Version 4.0

pitney bowes

Pitney Bowes Smart Access Management®

Product Documentation

January 25, 2023

Contents

1. Visitor Experience – Kiosk App

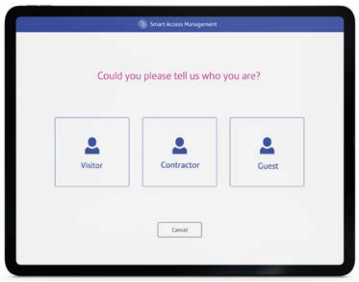
a. Experience Overview

Homepage

Pitney Bowes Smart Access Management kiosk app offers customised sign-in/sign-out for visitors and staff. Visitors can accept customised terms and conditions and can submit required documents via their mobile device. Information captured by the kiosk app is synced in real-time to the admin app.

Pitney Bowes Smart Access Management enables you to create the look and feel of kiosk app screens with custom text and colours for backgrounds, headers and footers and a custom logo for the home page and visitor badge.

Visitor type selection



Personal details (Portrait mode)

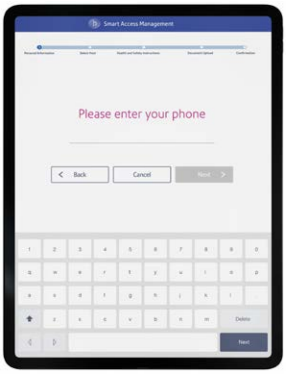
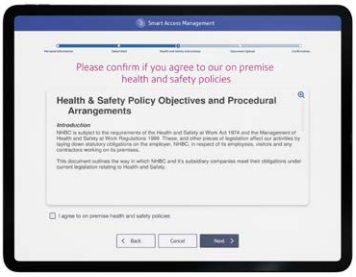


Photo capture (Portrait mode)

Health and safety instructions



b. Features Checklist

Facial Recognition
Identify or confirm a visitor or staff's identity via facial recognition technology.

E-Signature Capture
Offer visitors the ability to sign non-disclosure agreements or policy requirements.

Auto Sign-out
Set-up a time for all visitor types to be automatically signed-out.

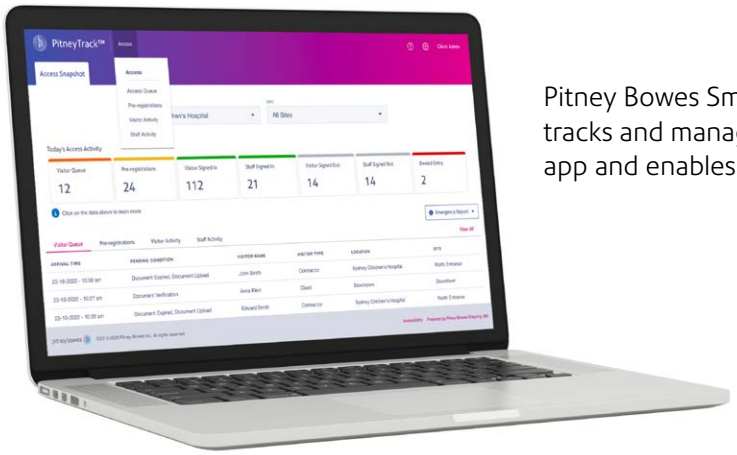
QR Code Sign In
Expedite pre-registered, returning visitors or staff sign-in by scanning a badge or QR code received by email.

Contactless Sign-in
Offer visitors and staff the ability to sign-in with a mobile device by scanning a QR code displayed on the screen.

Photo Capture
Capture a visitor photo during the sign-in process.

2. Admin Experience – Web App

a. Experience Overview



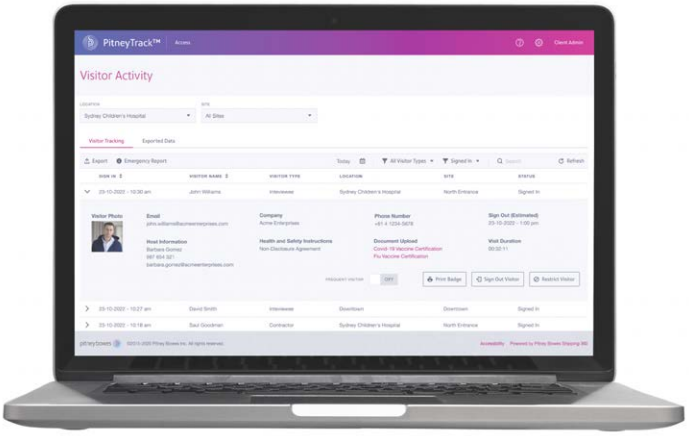
Homepage dashboard

Pitney Bowes Smart Access Management admin app tracks and manages information captured by the kiosk app and enables custom preference configurations.

