOC report.
7. In the event an audit reveals any non-conformity within Licensor's SOC Reports, the Licensor shall provide the Commonwealth, within **45 days** of the issuance of the SOC report, a documented corrective action plan that addresses each non-conformity that is identified within the SOC report, including any subcontractor's SOC report. The corrective action plan shall provide, in detail:
  - clear responsibilities of the personnel designated to resolve the non-conformity;
  - the remedial action to be taken by the Licensor or its subcontractor(s);
  - the dates when each remedial action is to be implemented; and
  - a summary of potential risks or impacts to the Commonwealth that are associated with the non-conformity(ies).
8. The Commonwealth may in its sole discretion agree, in writing, to accept alternative security report in lieu of a SOC report.

### **C. Security Requirements**

1. The Licensor shall conduct a third-party independent security/vulnerability assessment at its own expense no less frequently than on an annual basis.
2. The Licensor shall provide, at minimum, an executive summary of vulnerability assessment results to the Commonwealth upon request. Summary shall include, at minimum, scan date, identified vulnerabilities, severity classification, and remediation status.
3. The Licensor shall remediate any security/vulnerability assessment findings to align with the industry standards.

*Requirements for Non-Commonwealth Hosted Applications and/or Services*

Page 4 of 9

Updated 11/03/2023

4. The Licensor shall use industry best practices to protect access to the system with a firewall and firewall rules to prevent access by non-authorized users and block all improper and unauthorized access attempts.
5. The Licensor shall use industry best practices to secure access to public web interfaces, which shall include, but is not limited to, web application firewall (WAF) for services that handle non-public Commonwealth records.
6. The Licensor shall use industry best practices to provide applicable system intrusion detection and prevention in order to detect intrusions in a timely manner.
7. The Licensor shall use industry best practices, such as those outlined in NIST 800-83, to provide appropriate exploit and malware controls, on all servers, endpoints, and network components.
8. The Licensor shall provide access to Commonwealth data only to staff located within CONUS (any of the Continental United States and Hawaii). Access shall be based on the principle of least privilege.
  - (i) No offshore support shall be permitted from any countries that are identified as state sponsors of terrorism by the US Department of State, which shall be monitored by the purchasing Agency to ensure compliance through the life of the Agreement, Contract, or Purchase Order;
  - (ii) Access by offshore vendor resources shall be limited to solely that which is required to perform the Services, including support services;
  - (iii) Offshore vendor resources who are providing the services shall be trained in the proper handling of Commonwealth Data;
    - a. Any vendor offshore resources that are dedicated to the Commonwealth shall be required to undergo Commonwealth Security Awareness Training provided by the Commonwealth and the vendor shall provide monthly compliance report.
    - b. Vendor attests that offshore vendor resources shall comply with Management Directive 205.34 and Management Directive 245.18 and that the Vendor has trained the offshore resources in the proper handling of Commonwealth Data.
  - (iv) Offshore vendor resources that are providing the services shall be obligated to handle Commonwealth Data in ways at least as restrictive as the requirements outlined in the Agreement;
  - (v) Offshore vendor resources that are providing the services and require access

*Requirements for Non-Commonwealth Hosted Applications and/or Services*

Page 5 of 9

Updated 11/03/2023

must be uniquely identified (e.g., by a unique User ID);

- (vi) Offshore vendor resources that are providing the services shall access Commonwealth systems, data, or services in a manner that meets or exceeds the minimum requirements set forth in Commonwealth ITPs;
- (vii) The date, time (including time zone), resource name, source IP, and nature of the access (i.e., read-only or modify) shall be recorded in a log file which is maintained and preserved according to applicable data protection law(s) and industry best practice standards;
- (viii) Any offshore vendor resource access must be granted by an authorized Commonwealth resource and shall only be granted on least required privilege or need-to-know basis prior to any offshore vendor resource obtaining access and shall only be granted to offshore vendor resource that must have access to provide and/or support the services;
- (ix) The vendor shall agree explicitly in the agreement that with respect to any services provided by any offshore vendor resources, the vendor shall be obligated to comply with the terms and conditions of the Agreement, Contract or Purchase Order, as though the offshore vendor resources were located within the United States and that the vendor shall assume all obligations and risks associated with the use of offshore vendor resources as if those resources were located within the United States;
- (x) The purchasing agency shall ensure that background check requirements apply to all offshore vendor resources assigned to perform services under the Agreement, Contract or Purchase Order.
  - a. The vendor shall identify each offshore vendor resource that will perform services under the Agreement, Contract or Purchase Order and shall perform the following background checks on each individual offshore vendor resource providing services:
    - Drug Screening
    - Verification of previous employment
    - Review of academic qualifications
    - Review of professional qualifications
    - Checking Criminal-background
    - Credit reports

*Requirements for Non-Commonwealth Hosted Applications and/or Services*

Page 6 of 9

Updated 11/03/2023

- b. On an annual basis, the vendor shall provide written confirmation that the above required background checks have been completed and that the background checks did not identify any criminal record that includes a felony or misdemeanor (or equivalent) involving terroristic behavior, violence, use of a lethal weapon, or breach of trust/fiduciary responsibility or which raises concerns about building, system or personal security or is otherwise job-related. This written confirmation must be provided prior to the subject offshore vendor resource being provided access to Commonwealth data or systems. The vendor shall not assign any offshore vendor resource that fails to pass the background checks required in this section to any Commonwealth services and shall remove any access privileges already given to the offshore vendor resource unless the Commonwealth consents to the access, in writing, prior to the access.
- (xi) Unless requested by the Commonwealth during support and troubleshooting process, Licensor employees shall not record, stream, or photograph Commonwealth data while performing work under the Agreement.
- 9. The Licensor shall provide the services using security technologies and techniques in accordance with industry best practices including, but not limited to, the prevention and detection of intrusions, and any other inappropriate use or access of systems and networks.
- 10. The Licensor shall provide the Commonwealth with access to Commonwealth specific audit logs with respect to the services being provided to the Commonwealth within 24 hours of a written request from the Commonwealth's Enterprise Information Security Office.

**D. Data Protection**

- 1. The Licensor shall only host, handle, and process data in physical locations within CONUS.
- 2. The Licensor shall use industry best practices to protect their operational systems with applicable anti-virus, intrusion protection, incident response monitoring and reporting, network firewalls, application firewalls, and employ system and application patch management to protect its network and customer data from unauthorized disclosure.
- 3. The Licensor shall be solely responsible for applicable data storage required.
- 4. The Licensor shall encrypt all Commonwealth data in transit and at rest. The Licensor's method of data encryption shall meet or exceed National Institute

*Requirements for Non-Commonwealth Hosted Applications and/or Services*

Page 7 of 9

Updated 11/03/2023

Standards and Technology (NIST) encryption guidelines and standards in alignment with Commonwealth ITPs.

5. The Licensor shall take all commercially viable and appropriate measures to protect the data availability including, but not limited to, real-time replication, traditional backup, and/or georedundant storage of Commonwealth data in accordance with industry best practices and encryption techniques.
6. The Licensor shall have appropriate controls in place to protect critical or sensitive data and shall employ stringent policies, procedures, to protect that data particularly in instances where such critical or sensitive data may be stored on a Licensor-controlled or Licensor-owned electronic device.
7. The Licensor shall utilize a secured backup solution to prevent loss of data. Stored backups must be kept in an all-hazards protective storage environment at the primary location and any additional locations where the data is being maintained. All back up data and media shall be encrypted.

#### **E. Adherence to Policy**

1. The Licensor support and problem resolution solution shall provide a means to classify problems as to criticality and impact and with appropriate resolution procedures and escalation process for classification of each problem.
2. The Licensor shall abide by the Commonwealth's Information Technology Policies (<https://www.oa.pa.gov/Policies/Pages/itp.aspx>) that are applicable to the products and services provided, as set forth within the responsibilities section of each ITP.
3. The Licensor shall comply with all pertinent federal and state regulations and laws, including but not limited to, data protections, data security, privacy, and data breach notification.

#### **F. Closeout**

When the purchase order's or other procurement document's term expires or terminates, and a new purchase order or other procurement document has not been issued by a Commonwealth Agency within **60 days** of expiration or termination, or at any other time at the written request of the Commonwealth, the Licensor must promptly return to the Commonwealth all Commonwealth's data (and all copies of this information) that is in the Licensor's possession or control. The Commonwealth's data shall be returned in a format agreed to by the Commonwealth.

Upon confirmation that Commonwealth data is in possession or control of the Commonwealth, the Licensor shall ensure all residual user account(s) are promptly deleted

*Requirements for Non-Commonwealth Hosted Applications and/or Services*

Page 8 of 9

Updated 11/03/2023

or reset in the solution. The Licensor shall notify the Commonwealth within **10 business days** that all user account(s) have been deleted or reset.

