BOXPILOT | MARKETING PARTNERS

TECHNOLOGY POLICY - REVIEWED AND UPDATED 2024-03-01

JM Growth Partners, LLC O/A Boxpilot ("Boxpilot") has enacted this policy effective September 1, 2018 to protect the security and integrity of Boxpilot's Data and Information, as well as the Data and Information belonging to our Clients and/or Partners ("Clients"). It shall be reviewed, and updated, at minimum, annually on the anniversary date of its enactment.

1) Devices / Infrastructure

Boxpilot grants its employees and/or contractors ("Staff") the privilege of purchasing and using smartphones, tablets and computers ("Staff Devices") of their choosing at work for their convenience. Boxpilot reserves the right to revoke this privilege if Staff do not abide by the policies and procedures outlined below.

On accepting work with Boxpilot, Staff must agree to the terms and conditions set forth in this policy in order to be able to utilize Staff Devices to complete any Boxpilot work effort.

Acceptable Use

- Boxpilot defines acceptable business use as activities that directly or indirectly support the business of Boxpilot.
- Boxpilot defines acceptable personal use on Boxpilot company time as reasonable and limited personal communication or recreation, such as reading, game playing, online shopping, etc. If Staff are unsure if an activity is deemed acceptable, they should check with Boxpilot management.
- Staff Devices may not be used at any time to:
    - Store, transmit or access illicit materials/websites/data/resources.
    - Store or transmit proprietary information belonging to another company.
    - Harass others implicitly or explicitly through direct or indirect communication.
- All Boxpilot applications are cloud-based, and Staff may use Staff Devices to access all Boxpilot resources that are required in their role, as defined solely by Boxpilot.
- Boxpilot has a zero-tolerance policy for texting or emailing while driving and only hands-free talking while driving is permitted.
- Apps related to Boxpilot company usage are limited to email apps (e.g. Apple Mail, Gmail, Outlook, etc.), Meeting Apps (e.g. Zoom, WebEx, GoToMeeting, etc.), Cloud Storage (e.g. Google Drive, Sharefile, Box, Dropbox, etc.), Contact management (e.g. Hubspot, BrightPattern, etc.) and telephony (including Boxpilot company phone system through Zoom app).
- Boxpilot-related Data or Information ("Boxpilot Data") shall never be stored locally on Staff's personal devices. This Data or Information must be stored in Boxpilot's Google Drive account only.
- Data or Information belonging to, or related to any Boxpilot Client or Partner ("Client Data") shall never be stored locally on Staff's personal devices. Client Data must be stored either in Boxpilot's Sharefile account or a Client or Partner's preferred secure Cloud Storage account.
- "Rooted" (Android) or "Jailbroken" (iOS) devices are strictly forbidden from accessing any Boxpilot technology resources.

Devices and Support

- Smartphones including iPhone, and Android phones are allowed.
- Tablets including iPad and Android are allowed.
- Application connectivity issues are supported by Boxpilot; Staff should contact their respective manager for assistance and resolution.
- General network connectivity issues are not supported by Boxpilot; Staff should contact their respective service provider to determine the cause of any problems.
- Hardware issues are not supported by Boxpilot; Staff should contact the device manufacturer or their carrier for operating system or hardware-related issues.

Reimbursement

- Boxpilot will not reimburse Staff for a percentage of the cost of the device.
- Boxpilot will not reimburse Staff for the following charges: Home Internet Service, Mobile Phone Service, roaming, plan overages, etc.

Security

- In order to prevent unauthorized access, devices must be password protected using the features of the device and a strong password is required to access Boxpilot resources.
- All Boxpilot business applications are cloud-based, and will have their own specific passwords required for access. All passwords for all relevant applications must be different from any of the others.
- Boxpilot's strong password policy is: At least 12 characters, At least one upper-case letter, At least one lower-case letter; At least one number; At least one special character; Passwords must be changed every 180 days; Passwords may not be reused in the same calendar year; Passwords may not be reused between services; 5 failed attempts locks account.
- Staff access to Boxpilot and/or Client Data and Information is limited based on user profiles defined by Boxpilot and automatically enforced.
- For any Application where Two-Factor Authentication ("2FA") is available, Boxpilot will enforce the use of such added security for all Staff.
- Boxpilot Data and/or Client Data cached on Staff device(s) may be remotely wiped if 1) the device is lost, 2) Staff terminate their contract, 3) Boxpilot identifies a data or policy breach.
- In the event of a data or policy breach Boxpilot will notify any affected Staff and/or Clients within one business day by email and within two business days by phone.

Risks/Liabilities/Disclaimers

- While Boxpilot will take every precaution to prevent Staff's personal data from being lost in the event it must Remote Wipe a device, it is Staff's responsibility to take additional precautions, such as backing up personal data and information.
- Lost or stolen devices must be reported to Boxpilot within 24 hours. Staff are responsible for notifying their mobile carrier immediately upon loss of a device.
- Staff are expected to use their devices ethically at all times and adhere to Boxpilot's acceptable use policy as outlined above.
- Staff are personally liable for all costs associated with their device.
- Staff assume full liability for risks including, but not limited to, the partial or complete loss of Boxpilot and/or personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.
- Boxpilot reserves the right to take appropriate disciplinary action against Staff, up to and including termination, for noncompliance with this policy.
- Boxpilot reserves the right to pursue appropriate legal action against Staff, in the most extreme cases of noncompliance with this policy.

2) Vendors / Data Processors

Boxpilot selects Vendors and Data Processors who meet or exceed Data Security requirements of all Boxpilot Data and Client Data.

The following is a list of Vendors and Data Processors who have contact with Boxpilot Data and/or Client Data with links to their respective Privacy and Security information:

Contact/Company Data:

- Hubspot (CRM) - https://legal.hubspot.com/security
- BrightPattern (Contact Center Software) - https://www.brightpattern.com/security/
- Twilio (SMS/Telephony) - https://www.twilio.com/security
- Sendgrid (Email) - https://sendgrid.com/policies/security/

Data Storage:

- Google Drive - https://safety.google/security/

Communications:

- Google Mail (Email) - https://safety.google/security/
- Google Meet (Meetings) - https://support.google.com/meet/answer/9852160?hl=en
- Spoke Phone (Business Phone) - https://spokephone.com/terms/privacy/

3) Additional Information

Please review additional information, and/or contact the individual noted below with any questions or comments.

- Boxpilot Website - https://boxpilotmarketing.com/
- Boxpilot Trust & Privacy Policy - https://www.boxpilotmarketing.com/trust/
- Boxpilot Terms of Engagement - https://www.boxpilotmarketing.com/terms/

Key Technology Contact:
Kirko Papajanis
President
Direct (US) - +1-704-275-0231
Direct (Canada) - +1-416-341-7017
Email: kirko@boxpilotmarketing.com