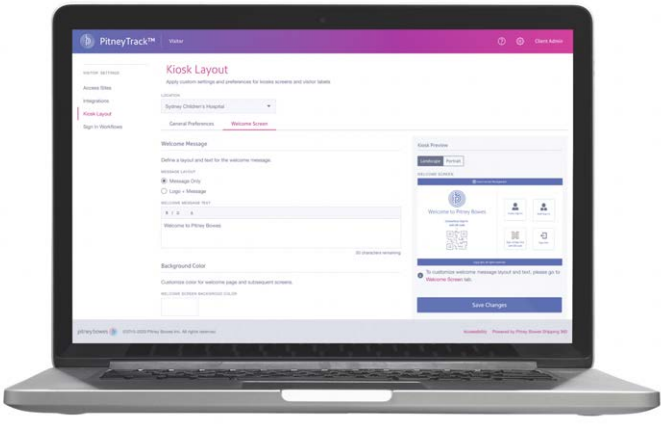
Visitor and Staff Reports:
View, import, export and manage reports that track user and staff activities.

Access Settings:
Manage access sites, visitor types, Webhook & Azure AD integrations, and the kiosk app customisation.

Product Settings:
Manage contacts, users, locations & sites, notifications and device settings.



Visitor Activity report



Kiosk Layout settings

2. Admin Experience – Web App

b. Features Checklist

Visitor and Staff Dashboards

Daily Activity Indicators
Offers tracking of daily visits of a location and site on the home page.

Visitor Queue Control / Document Approval
Enables document verification for sign-in approvals.

Searchable and Filterable Reports
Allows filtering of visitor and staff reports.

Visitor Restriction
Restrict sign-in and manage unwanted visitors on a given site with a single click.

Sign-out by the Admin App
Manually sign-out a given user with a single click.

Visitor Pre-registration
Create a pre-registration with an email and name of one or multiple visitors to send them registration instructions.

Emergency Report
Generate a report of visitors and staff logged in on a given site.

Exported Data Management
Manage and customise reports asynchronously.

Frequent Visitor Setting
Expedite the sign-in process of recurrent visitors to a single location and site.

Badge Printing
Print new visitor badges due to status or information updates.

Access Settings

Custom Visitor and Staff Types
Create and manage unlimited visitor and staff types.

Custom Site Settings
Allows individual configuration for a given site based on your business needs and preferences.

Custom Sign-in Workflows
Define and customise the sign-in workflow experience for a given visitor or staff type.

Custom Sign-in Limit
Set the maximum capacity for signed-in visitors at a given site.

Webhook Integration
Enable event-driven integrations to send real-time information to other systems.

Branding and Design Personalisations
Configure the kiosk app screen look & feel.

Phone Number OTP Verification
Verify the visitor's phone number by a one time password sent via SMS.

Active Directory Integration
Sync Azure AD read-only contact information.

Custom Notification Settings
Specify which visitors will receive given types of email and/or SMS notifications.

Product Settings and Preferences

Contact Management
Easily create, manage, import and export contacts through Address Book.

Custom Email & SMS Notification
Create customised visitor emails and SMS notifications via templates.

3. Technical Details

a. Governing Standards

The Pitney Bowes Smart Access Management solution is backed by Pitney Bowes Standards. The application is developed using the Agile framework. The code is written to the NIST 800-218 Secure Coding Standard. Vulnerabilities are detected and security validated with Static Application Security Testing (SAST) scans, Dynamic Application Security Testing (DAST), and 3rd party library scans. Remediation is required before the code can be deployed. Additionally, vulnerability scans occur on the solution infrastructure, operating system, and container layers with remediation and CIS Level 1 compliance occurring both prior to and after deployment. Pitney Bowes runs intrusion detection and blocks exploit attempts at the firewall, infrastructure, operating system, and container layers.