### Attachment 3

**COMMONWEALTH OF PENNSYLVANIA**  
**SAMPLE BUSINESS ASSOCIATE AGREEMENT**  
*(Business Associate Agreements as provided by Agencies may differ)*

**WHEREAS,** the \_\_\_\_\_ (Covered Entity) and \_\_\_\_\_ (Business Associate) intend to protect the privacy and security of certain Protected Health Information (PHI) to which Business Associate may have access in order to provide goods or services to or on behalf of Covered Entity, in accordance with the *Health Insurance Portability and Accountability Act of 1996*, as amended, Pub. L. No. 104-191 (HIPAA), the *Health Information Technology for Economic and Clinical Health (HITECH) Act*, as amended, Title XIII of Division A and Title IV of Division B of the *American Recovery and Reinvestment Act of 2009* (ARRA), as amended, Pub. L. No. 111-5 (Feb. 17, 2009) and related regulations, the HIPAA Privacy Rule (Privacy Rule), 45 C.F.R. Parts 160 and 164, as amended, the HIPAA Security Rule (Security Rule), 45 C.F.R. Parts 160, 162 and 164, as amended, 42 C.F.R. §§ 431.301—431.302, 42 C.F.R. Part 2, 45 C.F.R. § 205.50, 42 U.S.C. § 602(a)(1)(A)(iv), 42 U.S.C. § 1396a(a)(7), 35 P.S. § 7607, 50 Pa. C.S. § 7111, 71 P.S. § 1690.108(c), 62 P.S. § 404, 55 Pa. Code Chapter 105, 55 Pa. Code Chapter 5100, the Pennsylvania *Breach of Personal Information Notification Act*, Act of December 22, 2005, P.L. 474, No. 94, as amended, 73 P.S. §§ 2301—2329, and other relevant laws, including subsequently adopted provisions applicable to use and disclosure of confidential information, and applicable agency guidance; and,

**WHEREAS,** Business Associate may receive PHI from Covered Entity, or may create or obtain PHI from other parties for use on behalf of Covered Entity, which PHI may be used or disclosed only in accordance with this Agreement and the standards established by applicable laws and agency guidance; and

**WHEREAS,** Business Associate may receive PHI from Covered Entity, or may create or obtain PHI from other parties for use on behalf of Covered Entity, which PHI must be handled in accordance with this Agreement and the standards established by HIPAA, the HITECH Act and related regulations, the Privacy Rule, the Security Rule and other applicable laws and agency guidance.

**NOW, THEREFORE,** Covered Entity and Business Associate agree as follows:

**1. Definitions.**

- (a) **“Business Associate”** shall have the meaning given to such term under HIPAA, the HITECH Act and related regulations, the Privacy Rule, the Security Rule and agency guidance.
- (b) **“Covered Entity”** shall have the meaning given to such term under HIPAA, the HITECH Act and related regulations, the Privacy Rule, the Security Rule and agency guidance.



- (c) “**HIPAA**” shall mean the *Health Insurance Portability and Accountability Act of 1996*, as amended, Pub. L. No. 104-191.
- (d) “**HITECH Act**” shall mean the *Health Information Technology for Economic and Clinical Health (HITECH) Act*, as amended, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (Feb. 17, 2009).
- (e) “**Privacy Rule**” shall mean the standards for privacy of individually identifiable health information in 45 C.F.R. Parts 160 and 164, as amended, and related agency guidance.
- (f) “**Protected Health Information**” or “**PHI**” shall have the meaning given to such term under HIPAA, the HITECH Act and related regulations, the Privacy Rule, the Security Rule (all as amended) and agency guidance.
- (g) “**Security Rule**” shall mean the security standards in 45 C.F.R. Parts 160, 162 and 164, as amended, and related agency guidance.
- (h) “**Unsecured PHI**” shall mean PHI that is not secured through the use of a technology or methodology as specified in HITECH Act regulations, as amended, and agency guidance or as otherwise defined in the HITECH Act, as amended.

2. **Stated Purposes for Which Business Associate May Use or Disclose PHI.** The Parties hereby agree that Business Associate shall be permitted to use and/or disclose PHI provided by or obtained on behalf of Covered Entity for the following stated purposes, except as otherwise stated in this Agreement:

---

---

---

---

---

---

---

---

---

---

**NO OTHER DISCLOSURES OF PHI OR OTHER INFORMATION ARE PERMITTED.**

3. **BUSINESS ASSOCIATE OBLIGATIONS.**

- (a) **Limits on Use and Further Disclosure.** Business Associate shall not further use or disclose PHI provided by, or created or obtained on behalf of, Covered Entity

other than as permitted or required by this Addendum, as requested by Covered Entity, or as required by law and agency guidance.

- (b) **Appropriate Safeguards.** Business Associate shall establish and maintain appropriate safeguards to prevent any use or disclosure of PHI other than as provided for by this Agreement. Appropriate safeguards shall include implementing administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the electronic PHI that is created, received, maintained or transmitted on behalf of the Covered Entity and limiting use and disclosure to applicable minimum necessary requirements as set forth in applicable federal and state statutory and regulatory requirements and agency guidance.
- (c) **Reports of Improper Use or Disclosure.** Business Associate hereby agrees that it shall report to \_\_\_\_\_ at \_\_\_\_\_, within **two (2) days** of discovery any use or disclosure of PHI not provided for or allowed by this Agreement.
- (d) **Reports on Security Incidents.** In addition to following the breach notification requirements in section 13402 of the *Health Information Technology for Economic and Clinical Health Act of 2009* (“HITECH Act”), as amended, and related regulations, the Privacy Rule, the Security Rule, agency guidance and other applicable federal and state laws, Business Associate shall report to \_\_\_\_\_ at \_\_\_\_\_, **within two (2) days** of discovery any security incident of which it becomes aware. At the sole expense of Business Associate, Business Associate shall comply with all federal and state breach notification requirements, including those applicable to Business Associate and those applicable to Covered Entity. Business Associate shall indemnify the Covered Entity for costs associated with any incident involving the acquisition, access, use or disclosure of Unsecured PHI in a manner not permitted under federal or state law and agency guidance. For purposes of the security incident reporting requirement, inconsequential unsuccessful incidents that occur on a daily basis, such as scans, “pings,” or other unsuccessful attempts to penetrate computer networks or servers containing electronic PHI maintained by Business Associate, need not be reported in accordance with this section, but may instead be reported in the aggregate on a monthly basis.
- (e) **Subcontractors and Agents.** At any time PHI is provided or made available to Business Associate subcontractors or agents, Business Associate shall provide only the minimum necessary PHI for the purpose of the covered transaction and shall first enter into a subcontract or contract with the subcontractor or agent that contains substantially the same terms, conditions and restrictions on the use and disclosure of PHI as contained in this Agreement.
- (f) **Right of Access to PHI.** Business Associate shall allow, for any PHI maintained in a designated record set, Covered Entity to have access to and copy an individual’s

PHI within **five (5) business days** of receiving a written request from the Covered Entity. Business Associate shall provide PHI in the format requested, if it is readily producible in such form and format; or if not, in a readable hard copy form or such other form and format as agreed to by Business Associate and the individual. If the request is for information maintained in one or more designated record sets electronically and if the individual requests an electronic copy of such information, Business Associate must provide Covered Entity with access to the PHI in the electronic form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the Business Associate and Covered Entity. If any individual requests from Business Associate or its agents or subcontractors access to PHI, Business Associate shall notify Covered Entity within **five (5) business days**. Business Associate shall further conform with all of the requirements of [45 C.F.R. § 164.524](#) and other applicable laws, including the HITECH Act, as amended, related regulations and agency guidance. Business Associate shall indemnify Covered Entity for costs/damages associated with Business Associate's failure to respond within the time frames set forth in this subsection [3\(f\)](#).

- (g) **Amendment and Incorporation of Amendments.** Within **five (5) business days** of receiving a written request from Covered Entity for an amendment of PHI maintained in a designated record set, Business Associate shall make the PHI available and incorporate the amendment to enable Covered Entity to comply with [45 C.F.R. § 164.526](#), applicable federal and state law, including the HITECH Act, as amended and related regulations, the Privacy Rule, the Security Rule and agency guidance. If any individual requests an amendment from Business Associate or its agents or subcontractors, Business Associate shall notify Covered Entity within **five (5) business days**.
- (h) **Provide Accounting of Disclosures.** Business Associate shall maintain a record of all disclosures of PHI made by Business Associate which are not excepted from disclosure accounting requirements under HIPAA, HITECH and related regulations, the Privacy Rule or the Security Rule (all as amended) in accordance with [45 C.F.R. § 164.528](#) and other applicable laws and agency guidance, including the HITECH Act and related regulations. Such records shall include, for each disclosure, the date of the disclosure, the name and address of the recipient of the PHI, a description of the PHI disclosed, the name of the individual who is the subject of the PHI disclosed, and the purpose of the disclosure. Business Associate shall make such record available to the Covered Entity within **five (5) business days** of a written request for an accounting of disclosures. Business Associate shall indemnify Covered Entity for costs/damages associated with Business Associate's failure to respond within the time frames set forth in this subsection [3\(h\)](#).
- (i) **Requests for Restriction.** Business Associate shall comply with requests for restrictions on disclosures of PHI about an individual if the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for treatment purposes), and the PHI pertains solely to a health care item or service for

which the service involved was paid in full out-of-pocket. For other requests for restriction, Business associate shall otherwise comply with the Privacy Rule, as amended, and other applicable statutory and regulatory requirements and agency guidance.

