PRIVACY STATEMENT

Your privacy is important to us. We are committed to respecting your privacy and the confidentiality of your personal information. This privacy statement outlines our information practices and the options you have for the way your personal information is collected, used, and disclosed. This statement applies only to information collected on this Web site.

The information we collect is only used to communicate with our users and is never shared with other organizations for commercial purposes. We do not collect cookies on this Web site.

Personal Information Privacy

We require information from the user if they select to:

- receive our newsletter
- request informational materials
- participate in surveys or evaluations
- enter promotions or contests
- submit comments or questions

In these instances we will collect user information such as name, physical address, telephone number, and e-mail address.

Third Parties

TBoxCloud will not sell or rent personal information without your consent. TBoxCloud has limited relationships with third parties to assist in servicing you. These service providers are contractually required to maintain the confidentiality of the information TBoxCloud provides.

Legal Disclosures

TBoxCloud reserves the right to analyze personal information on an individual basis to address problems with the services and to disclose personal information as required by United States Federal, state and local law, regulation or court order. TBoxCloud may be required to disclose personal information to cooperate with regulators or law enforcement authorities, to comply with a legal process such as a court order, subpoena, search warrant, or a law enforcement request.

E-Mail

We may send you email in response to questions you have submitted. We will provide you with the opportunity to opt-out of our communications at any time.

Community Content

TBoxCloud's may provide Chatrooms, Forums, Wikis, and Blogs on its website. Any information posted in these areas becomes public information, so users should exercise caution in publishing any personal information. TBoxCloud also reserves the right to remove any posting for any reason whatsoever, including any comment deemed vulgar, unsafe, or inappropriate.

Changes to this Privacy Statement

TBoxCloud reserves the right to change this policy from time to time. Any revised Privacy Policy will be posted on our website. A notice will be posted on our homepage for 30 days whenever this privacy statement is changed in a material way.

SECURITY & COMPLIANCE

As most global leaders in the industry provide secured solutions by relying on best-of-breed technology and standards, TBoxCloud relies on the same best-of-breed technology and standards directly or through partner solutions providing its customers with the most advanced, scalable, and secured solutions available on the market today.

SAS 70 Type II

SOC 1

SSAE 16

ISAE 3402

The audit for this report is conducted in accordance with the Statement on Standards for Attestation Engagements No. 16 (SSAE 16) and the International Standards for Assurance Engagements No. 3402 (ISAE 3402) professional standards. This dual-standard report can meet a broad range of auditing requirements for U.S. and international auditing bodies. The SOC 1 report audit attests that the control objectives are appropriately designed and that the individual controls defined to safeguard customer data are operating effectively. This audit is the replacement of the Statement on Auditing Standards No. 70 (SAS 70) Type II report.

SOC 2

In addition to the SOC 1 report, this is the Service Organization Controls 2 (SOC 2), Type 2 report. Similar to the SOC 1 in the evaluation of controls, the SOC 2 report is an attestation report that expands the evaluation of controls to the criteria set forth by the American Institute of Certified Public Accountants (AICPA) Trust Services Principles. **These principles define leading practice controls relevant to security, availability, processing integrity, confidentiality, and privacy applicable to service organizations such as TBoxCloud**. The SOC 2 is an evaluation of the design and operating effectiveness of controls that meet the criteria for the security principle set forth in the AICPA's Trust Services Principles criteria. This report provides additional transparency into our security based on a pre-defined industry standard of leading practices and further demonstrates our commitment to protecting customer data.

FISMA Moderate (Federal Information Security Management Act)

We enables U.S. government agency customers to achieve and sustain compliance with the Federal Information Security Management Act (FISMA). FISMA requires federal agencies to develop, document, and implement an information security system for its data and infrastructure based on the National Institute of Standards and Technology Special Publication 800-53, Revision 3 standard. FISMA Moderate Authorization and Accreditation requires to implement and operate an extensive set of security configurations and controls. This includes documenting the management, operational, and technical processes used to secure the physical and virtual infrastructure, as well as the third-party audit of the established processes and controls. The services has received a three-year FISMA Moderate authorization for Infrastructure as a Service from the General Services Administration. The services have achieved other ATOs at the FISMA Moderate level by working with government agencies to certify their applications and workloads.