The security framework is derived from the NIST 800-53 Rev 5 standard. Data security is based upon a rigorous analysis and backed by the FIPS-199 Data Categorisation process. Additionally, Pitney Bowes employs industry standard Privacy Impact Analysis (PIA) to back a robust, standards-based security posture in order to secure the product.

b. Data and processing residency

For customers in the UK, data is located and processed in the AWS London region. For customers in Australia, data is located and processed in the AWS Sydney region. Pitney Bowes leverages MongoDB Atlas which has also been provisioned in London and Sydney respectively.

c. Encryption across the platform

Data in transit and at rest is always encrypted. Pitney Bowes does not terminate TLS at the first load balancer but rather continues with encryption leveraging TLS 1.2 at all processing stages including within Kubernetes and between the processing logic and data stores. Further, Pitney Bowes leverages AWS FIPS 140-2 validated endpoints wherever available.

Data at rest is encrypted using AWS KMS which is FIPS level 2 certified.

4. User Access (customer)

Access to Pitney Bowes Smart Access Management is based on a shared responsibility model. Clients may opt to use Pitney Bowes provided logins or may integrate to their company Active Directory and provide SAML 2 tokens. Integration to a client Active Directory provides ease of management of user life cycle as staff turnover will be handled seamlessly through the client platform.

If a client chooses to leverage Pitney Bowes for authentication, they must adhere to the following password policy:

- **Password Length:** 8 characters
- **Password complexity:** 1 upper case, 1 digit or special character
- **MFA (via email or app):** enabled at client request
- **Login Attempts:** 6 attempts
- **Inactivity auto-logout:** 1 hour

5. Administrator Access to the portal (pb)

Pitney Bowes Smart Access Management sits on the Shipping 360® software platform. Please refer to our Shipping 360 white paper for more information.

Pitney Bowes follows NIST 800-53 standards for gaining privileged access to the system. Pitney Bowes maintains strict segregation of duties in the approval cycle and follows the principles of least privilege in granting access rights to the platform.

All access requests are initiated as tickets with the requester's role, desired access, and justification. Once approved by the manager, the access request is reviewed by the Information Systems Security Manager who then grants, denies, or modifies the access request. Pitney Bowes conducts quarterly access reviews for all privileged users.

Pitney Bowes maintains a strict segregation of duties amongst privileged users. The roles and rules are available on a need to know basis to external parties, so please contact your sales rep should you require detailed information in this area.

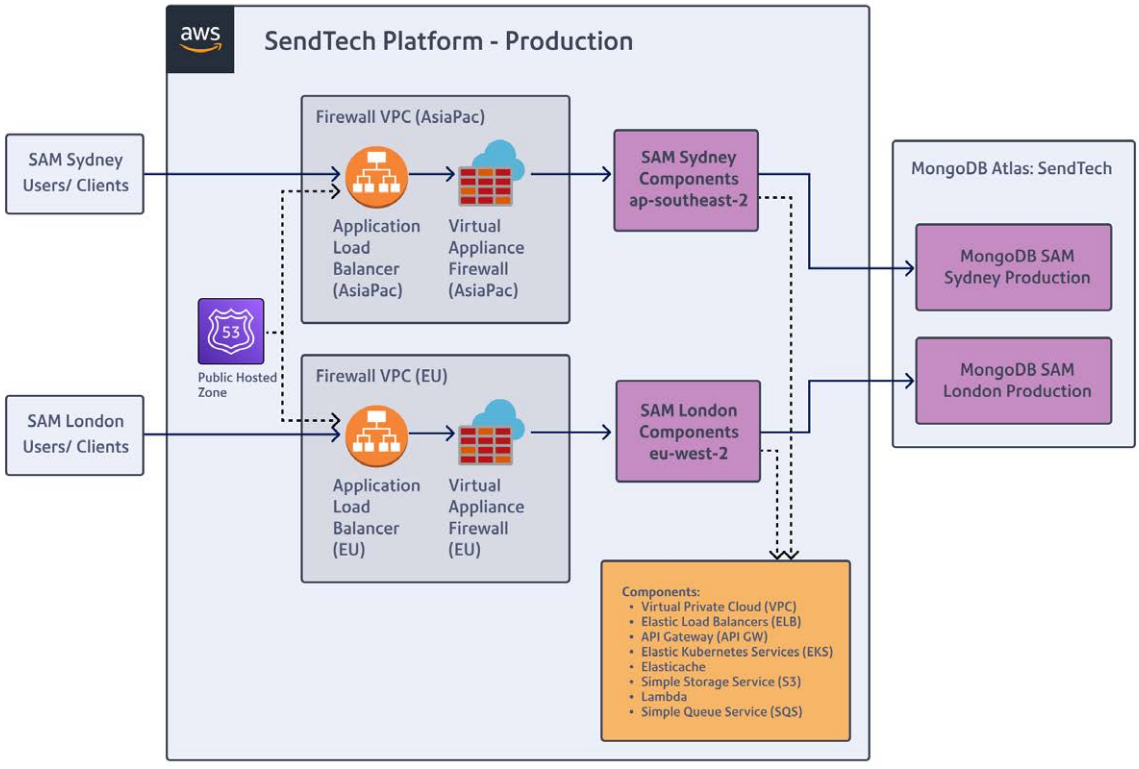
Once privileged access is granted certain immutable roles are enforced. All access requires MFA. Privileged users are logged out after 15 minutes of inactivity. Access to data and backups is strictly segregated.