- (j) **Access to Books and Records.** Business Associate shall make its internal practices, books and records relating to the use or disclosure of PHI received from, or created or received, by Business Associate on behalf of the Covered Entity, available to the Secretary of Health and Human Services or designee for purposes of determining compliance with applicable laws and agency guidance.
- (k) **Return or Destruction of PHI.** At termination of this Agreement, Business Associate hereby agrees to return or destroy all PHI provided by or obtained on behalf of Covered Entity. Business Associate agrees not to retain any copies of the PHI after termination of this Agreement. If return or destruction of the PHI is not feasible, Business Associate agrees to extend the protections of this Agreement to limit any further use or disclosure until such time as the PHI may be returned or destroyed. If Business Associate elects to destroy the PHI, it shall certify to Covered Entity that the PHI has been destroyed.
- (l) **Maintenance of PHI.** Notwithstanding subsection 3(k) of this Agreement, Business Associate and its subcontractors or agents shall retain all PHI throughout the term of the Agreement and shall continue to maintain the information required under the various documentation requirements of this Agreement (such as those in subsection 3(h)) for a period of **six (6) years** after termination of the Agreement, unless Covered Entity and Business Associate agree otherwise.
- (m) **Mitigation Procedures.** Business Associate agrees to establish and to provide to Covered Entity upon request, procedures for mitigating, to the maximum extent practicable, any harmful effect from the use or disclosure of PHI in a manner contrary to this Agreement or the Privacy Rule, as amended. Business Associate further agrees to mitigate any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of this Agreement or applicable laws and agency guidance.
- (n) **Sanction Procedures.** Business Associate agrees that it shall develop and implement a system of sanctions for any employee, subcontractor or agent who violates this Agreement, applicable laws or agency guidance.
- (o) **Grounds for Breach.** Non-compliance by Business Associate with this Agreement or the Privacy or Security Rules, as amended, is a breach of the Agreement, if Business Associate knew or reasonably should have known of such non-compliance and failed to immediately take reasonable steps to cure the non-compliance. Commonwealth may elect to terminate Business Associate's contract for such breach.

- (p) **Termination by Commonwealth.** Business Associate authorizes termination of this Agreement by the Commonwealth if the Commonwealth determines, in its sole discretion, that the Business Associate has violated a material term of this Agreement.
- (q) **Failure to Perform Obligations.** In the event Business Associate fails to perform its obligations under this Agreement, Covered Entity may immediately discontinue providing PHI to Business Associate. Covered Entity may also, at its option, require Business Associate to submit to a plan of compliance, including monitoring by Covered Entity and reporting by Business Associate, as Covered Entity in its sole discretion determines to be necessary to maintain compliance with this Agreement and applicable laws and agency guidance.
- (r) **Privacy Practices.** Covered Entity will provide Business Associate with all applicable forms, including but not limited to, any form used for Notice of Privacy Practices, Accounting for Disclosures, or Authorization, upon the effective date designated by the Program or Covered Entity. Covered Entity may change applicable privacy practices, documents and forms. The Business Associate shall make reasonable endeavors to implement changes as soon as practicable, but not later than **45 days** from the date of notice of the change. Business Associate shall otherwise comply with all applicable laws and agency guidance pertaining to notices of privacy practices, including the requirements set forth in [45 C.F.R. § 164.520](#).

#### 4. OBLIGATIONS OF COVERED ENTITY.

- (a) **Provision of Notice of Privacy Practices.** Covered Entity shall provide Business Associate with the notice of privacy practices that the Covered Entity produces in accordance with applicable law and agency guidance, as well as changes to such notice. Covered Entity will post on its website any material changes to its notice of privacy practices by the effective date of the material change.
- (b) **Permissions.** Covered Entity shall provide Business Associate with any changes in, or revocation of, permission by individual to use or disclose PHI of which Covered Entity is aware if such changes affect Business Associate's permitted or required uses and disclosures.
- (c) **Restrictions.** Covered Entity shall notify Business Associate in writing of any restriction to the use or disclosure of PHI that the Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522, as amended, and other applicable laws and applicable agency guidance, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.
- (d) **Requests.** Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under HIPAA, HITECH and

related regulations, the Privacy Rule or the Security Rule, all as amended, if done by Covered Entity.

**5. MISCELLANEOUS.**

- (a) **Regulatory References.** A reference in this Addendum to a section in HIPAA, HITECH and related regulations, the Privacy Rule or the Security Rule refers to the most current version of the section in effect or as amended.
- (b) **Amendment.** The parties agree to take such action as is necessary to amend this Addendum from time to time in order to ensure compliance with the requirements of the HIPAA, HITECH and related regulations, the Privacy Rule, the Security Rule and any other applicable law, all as amended.
- (c) **Conflicts.** In the event that any terms of this Agreement are inconsistent with the terms of the Agreement, then the terms of this Agreement shall control.

#### Attachment 4

**Sign-Off Document No. \_\_\_\_\_, under Agreement No. \_\_\_\_\_**  
**Between**  
**[Licensor \_\_\_\_\_], and the Commonwealth of PA, [Agency]**  
**[Licensor \_\_\_\_\_] Agency-level Deployment**

This document becomes, upon its execution by the signatories named below, a legally valid, binding part of Software/Services License Requirements Agreement No. \_\_\_\_\_ between the Commonwealth and \_\_\_\_\_ (Licensor) and is subject to the terms of that Agreement.

Scope of Deployment (need not be entire agency):

Nature of Data implicated or potentially implicated:

Agency Policies to which Licensor. is subject (incorporated by reference):

Background checks (describe if necessary):

Additional requirements (describe with specificity):

Is Licensor. a Business Associate (yes or no)?

If yes, the attached Business Associates Agreement, as completed by the Agency, is applicable and is hereby incorporated into this Sign-Off Document by reference.

Agency Contact Person signature and Date: \_\_\_\_\_

**[Licensor \_\_\_\_\_]**  
**Authorized Signatory and Date:** \_\_\_\_\_

## **EXHIBIT A**

# ON-DEMAND SUBSCRIPTION SERVICES AGREEMENT

## for the Commonwealth of Pennsylvania

(Last modified July 5, 2024)

Thanks for using our on-demand subscription services. These terms define the terms and conditions under which you're allowed to use the on-demand subscription services and how we'll treat your account while you're utilizing the on-demand subscription services. If you have any questions about our terms, feel free to [contact us](#).

We'll start with the basics, including a few definitions that should help you understand this agreement. This On-Demand Subscription Services Agreement (this "Agreement") is between you and Pitney Bowes Inc. ("we", "us", and "our"). This Agreement will only apply if the on-demand subscription services identified in your order form (the "Order") are not covered by one or more separate On-Demand Subscription Services Agreements. Your on-demand subscription services may also require one or more Statements of Work (each a "SOW").

The web sites through which you access the on-demand subscription services (each a "Site"; the on-demand subscription services and the Sites are collectively called the "Services") are owned and operated by us or our vendors. Additional product-specific terms applicable to certain of the Services ("Product Terms") are attached to this Agreement as Exhibit A-1.

### **1. Eligibility**

In order to use the Services, you must provide true, complete and up to date contact information for so long as you access the Services. You won't use the Services in a way that violates any laws or regulations, including any relating to data protection and privacy. We may refuse service or close your account if you fail to comply with this Agreement.

### **2. Use of the Service**

a) As long as you continue to comply with the terms of this Agreement, we grant you a non-exclusive, non-transferable license to access and use the Services for the number of months, and for up to the number of users, number of locations, transactions, or other volume metrics specified in the Order. If applicable, you may upgrade your plan for additional fees. We reserve all rights to the Services not expressly granted to you in this Agreement.



b) You agree that you will use the Services only for business or commercial purposes and not for personal, family or household purposes.

c) You won't use the Services for or make the Services available to any third party, unless permitted in the Product Terms. In addition, you agree not to use the Services to send infringing, obscene, threatening or unlawful or tortious material or disrupt other users of the Services. Disruptions include but are not limited to denial of service attempts, distribution of advertising or chain letters, propagation of computer worms and viruses, or use of the Services to make unauthorized entry to any other device accessible via the Services. For the Services and related software, you will not (i) make derivative works; (ii) sublicense, sell, rent, lease, lend, time-share, disclose, transfer or host the Services, documentation or any other confidential or proprietary information to or for any other parties; (iii) use the Services to modify or reproduce a third party's materials unless you have the legal right to do so; (iv) distribute any part of the Services over any network, including a local area network; or (v) extract any data from the Services and use such data for any purpose other than for your use of the Services.

d) If you are delivered software for on premise installation as part of the Service ("Software") the following additional terms apply: You won't (i) reverse engineer, decompile or disassemble the Software; (ii) make copies of the Software, other than a reasonable number of copies for use for disaster recovery purposes; and (iii) separate the components of the Software, or install and use such components separately and independently of the Software they comprise.

e) If you do not comply with this Section 2, you may be in material breach of this Agreement, and we may have the right to immediately terminate your use of the Services.

### **3. Term and Termination; Suspension**

Reserved.

### **4. Changes**

We may change the Services and any features from time to time, and if such changes are material, we will notify you by sending an email to the last email address you gave to us. If you do not wish to continue using the modified Services, you may terminate your use of the Service, effective the last day of the current Billing Period for which you have paid in advance. We may change any terms of this Agreement only in writing and after obtaining signatures from both parties.

### **5. Account and Password**

By registering for the Services, you will be prompted to establish certain passwords and provide other access information to enable you to use the Services. You represent that you have all necessary authority to establish an account with us on behalf of the

business. The account name, password and access information is confidential information and should be used solely by you to access your account and use the Services. You are responsible for keeping your account name, password and access information confidential. You will take all reasonable steps to prevent unauthorized access to your account and you will immediately notify us of any unauthorized use of your accounts or any other breach of security.

## **6. Account Disputes**

We don't arbitrate disputes over who owns an account. You won't request access to or information about an account that's not yours. We decide who owns an account based on the information that has been provided to us with respect to the account, and if multiple people or entities are identified, then we will rely on the contact information listed for that account.

## **7. Fees; Payment Terms**

Reserved.

## **8. Personal Information**

If any of the Services collects or stores individually identifiable personal information, then we will comply with our privacy statement located at <http://www.pitneybowes.com/us/legal/privacy-statement.html> and attached to this Agreement as Exhibit A-2, as it may be updated by us from time to time (the "Privacy Statement"). Notwithstanding anything in the Privacy Statement, the Commonwealth reserves the right to pursue any claims or complaints in an appropriate court or forum.

## **9. Trademarks**

Pitney Bowes, the Pitney Bowes logo, and associated brand names and domain names are our intellectual property in the United States and other countries. All marks not owned by us are the property of their owners. You may not use, and nothing contained on the Sites or in this Agreement grants any right to use, any trademark displayed on the Site without our written permission or from the owner of the trademark. In addition, except as explicitly set forth in this Agreement, you will not use any copyrighted work displayed on the Sites or any of our other intellectual property without our prior written consent.

## **10. Feedback; Data Rights; Consents**

a) You agree to allow us to use any feedback, comments, ideas, know-how and suggestions ("Feedback") in any form that you provide the Feedback to us. Feedback is not confidential even if you designate it as confidential, provided however, paragraph 14 of the SSLRA governs the terms and conditions related to confidential information. We

may use the Feedback in any of our commercial offerings, for our internal purposes or fulfilling our obligations under our agreements with you.

b) As between you and us, you own all data that you provide to us as part of the Services (“End User Data”). Subject to your rights in the End User Data, we own all usage data that results from the Services. You grant to us (and our affiliates and vendors, if applicable) the right to use your End User Data as necessary to provide the Services and as provided in our Privacy Statement. We also have the right to use, without limitation, any anonymized or aggregated data from your End User Data that does not identify you or any end user of the Service in any of our commercial offerings, for our internal purposes or fulfilling our obligations under our agreements with you, all in accordance with our Privacy Statement. You’ll ensure that you have the appropriate rights to (including the right to provide to us) all data, files, materials or other information that you provide to us in connection with our provision of the Services.

c) Some of the features and functionalities of the Services may enable you to send communications via email, text message, and/or mobile app push notification to another person or entity. By providing or otherwise transferring personal information of another person or information of another entity to the Services, you must obtain from such person or entity all required consents and other authorizations necessary to use their information (the “Consents”). You will only utilize such functionality of the Services if all required Consents have been obtained, and you grant to us the right to process such information as necessary to provide the Services.

## **11. Product Support**

As part of your access to the Services, we will provide you with product support in accordance with the terms you will find at: <https://www.pitneybowes.com/us/sendtech-on-demand-subscription-services/product-support-terms.html>, and attached to this Agreement as Exhibit A-3.

## **12. LIMITATION OF LIABILITY**

**RESERVED.**

## **13. INDEMNITY**

**RESERVED.**

## **14. SERVICE AVAILABILITY; DISCLAIMERS**

**a) YOUR ACCESS TO AND USE OF THE SERVICES MAY BE INTERRUPTED FROM TIME TO TIME FOR VARIOUS REASONS, INCLUDING MALFUNCTION OF EQUIPMENT, PERIODIC UPDATING, MAINTENANCE OR REPAIR OF THE SITES, OR OTHER ACTIONS THAT WE MAY ELECT TO TAKE.**

**b) EXCEPT AS EXPRESSLY STATED IN ANY PRODUCT SPECIFIC TERMS OR THE ENTERPRISE SAAS SOFTWARE/SERVICES LICENSE REQUIREMENTS AGREEMENT (“SSLRA”), TO THE MAXIMUM EXTENT PERMITTED BY LAW, THE SERVICES AND THE CONTENT ON THE SITES, INCLUDING ANY THIRD PARTY SERVICE OR DATA, ARE PROVIDED BY US “AS IS” WITHOUT WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ACCURACY, RELIABILITY AND NON-INFRINGEMENT. WE DON’T GUARANTEE THAT THE SERVICES WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT WE WILL CORRECT ALL ERRORS.**

## **15. Third Party Sites and Data**

The Sites and this Agreement may contain links to third party websites, including links to the websites of carriers (“Linked Sites”). The Linked Sites are not under our control and we are not responsible for the contents of any Linked Site, including any link contained in a Linked Site, or any changes or updates to a Linked Site. You should contact the site administrator or webmaster for those Linked Sites if you have any concerns regarding such links or the content located there. If the Services perform an address validation function, license terms applicable to use of the USPS data related to such function are found at <http://www.pb.com/license-terms-of-use/usps-terms.html> and are incorporated in this Agreement by reference and are attached to this Agreement as Exhibit A-4. Notwithstanding anything contained in the USPS license terms, the Commonwealth does not have the authority to and shall not indemnify an entity. The Commonwealth agrees to pay for any loss, liability or expense, which arises out of or relates to the Commonwealth’s acts or omissions with respect to its obligations hereunder, where a final determination of liability on the part of the Commonwealth is established by a court of law or where settlement has been agreed to by the Commonwealth. This provision shall not be construed to limit the Commonwealth’s rights, claims or defenses which arise as a matter of law or pursuant to any other provision of this Agreement. This provision shall not be construed to limit the sovereign immunity of the Commonwealth.

## **16. Compliance with Laws**

Each party will comply with all applicable federal, state and local laws, rules and regulations, including export regulations and privacy laws. You will be responsible for the content of all data submitted to us to the extent you have sole control over the data in connection with our provision of the Services and will comply with all laws, rules and regulations relating to the use, disclosure and transmission of such data.

You represent and warrant that you have maintained and will maintain any and all certifications, licenses or other authorizations necessary or proper in furtherance of your use of the Service, including without limitation, federal certification pursuant to United States Department of Transportation regulations regarding the identification, processing and transportation of hazardous materials, if applicable.

## **USPS Regulations**

If you use the Service to print postage or send parcels, letters, and flats (“Packages”) with the USPS, you must comply with all USPS regulations applicable to the use of the Service. If you: (a) use your account in a fraudulent or unlawful manner; (b) do not use your account during a consecutive twelve month period; (c) fail to exercise sufficient control over your account to prevent fraudulent or unlawful use; (d) cause or allow the account to be utilized outside the United States without the prior written authorization of USPS Headquarters; or (e) otherwise fail to abide by the provisions of postal regulations and these terms regarding care and use of your account, then your account may be cancelled. You acknowledge and agree that your account may be closed and your ability to use the Service terminated by us for any of the reasons described above or upon demand by the USPS. You agree that any use of the Service to fraudulently deprive the USPS of revenue can cause you to be subject to civil and criminal penalties applicable to fraud and/or false claims against the United States. The submission of a false, fictitious, or fraudulent statement can result in imprisonment for up to five (5) years and a fine of up to \$10,000 (18 U.S.C. 1001). In addition, a civil penalty of up to \$5,000 and an additional assessment of twice the amount falsely claimed may be imposed (31 U.S.C. 3802). The mailing of matter bearing a fraudulent imprint is an example of a violation of these statutes. The USPS has granted to us the license as a PC postage vendor to create a shared postage evidencing system that users will use to dispense postage. As a user of such Service, you must understand and acknowledge that authorization to use the Service is granted by the USPS. You agree to abide by all rules and regulations governing its use. The USPS may deny use of or revoke authorization to use a postage evidencing system in the event of (i) failure to comply with rules and regulations; (ii) submission of false or fictitious information; (iii) entering of a series of unpaid or short-paid mail pieces and/or packages in the mail stream; (iv) use of the system for any illegal scheme or enterprise; (v) use of the system outside the customs territory of the United States; or (vi) possession of a decertified system. You must make the postage evidencing system and transaction records available and surrender the system to us, the USPS, or its agent when notified to do so.

### **17. Assignments**

Reserved.

### **18. U.S. Government Restricted Rights**

If you are an agency of the United States Government, use of the Services by the Government constitutes acknowledgment of our proprietary rights in software contained in the Services, and such software will be: (i) deemed “commercial computer software” or “commercial computer software documentation” and the Government’s rights with respect to such software and documentation are limited by this Agreement, pursuant to FAR § 12.212(a) and/or DFARS § 227.7202-1(a), as applicable, or their successors; and (ii) subject to “RESTRICTED RIGHTS,” as described in FAR52.227-14 and/or

DFAR252.227-7013 et seq., as applicable. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in these regulations.

## **19. Choice of Law; Arbitration; WAIVER OF JURY TRIAL**

Reserved.

## **20. Force Majeure**

Except for a party's payment obligations, neither party will be liable for any delays or failure in performance from any cause beyond their control and without the fault or negligence of the nonperforming party. This includes acts of God, changes to law or regulations, embargoes, war, terrorist acts, riots, strikes, power disruptions, and any disruption of internet service not caused by us. This provision shall become effective only if the party failing to perform promptly notifies the other party of the extent and nature of the problem, limits delay in performance to that required by the event, and takes all reasonable steps to minimize delays.