a. Supply Chain Integrity (policy and practical procedure)

1. Adhere to NIST 800-153 Rev 5 controls on our supply chain

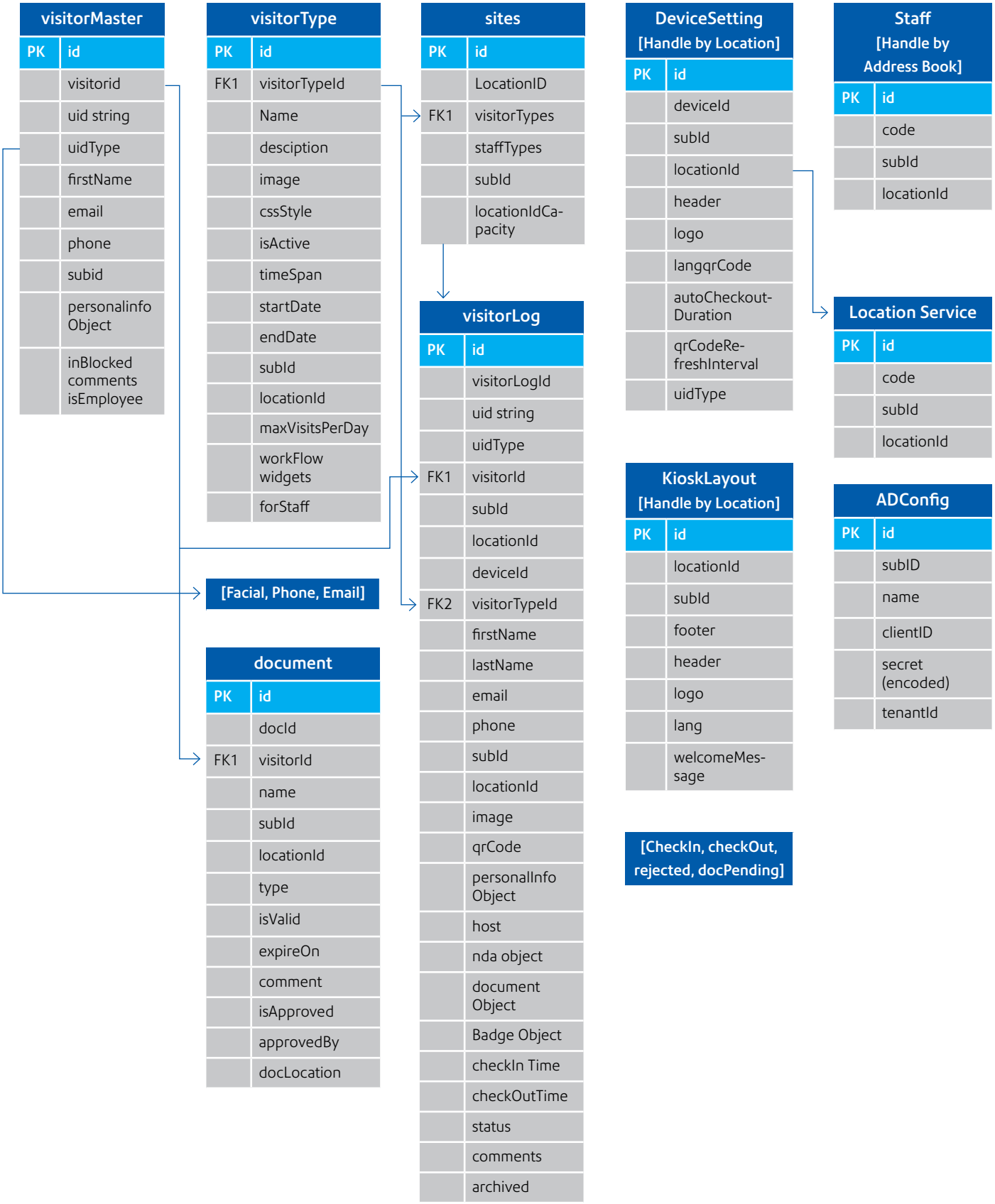
6. Technical Architecture

a. High-level Deployment



6. Technical Architecture

b. Data Architecture



6. Technical Architecture

c. Data Retention

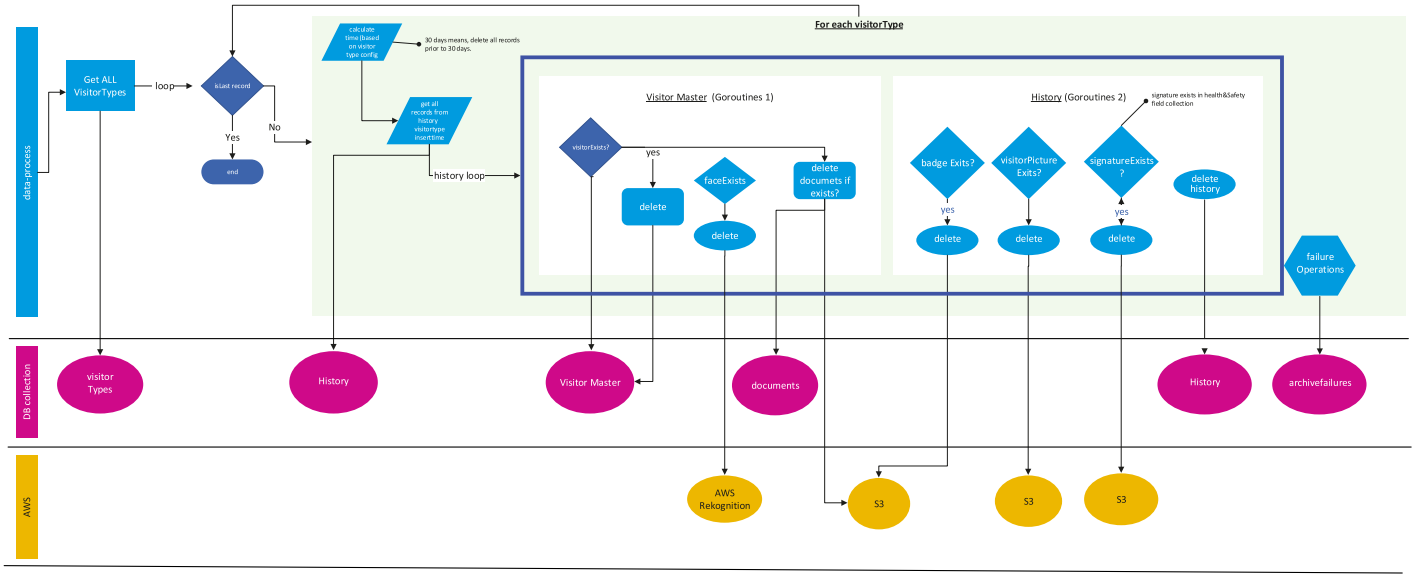
How long is data and documentation stored for?

This is up to you based on your company data privacy policies. Data purging can be configured within workflows. Different data retention periods can be set for staff and visitors.

Data retention periods can be set from 1 day, 7 days, 14 days, 30 days, 90 days, 180 days, 270 days, 1 year, and 2 years – as a default the period will be selected as - 90 days. Daily runs will occur at 12 a.m. to remove all data in accordance with the specified data retention periods.

On termination of your use of the service, unless a shorter period has been selected by you, all data and documentation will be deleted 30 days after the effective date of termination, after which, we shall have no obligation to maintain or provide any of your data and will, unless legally prohibited, delete all your data and documentation in our possession.

Data Retention Workflow



United Kingdom
Langlands House
130 Sandringham Avenue
Harlow
CM19 5QA
pitneybowes.com/uk

Australia
Level 1, 68 Waterloo Road
Macquarie Park NSW 2113
pitneybowes.com/au

New Zealand
Building B, Unit 2 & 3
72 Apollo Drive
Rosedale
Auckland 0632
pitneybowes.com/nz

India
Unit No 015
Ground floor
Time Tower Building
M G Road Gurgaon
Haryana – 122002
pitneybowes.com/in

Brazil
Alameda Tocantis, 630 – Alphaville –
Galpão 3
Barueri - SP - CEP 06455-020
pitneybowes.com/br