## **21. Notices**

Notices under this Agreement will be effective (i) in the case of a notice to you, when we send it to the last email or physical address you gave us or any address you may later provide; (ii) in the case of a notice to us alleging a breach of this Agreement, when delivered to us by email to [legalnotices@pb.com](mailto:legalnotices@pb.com) or by overnight courier to Pitney Bowes Inc., 3001 Summer Street, Stamford, CT 06926 along with a copy to our legal counsel: Attn. Chief Legal Officer and Corporate Secretary, or any addresses we may later provide; and (iii) in the case of any other notice to us, when delivered to us by physical mail to Pitney Bowes Inc., EVP & President, Pitney Bowes Sending Technology Solutions, 3001 Summer Street, Stamford, CT 06926 or when you create a case at <https://www.pitneybowes.com/us/contact-us.html> (follow the instructions under "how to create a case").

## **22. Independent Contractor**

Reserved.

## **23. Miscellaneous**

Neither party will be subject to pre-printed or standard terms contained on any purchase order or other purchasing document, and we specifically disclaim such terms. If there's a conflict between the Product Terms and any other provision of this Agreement, the Product Terms will govern and control. However, the SSLRA supersedes and takes precedence over the terms and conditions of this Agreement and the Product Terms. Each Party will cooperate with the other and take such other actions as may reasonably be requested from time to time in order to carry out the intent and accomplish the purposes of this Agreement, including our right to verify your compliance with this

Agreement and any Orders at all locations which you access the Services. If we don't immediately take action on a violation of this Agreement, we're not giving up any rights under this Agreement, and we may still take action at a later point. Each party will also keep confidential the terms and conditions of the Agreement and the SOW(s), unless disclosure is required by law or court order.

**Exhibit A-1 to On-Demand Subscription Service Agreement for the Commonwealth of  
Pennsylvania**

Product Terms for

SendPro® 360 Locker Management, ParcelPoint™ Smart Locker  
Management, SendPro® 360 Receiving and PitneyTrack™ Inbound

(Last modified December 13, 2022)

**Use of the Service**

Reserved.

**Our Responsibilities**

The Service may be inaccessible or inoperable during certain periods so that we can perform routine maintenance support services (“Scheduled Downtime”). Scheduled Downtime will be scheduled outside normal business hours, such as nights and weekends. We’ll use reasonable commercial efforts to minimize any disruption, inaccessibility and/or inoperability of the Services in connection with Scheduled Downtime or other disruption of Service.



**PitneyShip®, SendPro® 360 Sending, PitneyShip® Pro, PitneyShip® Enterprise and  
ShipAccel™ Software**

**Product Terms**

(Last modified July 5, 2024)

**Defined Terms**

“Package(s)” means parcels, letters, and flats shipped under this Agreement.

“Carrier” means a third-party shipping vendor that you use within the Service.

“Tender” means the transfer of physical custody of a Package that has a PBI compliant shipping label affixed to it, by you to a Carrier as demonstrated by the scanning of the label by the Carrier.

**Use of the Service**

In order to use the Service, you must complete the registration process.

Each individual Package Tendered for shipment must originate from a location in the U.S. or certain U.S. territories. You agree that you will only Tender Packages to a Carrier with shipping labels that correspond to the transportation method you selected.

**Fees**

The fees for the use of the Service don’t include the postage, shipping or other charges imposed by the Carrier for printing postage or labels and sending Packages through the United States Postal Service (the “USPS”) or another Carrier.

**Trial Period**

Reserved

**Credit Cards; Accounts with The Pitney Bowes Bank, Inc.**

Reserved.

**Carrier Requirements**

As part of the Service, Pitney Bowes partners with Carriers that enable you to print shipping labels, and these Carriers are responsible for shipping your items. As part of your use of the Service, you must comply with the requirements of those Carriers.

If you use the Service for shipping with the USPS, you must comply with all applicable terms, conditions, rules and regulations established by the USPS. Failure to comply may

constitute a material breach and the USPS may provide written notice of termination. However, if allowed by USPS, you will have ten (10) days from date notice is received from USPS or a copy of such written notification from us, whichever is earlier, to cure your violations of USPS policies and procedures and have USPS rescind its termination notice.

You may be entitled to receive discounted rates for Packages you Tender to the USPS for shipment.

Rates are subject to change at any time.

If you use the Service to send Packages with a Carrier other than the USPS, you must comply with the requirements of that Carrier, unless you have a separate agreement with the Carrier, in which case the terms of your agreement take precedence and govern.

### **Third-Party Systems**

We may provide functionality to enable you to link your account to certain third-party systems, such as marketplaces, enterprise resource planning systems (or ERPs), warehouse management systems, and healthcare system platforms. These third-party systems ("TPS"), their authentication process and any data they provide us (and its accuracy) are not under our control and we are not responsible for it. You must be the TPS account holder of any account you link to us and will comply with all TPS terms and conditions.

### **HIPAA**

Reserved.

# SendSuite® Tracking Online Product Terms

(Last modified October 13, 2022)

## **Our Responsibilities**

The Service may be inaccessible or inoperable during certain periods so that we can perform routine maintenance support services (“Scheduled Downtime”). Scheduled Downtime will be scheduled outside normal business hours, such as nights and weekends. We’ll use reasonable commercial efforts to minimize any disruption, inaccessibility and/or inoperability of the Services in connection with Scheduled Downtime or other disruption of Service.

## **SendPro® Enterprise Subscription**

### **Product Terms**

(Last modified July 5, 2024)

#### **Defined Terms**

“Package(s)” means parcels, letters, and flats shipped under this Agreement.

“Carrier” means a third-party shipping vendor selected by you through the Service.

“Tender” means the transfer of physical custody of a Package that has a PBI compliant shipping label affixed to it, by you to a Carrier as demonstrated by the scanning of the label by the Carrier.

#### **Use of the Service**

Reserved.

Each individual Package Tendered for shipment must originate from a location in the U.S. or certain U.S. territories. You agree that you will only Tender Packages to a Carrier with shipping labels that correspond to the transportation method you selected.

#### **Fees**

The fees for the use of the Service don’t include the postage, shipping or other charges imposed by the Carrier for printing postage or labels and sending Packages through the United States Postal Service (the “USPS”) or another Carrier.

#### **Using USPS**

If you use the Service for shipping with the USPS, the USPS must approve your registration prior to use of their shipping services and you must comply with all applicable terms, conditions, rules and regulations established by the USPS. Failure to comply may constitute a material breach and the USPS may provide written notice of termination. However, if allowed by USPS, you will have ten (10) days from date notice is received from USPS or a copy of such written notification from us, whichever is earlier, to cure your violations of USPS policies and procedures and have USPS rescind its termination notice. You may be entitled to receive discounted rates for Packages you Tender to the USPS for shipment. These rates will be programmed into the Service and will be made available to you for the duration of this Agreement. Rates are subject to change at any time.

When you print USPS postage or labels using the Service, the following information is collected in order to generate valid postage indicia: (1) the date and time of the transaction;

(2) the destination ZIP Code™; (3) the rate category of each indicium created and the details of any associated special services, such as special handling or restricted delivery; and (4) the amount of postage printed.

If you use the Service to print electronic USPS Tracking (formerly Delivery Confirmation), Signature Confirmation™, or the electronic Priority Mail Express® label, complete return and destination address data, package descriptions, reference IDs, and delivery statuses for each label printed by you is maintained by us for accounting and reporting purposes.

### **Non-USPS Carrier Requirements**

If you use the Service to send Packages with a Carrier other than the USPS, you must comply with the requirements of that Carrier, unless you have a separate agreement with the Carrier, in which case the terms of your agreement take precedence and govern.

### **HIPAA**

Reserved.

## **Exhibit A-2**

# **Business Privacy Statement**

This Privacy Statement was last updated on May 17, 2024.

Pitney Bowes is committed to respecting the privacy of our clients and users. This Privacy Statement describes how our websites, services, and products operate, and how we collect, use, and share information.

This Privacy Statement applies to pitneybowes.com and Pitney Bowes websites, services, and products that collect data and display these terms, and that are owned and operated by Pitney Bowes and Pitney Bowes subsidiaries, collectively, "Pitney Bowes". Pitney Bowes websites, services and products are referred to in this statement as "Sites". These terms do not apply to Pitney Bowes sites that do not display or link to this statement or that have their own privacy statements. For example, the terms of this statement apply to Sites where we provide products, services, or applications as a business-to-business provider to a client for that client's business or commercial use. In contrast, where we provide products, services, or applications direct to individual consumers for personal or household use, the data collection and processing is governed by a different privacy statement (which you can review by clicking [here](#)) and not this Privacy Statement.

**The following topics are presented in this Privacy Statement:**

1. [Personal Information Users Actively Provide to Us](#)
2. [Personal Information that We Collect Passively from Use of the Site](#)
3. [Using and Retaining Personal Information](#)
4. [Sharing Personal Information](#)
5. [Protecting Personal Information](#)
6. [Visiting Nonaffiliated Pitney Bowes Websites](#)
7. [Cross Border Data Transfer](#)
8. [Data Privacy Framework \(DPF\) Notice](#)
9. [Your Choices](#)
10. [Your Rights](#)
11. [Country/Region-Specific Notices](#)
12. [State-Specific Notices \(U.S.A.\)](#)
13. [Product-Specific Statements](#)
14. [Use of Sites by Minors](#)
15. [Changes to this Privacy Statement](#)
16. [Contact Us About this Privacy Statement](#)

## **1. Personal Information Users Actively Provide to Us**

This section describes the various types of information that we may collect. In order to provide you with access to certain services or data within our Sites, we may require that you provide certain personal information, which may include, but is not limited to the examples listed below, "Personal Information". Pitney Bowes also collects non-personal information that does not, on its own, identify an individual person. When non-personal information is combined with other information so that it does identify an individual person, we treat that combination as Personal Information.

The following are examples of the types of information that is considered Personal Information and that may be collected directly from you (or someone acting on your behalf):

- Business Contact information (including Name, Street Address, Email Address, Telephone Number)
- Government issued IDs (such as tax identification number) provided by you for business purposes
- Pitney Bowes business user account username, password, and other information used in combination to verify identity
- Corporate financial information (including credit/debit card and bank account information, credit and repayment history, and payment default information)
- Geolocation, demographic, shipping/receiving, billing, and other information related to the purchase or delivery of Pitney Bowes products and services or services you access through the Sites
- Any other personal information or characteristics about an individual that identifies such individual alone or that, if used in combination with one of the above or with other non-personally identifiable information, allows someone to identify such individual, such as date or place of birth, geographic data, or photographic images

By accessing and utilizing our Sites, including any interactive or automated chat or customer support features that may be made available on our Sites, or providing feedback to us or in connection with any optional surveys, you consent to the collection, use, disclosure, storage, and processing of Personal Information in accordance with this Privacy Statement. Please note, by law you are not required to provide us with your Personal Information. By electing to not share your Personal Information with us, you may be unable to take advantage of our Sites and we may be unable to provide you with all of the functionality we offer through our Sites or to fulfill your request.

## **2. Personal Information that We Collect Passively from Use of the Site**

Pitney Bowes Sites may use several automated data collection tools and techniques including cookies, clickstream, and web beacons.

### **Cookies**

## **Clickstream Web Beacon IP Address Do Not Track Requests**

### **3. Using and Retaining Personal Information**

Personal information we collect through our Sites may be used to provide Pitney Bowes products and services pursuant to the terms and conditions of contracts with our business clients. The legal basis for our use of your Personal Information in that context is to service the business client's contract and to carry out our legitimate business interests. We may also use your Personal Information to provide you as a client business representative with information regarding our products and services, or for marketing and promotions we believe you or your employer may find of interest. When we use your Personal Information in that context, the legal basis we use is legitimate business interest and, where required, your consent. We also may use the Personal Information you provide for our internal purposes, such as Site customization, enhancement or development, administration and operation of our Sites, data analytics, to help build, train, and improve the accuracy of our automated methods of processing, to communicate with you about your account, to fulfill any other purpose for which you provide it, and compliance with our legal obligations, policies and procedures, including performance of Pitney Bowes obligations under sales contracts, leases or licenses between you and Pitney Bowes. In such instances, the legal basis for processing your Personal Information is to perform under our business client contracts and to exercise our legitimate business interests.

Unless a longer retention period is required or allowed by law, we retain your Personal Information for the period disclosed to you at the time of collection, if any, or for the period necessary to fulfill any of the relevant purposes disclosed in this Privacy Statement.

### **4. Sharing Personal Information**

Pitney Bowes does not sell Personal Information to third parties. However, there are certain situations where we may share your Personal Information where permitted or required by law, for example:

1. Within the Pitney Bowes family of businesses, among personnel whose job duties require access to your Personal Information. Our legal basis for sharing your Personal Information in this instance is our contract with our business client and our legitimate business interests;
2. With third parties that perform services for us or on our behalf (such as credit card companies, credit and/or investigative reporting agencies, finance



companies, transport companies, consultants, advisors and market research firms). Our legal basis for sharing your Personal Information in this instance is our contract with our business client and our legitimate business interests; or

3. For marketing campaigns conducted by us or other companies or organizations that offer related products or services we believe may be of interest to our clients, subject to your rights and choices as described in this Privacy Statement. Our legal basis for sharing your Personal Information in this instance is your consent when required, and our legitimate business interests.

Our service providers are required to keep the Personal Information received from us confidential and secure in accordance with this Privacy Statement and they may not use it for any purpose other than the purpose for which Pitney Bowes provided it.

We may also make information available to third parties in the following circumstances:

1. When we have a good faith belief it is required by law or to otherwise cooperate with law enforcement activity;
2. When we have a good faith belief it is necessary to protect our rights or property from fraudulent, abusive, or unlawful activity; or
3. In the event of a proposed or actual merger, acquisition, liquidation, dissolution, or sale of assets.

In these circumstances, the legal basis for sharing your Personal Information is our legitimate business interests. Although your consent will not be required in these instances, we will attempt to notify you, to the extent the law requires.

Depending upon local law, you may either opt-in or opt-out of having your Personal Information shared for marketing or other purposes. In the event you opt-in, we will use and share your Personal Information as described in this Privacy Statement. In the event you opt-out, we will share your preference with the applicable third parties as appropriate. For information on how to do this, see the Your Choices section of this Privacy Statement below.

## **5. Protecting Personal Information**

We maintain reasonable administrative, technical, and physical safeguards to protect the Personal Information we collect and process. No data transmission over the internet or data storage system can be guaranteed to be 100% secure. If you feel that the security of any data that we hold about you has been compromised, please immediately notify us of the problem by contacting us in accordance with the Contact Us section below.

The safety and security of your information also depend on you. Where we have given you (or where you have chosen) a password for access to certain parts of the Sites, you are responsible for securing and managing your login credentials.

## **6. Visiting Nonaffiliated Pitney Bowes Websites**

Our Sites may include links to third-party websites that operate independently from Pitney Bowes. Linked websites may have their own privacy statements or notices. Clicking on those links may allow those website owners to collect or share data about you. We are not responsible for: the content of any websites that are not affiliated with or owned by Pitney Bowes, any use of those websites, or the privacy practices of those websites; and we strongly suggest you review their privacy statement for more information. Any information you provide when you visit a nonaffiliated Pitney Bowes website is subject to the privacy statement and terms of use posted on that website.

## **7. Cross Border Data Transfer**

The international footprint of Pitney Bowes involves transfers of Personal Information between different subsidiaries, as well as to third parties located in the countries where we or our service providers operate. We may process, store, and transfer the Personal Information we collect, in and to a country outside your own, including outside the United States. Those countries may not have the same data protection laws as the country in which you initially provided the information. By providing Personal Information or engaging with our Sites, you consent to this transfer, storing, or processing.

Some countries restrict certain transfers of Personal Information. Pitney Bowes complies with those restrictions by taking at least one or more of the following actions, including:

- Pitney Bowes Inc. and its wholly-owned U.S. subsidiaries that receive Personal Information from countries outside of the United States adhere to applicable law and regulations regarding client, partner and employee Personal Information moving across geographical and jurisdictional borders.
- Where required or permitted, Pitney Bowes implements Standard Contractual Clauses approved by the EU Commission, or similar clauses in other jurisdictions, where available, between our corporate entities, our partners, and our clients.
- Where applicable, Pitney Bowes relies on adequacy decisions, as adopted by the applicable authority or regulatory body. In particular, information about the Data Privacy Framework (DPF) and Pitney Bowes commitment to comply with the EU-US DPF, the UK Extension to the EU-US DPF, and the Swiss-US DPF may be found in the Data Privacy Framework (DPF) Notice section below.

Additional information may be found under the sections below concerning Country-Specific and State-Specific Notices for the geographies in which you are located.

## **8. Data Privacy Framework (DPF) Notice**

Pitney Bowes has self-certified its commitment to comply with the EU-US Data Privacy Framework, the UK Extension to the EU-US DPF (the UK Data Bridge), and the Swiss-U.S. DPF as set forth by the United States Department of Commerce regarding the collection, use, processing, and retention of Personal Information transferred from the European Union, Switzerland, and the United Kingdom (and Gibraltar) to the United States.

Pitney Bowes has self-certified its commitment to comply with the EU-U.S. DPF Principles and relies on the European Commission's adequacy decision for the EU-U.S. DPF for such transfers.

Pitney Bowes has self-certified its commitment to comply with the UK Data Bridge and the Swiss-U.S. DPF and relies on the UK Data Bridge or the Swiss-U.S. DPF to receive Personal Information from the United Kingdom (and Gibraltar) or Switzerland, respectively, as applicable.

We have certified to the United States Department of Commerce that we adhere to the DPF Principles with respect to Personal Information. If there is any conflict between the terms in this Privacy Statement and the DPF Principles, the DPF Principles shall govern. To learn more about the DPF program, and to view our certification page, please visit <https://www.dataprivacyframework.gov> and search for "Pitney Bowes".

Pitney Bowes is responsible for the processing of Personal Information it receives, under the DPF, and subsequently transfers to a third party acting as an agent on its behalf. Pitney Bowes complies with the DPF Principles for all onward transfers of Personal Information, including the onward transfer liability provisions.

With respect to Personal Information received or transferred pursuant to the DPF, Pitney Bowes is subject to the regulatory enforcement powers of the United States Federal Trade Commission. In certain situations, we may be required to disclose Personal Information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

### **Complaints and Free Dispute Resolution Procedure**

In compliance with the EU-U.S. DPF, the UK Data Bridge, and the Swiss-U.S. DPF, Pitney Bowes commits to resolve complaints about your privacy and our collection or use of your Personal Information. As described more fully below, in the first instance, we try to work with you directly to resolve your complaint. If that process fails, we pay for an alternative dispute resolution process, giving you an independent recourse mechanism for resolving the complaint.

Accordingly, if you believe Pitney Bowes processes your Personal Information beyond the scope of our DPF certification, you may direct any inquiries or complaints concerning our compliance to us at the information in the Contact Us section below. Pitney Bowes will respond in a manner consistent with the DPF or applicable law.

If you do not receive timely acknowledgment of your DPF Principles-related complaint from us, or if we have not addressed your DPF-Principles complaint to your satisfaction, you may file a complaint with our U.S.-based alternative dispute resolution provider, or under certain conditions, more fully described on the Data Privacy Framework website and in Annex I of the DPF, you may be able to invoke binding arbitration when other dispute resolution procedures have been exhausted. Please contact or visit the DPF Program website at <https://www.dataprivacyframework.gov/s/article/How-to-Submit-a-Complaint-Relating-to-a-Participating-Organization-s-Compliance-with-the-DPF-Principles-dpf> for more information or to file a complaint. For more information or to file a complaint with our U.S.-based alternative dispute resolution provider, please visit <https://www.jamsadr.com/DPF-Dispute-Resolution>. The services of the alternative dispute resolution provider are provided at no cost to you.

## 9. Your Choices

If you are a Pitney Bowes customer, you may receive transactional communications about your account and the Pitney Bowes products and services, which you own, lease, rent, license or to which you subscribe.

In some jurisdictions, you may have to opt-in to receive marketing communications. In the event you opt-in, we will use and share your Personal Information as described in this Privacy Statement. If you wish to opt-out of receiving marketing communications from Pitney Bowes, you may do so by (i) following the instructions provided in our marketing communications, or (ii) indicating your preferences on the relevant account profile/preferences section (such as Your Account), or (iii) clicking [opt-out](#) to be removed from marketing communications. In the event you opt-out, we will share your preference with applicable third parties as appropriate. You will continue to receive transactional communications about your account, any events that you have registered to attend, and the Pitney Bowes products and services which you own, lease, rent, and license or to which you subscribe.

Some of our products and services contain settings that allow users or administrators to control how the products collect information. If you wish to request changes to your Personal Information, you may do so by (i) indicating your preferences on the relevant account profile/preferences section (such as Your Account), or (ii) [clicking here](#) to update the physical location of a product or billing address. Please note, by electing to not share certain Personal Information with us, we may be unable to provide you with all of the functionality we offer through our Sites.

## 10. Your Rights

Subject to applicable exceptions, you may have the right under applicable privacy and data protection laws to request, as it relates to your Personal Information:

- (i) access,
- (ii) correction,
- (iii) deletion,
- (iv) restriction of our processing,
- (v) objection to our processing, or
- (vi) a copy for data portability.

If you would like to make a request, please use the contact information listed below in the Contact Us section of this Privacy Statement. We will respond to your request in a timing and manner consistent with applicable law. We may need to verify your identity before we can act on your request. In some jurisdictions, you can designate an authorized agent to make a request on your behalf. Please provide the agent with written permission, signed by you, for the agent to submit with the request. We may contact you to verify your identity and the authorized agent's permission before we can act on your request.

Please note that we may reject or decline requests, or limit the information we provide access to, if we determine it could risk the privacy of others, or if unreasonable or repetitive, or if it would require disproportionate effort, or for which a response is not otherwise required by local law.

As permitted by law, we may charge a reasonable fee in connection with responding in certain circumstances (such as if your request is frivolous/vexatious, repetitive, or excessive), but we do not charge for lodging a request.

Please understand that we cannot delete Personal Information in certain circumstances, such as where retention is required for our legitimate business or recordkeeping purposes, to fulfill a transaction you initiated prior to your request, or otherwise required by law (such as for fraud prevention or legal compliance). Please note that we will not unlawfully discriminate against you for exercising your privacy rights.

## **11. Country/Region-Specific Notices**

Pitney Bowes Inc. is a global corporation with subsidiary companies located around the world. This Privacy Statement establishes our global principles (to the extent the law permits and/or requires) for the collection, use and disclosure of information gathered through our Sites. The country in which you are doing business with us or where the Site you are visiting is located or hosted may have specific requirements concerning Personal Information, which you may find below. If you believe that there are disclosures required by a law that is applicable to you, which you do not see in this Privacy Statement, please contact us as provided in this Privacy Statement.

**Australia**  
**Brazil**  
**Europe**

## 12. State-Specific Notices (U.S.A.)

### California

This section applies only to individuals who reside in the state of California.

#### Notice at Collection

We collect the categories of Personal Information for the purposes and retention described in this Privacy Statement. Additional information about your rights and other notice is provided in this section below.

#### **Additional Disclosures Under the California Consumer Privacy Act (“CCPA”) As Amended by the California Privacy Rights Act (“CPRA”)**

The following chart includes: (1) the categories of Personal Information, as defined under California law, that we plan to collect and have collected and disclosed within the preceding 12 months; and (2) the categories of third parties to which we disclosed Personal Information for our operational business purposes within the preceding 12 months.

<b>Categories of Personal Information</b>	<b>Disclosed to Which Categories of Third Parties for Operational Business Purposes</b>
<b>Identifiers</b> , such as name, contact information, online identifiers, IP address, account identifier, or email address.	Affiliates; vendors
<b>Personal information, as defined in the California customer records law</b> , such as name, contact information, insurance policy number, education, employment, employment history, financial information, medical information and health insurance information.	Affiliates; vendors
<b>Characteristics of protected classifications under California or federal law</b> , such as sex, age, race, religion, national origin, disability, medical conditions and information, citizenship, immigration status and marital status.	Affiliates; vendors
<b>Commercial information</b> , such as transaction information, purchase history and financial details.	Affiliates; vendors; business partners

<b>Internet or network activity information</b> , such as browsing history, online behavior, and interactions with our and other websites, applications and systems.	Affiliates; vendors; professional advisors, such as legal advisors; legal authorities, government agencies, and regulators
<b>Geolocation data</b> , such as device location, your physical location, and IP location.	Affiliates; vendors
<b>Audio, electronic, visual, and similar information</b> , such as images and audio, video or call recordings created in connection with our business activities.	Affiliates; vendors; professional advisors, such as legal advisors; legal authorities, government agencies, and regulators
<b>Professional or employment-related information</b> , such as employer.	Affiliates; vendors; professional advisors, such as legal advisers, accountants, and financial advisers; legal authorities, government agencies and regulators
<b>Inferences</b> drawn from any of the personal information listed above to create a profile or summary about, for example, an individual's preferences and characteristics.	Affiliates; vendors

## Your Rights as a California Resident

**Right to Disclosure of Information:** You have the right to request that we disclose certain information regarding our practices with respect to Personal Information. If you submit a valid and verifiable request and we confirm your identity and/or authority to make the request, we will disclose to you any of the following at your direction:

1. The categories of Personal Information we have collected about you in the last 12 months.
2. The categories of sources for the Personal Information we have collected about you in the last 12 months.
3. Our business or commercial purpose for collecting that Personal Information.
4. The categories of third parties with whom we share that Personal Information.
5. The specific pieces of Personal Information we collected about you.
6. If we disclosed your Personal Information to a third party for a business purpose, a list of the Personal Information types that each category of recipient received.

**Right to Delete Personal Information:** You have the right to request that we delete your Personal Information collected from you and retained, subject to certain exceptions. Upon receiving a verified request to delete your Personal Information, we will do so unless otherwise authorized by law.

**Right to Correct Your Personal Information:** If you find that we maintain inaccurate Personal Information, you have the right to request that we correct such inaccuracy. You may also be able to update or make corrections through your account.

**Right to Limit Use of Sensitive Personal Information:** You have the right to instruct us to limit our use of your Sensitive Personal Information to that which is necessary to provide the Services. You may do so by contacting us as detailed below.

**Right to Opt Out of the Sale or Sharing of Your Personal Information:** You have a right to opt-out of the sale or sharing of your Personal Information. You may, at any time, direct businesses that sell your Personal Information to third parties not to sell or share your Personal Information. You may do so by contacting us as detailed below.

**Right to Non-Discrimination:** You have the right not to be discriminated against for the exercise of your California privacy rights described above.

### **Your Rights Under California's Shine the Light Act**

California residents are legally entitled (at no charge and no more than once per year) to request information about how we may have shared your information with others for their direct marketing purposes. To make such a request, please refer to the instructions provided in the Contact Us section below.

### **How to Exercise These Rights**

If you wish to submit a request to exercise one or more of the rights listed above or if you have questions or concerns with respect to our Privacy Statement, please contact us using the information provided in the Contact Us. Please include your question or concerns in your letter to us, including the Pitney Bowes brands, Sites, products, and services relevant to your question or concern.

We will respond to verifiable requests for disclosure or deletion of Personal Information free of charge, within 45 days of receipt. We may extend the period where reasonably necessary, taking into account the complexity and number of requests, and will inform you of the extension.

To protect your privacy and the security of your information, we verify such requests by requesting identification documents and other documentation necessary to confirm your identity. Any additional information you provide will be used only to verify your identity and not for any other purpose.

### **Authorized Agents**

If you want to make a request as an authorized agent on behalf of a California resident, you may use the submission methods noted above. As part of our verification process, we may request that you provide, as applicable, proof concerning your status as an



authorized agent. In addition, we may require the individual on whose behalf you are making the request to verify their own identity or your permission to submit the request.

**Additional Information About Disclosure of Personal Information of California Residents**  
Pitney Bowes does not sell your Personal Information to third parties. However, there are certain situations where we may share your Personal Information where permitted by law, for example:

1. Within the Pitney Bowes family of businesses,
2. With third parties that perform services for us or on our behalf (such as credit card companies, credit and/or investigative reporting agencies, finance companies, transport companies, consultants, advisors and market research firms), or
3. For marketing campaigns conducted by us or other companies or organizations that offer Pitney Bowes-related products or services we believe may be of interest to our clients.

Our service providers are required to keep the Personal Information received from us confidential and secure in accordance with this Privacy Statement and they may not use it for any purpose other than the purpose for which Pitney Bowes provided it.

As outlined in the Your Rights section you have the right to know more about the Personal Information we have about you. To obtain this information, please refer to the instructions provided in the Your Rights section.

If you wish to opt-out of receiving marketing communications from Pitney Bowes or make changes to your Personal Information, please refer to the instructions provided in the Your Choices and Contact Us sections.

## **13. Product-Specific Statements**

Pitney Bowes offers a wide range of products and services. In some instances, additional data collection practices and privacy statements may apply to specific Pitney Bowes products. Those privacy statements are provided within the product and may be found below. In case of contradictions between the general Privacy Statement of Pitney Bowes and the information in a product-specific statement, the information in the product-specific statement will take precedence.

- [Personal Shipping](#)

## **14. Use of Sites by Minors**

Pitney Bowes does not direct its Sites to minors and we do not knowingly collect Personal Information from minors. If we become aware of such processing, we will take steps to stop it and to delete such Personal Information. If you believe we mistakenly or

unintentionally collected any information from a child, please notify us by using the contact information listed below in the Contact Us section of this Privacy Statement.

## **15. Changes to this Privacy Statement**

Pitney Bowes may change this Privacy Statement from time to time and at its discretion. We will indicate at the top of the Privacy Statement when it was most recently updated. We will not use your Personal Information in ways that differ materially from this Privacy Statement without prior notice to you. You are responsible for ensuring we have a current and deliverable email address for you. Please check back periodically to see any updates or changes to our Privacy Statement. Your continued use of our Sites indicates your consent to this Privacy Statement and any amended version of it.

## **16. Contact Us About this Privacy Statement**

If you have any questions or comments about this Privacy Statement, please contact us at:

Global Data Protection Office  
c/o Pitney Bowes Inc.  
3001 Summer St  
Stamford, CT USA 06926-0700

or

Email us @ [privacyoffice@pb.com](mailto:privacyoffice@pb.com)

Please see below for contact information for the following countries, which should be used if you have a question, comment, or complaint about this Privacy Statement for your specific country

**Australia**

**Brazil**

**Germany**

**India**

**Japan**

# On-Demand Subscription Services Product Support Terms

(Last modified: September 2023)

As part of your access to the Services, we will provide you with the following:

a) SELF HELP. 24/7 access to web self-help and user and support articles.

b) TECHNICAL SUPPORT. We provide technical support via chat, over the phone and via the Internet (“Remote Support”) unless otherwise specified. To receive Remote Support you must provide us access to your device. When submitting an issue, you will be requested to provide sufficient detail for us to reproduce the problem. Additional support, such as diagnosis of your IT environmental or infrastructure issues, may be available, subject to additional terms and fees.

(i) Chat Support. Contact PB within the Services product if applicable or at <https://www.pitneybowes.com/us/support/contact-us.html>.

(ii) Telephone Support. PB product support is available from 7 am to 7 pm Central Time, Monday through Friday, excluding PB observed US holidays (“Normal Operating Hours”). Contact numbers are located at <https://www.pitneybowes.com/us/support/contact-us.html>.

(iii) Electronic Requests. You may submit a request to PB Product Support electronically by going to [www.pitneybowes.com](http://www.pitneybowes.com), signing in to Your Account, and submitting a ticket 24 hours a day, 7 days a week. Requests received outside Normal Operating Hours are processed the next business day.

(iv) If there are 50 or more users within your organization, then you must identify a limited number of staff who are responsible for escalating requests for support assistance to us (“Authorized Personnel”). We will provide remote technical support assistance to the Authorized Personnel for issue resolution with the Services. Authorized Personnel will then be responsible for providing technical support to other users within your organization. Any issue escalated to us for technical support must be related to Services provided by us (and not to your organization’s operating environment or other hardware or software). Additional fees will apply if your organization does not have Authorized Personnel available.

## PREMIER SUPPORT ADD-ON SUPPLEMENT OPTION

Under your On-Demand Subscription Service product support, you may elect to purchase supplemental PREMIER SUPPORT. This option is charged at an annual or monthly rate as set forth in your Order and will make the following Premier Support service benefits available to you:

- Upon initial sign up for Premier Support, your assigned Account Manager will contact you at the phone number you provide with your Order, confirm future preferred method of contact, and discuss the following benefits.
- You will be given a premier 4-digit PIN number to access the team of Premier Support Agents and Case Managers. This gives you direct access to Level 2 Support Desk Agents and Case Managers for product support issues.
- When you use the premier PIN code, your call will be queued in front of all non-Premier calls and routed to the Level 2 Support Desk Agents. As a result your call will be answered ahead of any other non-Premier callers. Your product support case will be managed by a single point of contact all the way through the resolution of your case. If Pitney Bowes determines a dispatch of a technician to your site must be created, your assigned Case Manager will coordinate the field technician visit with our dispatch center so that it is handled in an expedited manner and follow up to ensure successful resolution.
- You are able to request alternate forms of remote access sessions for product support initiated by you. Upon your request, we will make reasonable attempt to employ the remote access technology that you choose for product support.
- Should any parts be required, we will make reasonable attempt to expedite the part(s) to your location for next day installation and repair.
- Your assigned Account Manager will conduct a support assessment two (2) times per calendar year which would include consultative analysis to ensure you are optimizing the value of this level of support.

#### **Exhibit A-4**

##### **USPS License Terms for use of the USPS Data**

(Last modified July 10, 2020)

The following terms apply solely to your use of the United States Postal Service (“USPS”) data that is provided under license to you from the licensor from which you receive the USPS data (“Licensor”). Absent a signed Agreement, your use of the USPS Data constitutes acceptance of the terms set forth herein. Capitalized terms used herein and not otherwise defined have the meaning assigned to them in the Agreement. The terms and conditions set forth below supersede any conflicting terms and conditions in the Agreement.

a) The delivery point validation (the “DPV® Product”), LACSLink® and SuiteLink® and any updates, materials, know-how, computer code, and technical information (hereinafter collectively, the “USPS Data”) are confidential and proprietary to the USPS and shall remain the property of USPS. You shall maintain the USPS Data in strict confidence in accordance with the terms of the Agreement.

b) You are prohibited from: (i) modifying, improving, correcting, or enhancing the USPS Data in any way; (ii) combining the USPS Data, or any portion thereof, with other information, data, software or the like to create any derivative product of the USPS Data; or (iii) make or reduce to practice any invention, idea or concept, whether patentable or not, on or relating to the USPS Data or any portion thereof without the prior written approval of USPS.

c) You shall not: (i) use the USPS Data or any of its technology to compile a list of delivery points not already in your possession or to otherwise create a mailing list or portion thereof; (ii) rent, sell, distribute or otherwise provide any of your proprietary address lists, service products, or other system of records that contain address attributes derived or updated through the use of the USPS Data; or (iii) in addition to the foregoing, use SuiteLink for any purposes other than for improving business delivery addresses in multi-occupation buildings for use on letters, flats, postcards, packages, leaflets, magazines, advertisements, books and other printed material, and any other item that will be delivered by USPS.

d) You are not permitted to export the USPS Data outside the United States or its territories.

e) You agree and acknowledge that USPS retains all right, title and interest in the USPS Data, and all trademarks, trade dress, service marks, trade secrets, copyrights, patents and other intellectual property rights related thereto.

f) The USPS shall be a third-party beneficiary with respect to the license to the USPS Data granted hereunder and thereby shall have the right to directly enforce against you the restrictions with respect to the USPS Data set out herein.

g) NEITHER LICENSOR NOR THE USPS SHALL BE LIABLE FOR ANY DESIGN, PERFORMANCE OR OTHER FAULT OR INADEQUACY OF THE USPS DATA. This disclaimer is in addition to any other disclaimers of warranties set out in the Agreement.

h) To satisfy USPS requirements THE DPV PRODUCT SHALL CONTAIN DISABLING DEVICE(S) DESIGNED TO PREVENT USE NOT PERMITTED BY THIS LICENSE. Licensor shall document all disabling devices to you. In the event you encounter the “Stop DPV Processing” function, you shall contact Licensor in order to restore DPV processing capability. Licensor shall immediately notify USPS of your name and address. At the sole discretion of the USPS, Licensor may not have the right to restore your DPV processing capability.

i) Notwithstanding any provision set out in the Agreement regarding any limitation of liability, you shall promptly reimburse Licensor to the full amount of any damages or other claims that Licensor is required to pay, and shall otherwise hold Licensor harmless from demands, costs and damages paid to third parties, which are a result of your failure to comply with any of the obligations set out in these provisions.

j) Notwithstanding anything to the contrary elsewhere in the Agreement or any applicable order, the USPS Data is not licensed on a perpetual basis and may only be licensed for the limited term set out in the applicable order. You may elect to renew your term license to the USPS Data to the extent Licensor continues to offer a license to the USPS Data, for an additional term upon payment of the applicable renewal fees. Licensor shall have the right to terminate your license to the USPS Data if (i) the USPS cancels Licensor’s or its licensors’ right to distribute the USPS Data, (ii) you are in breach of any of the foregoing provisions; or (iii) the Agreement or applicable order is terminated.