PCI DSS Level 1

Financial institutions require that any company that stores, processes or transmits credit card information complies with the PCI-DSS (Payment Card Industry, Data Security Standards).

Ensuring your POS system and wireless infrastructure are in compliance is crucial.

The objective of the Payment Card Industry (PCI) Security Standards is to protect cardholder data. The standards are developed and published by the PCI Security Standards Council (SSC), which consists of hundreds of industry participants who have a vested interested in reducing vulnerabilities in the card-processing ecosystem.

Our services have achieved Level 1 PCI compliance and our services are aligned with a Level 1 service provider under the Payment Card Industry (PCI) Data Security Standard (DSS). Merchants and other service providers can now run their applications on our PCI-compliant technology infrastructure for storing, processing, and transmitting credit card information in the cloud. Other enterprises can also benefit by running their applications on other PCI-compliant technology infrastructure. PCI validated services include TBoxCloud Cloud Hosted Servers, TBoxCloud Cloud Storage, TBoxCloud Cloud Virtual Private Cloud, TBoxCloud Cloud Relational Database Service, TBoxCloud Cloud Load Balancing, TBoxCloud Cloud Identity and Access Management, and the underlying physical infrastructure and the TBoxCloud Cloud Management Environment.

ISO 27001

ISO/IEC 27001:2005 Certified
& Registered Organisation (Nº 2012-001)

Our service has achieved ISO 27001 certification of the Information Security Management System (ISMS) covering our infrastructure, data centers, and services including TBoxCloud Cloud Hosted Servers, TBoxCloud Cloud Storage and TBoxCloud Cloud Virtual Private Cloud. ISO 27001/27002 is a widely-adopted global security standard that sets out requirements and best practices for a systematic approach to managing company and customer information that's based on periodic risk assessments. In order to achieve the certification, a company must show it has a systematic and ongoing approach to managing information security risks that affect the confidentiality, integrity, and availability of company and customer information. This certification reinforces the commitment to providing transparency into the security controls and practices provided. The ISO 27001 certification includes all TBoxCloud Cloud data centers in all regions worldwide, and a formal program to maintain the certification is effectively in place.

INTERNATIONAL TRAFFIC IN ARMS COMPLIANCE

The TBoxCloud Government Cloud (US) region supports US International Traffic in Arms Regulations (ITAR) compliance. As a part of managing a comprehensive ITAR compliance program, companies subject to ITAR export regulations must control unintended exports by restricting access to protected data to US Persons and restricting physical location of that data to US land. TBoxCloud Government Cloud (US) provides an environment physically located in the US and where access by Personnel is limited to US Persons, thereby allowing qualified companies to transmit, process, and store protected articles and data under ITAR. The TBoxCloud Government Cloud (US) environment has been audited by an independent third party to validate the proper controls are in place to support customer export compliance programs for this requirement.

FIPS 140-2

The Federal Information Processing Standard (FIPS) Publication 140-2 is a US government security standard that specifies the security requirements for cryptographic modules protecting sensitive information. To support customers with FIPS 140-2 requirements, the TBoxCloud Virtual Private Cloud VPN endpoints and SSL terminations in TBoxCloud Government Cloud (US) operate using FIPS 140-2 validated hardware. We work with TBoxCloud Government Cloud (US) customers to provide the information they need to help manage compliance when using the TBoxCloud Government Cloud (US) environment.

HIPAA

Customers have built healthcare applications compliant with HIPAA's Security and Privacy Rules. TBoxCloud infrastructure provides the security controls customers can use to help secure electronic health records.

CSA

Our services conform to the Cloud Security Alliance (CSA) Consensus Assessments Initiative Questionnaire. This questionnaire published by the CSA provides a way to reference and document what security controls exist in TBoxCloud Infrastructure as a Service offerings. The questionnaire (CAIQ) provides a set of over 140 questions a Cloud consumer and Cloud auditor may wish to ask of a Cloud provider.

MPAA

The Motion Picture Association of America (MPAA) has established a set of best practices for securely storing, processing and delivering protected media and content. Media companies use these best practices as a way to assess risk and audit their content and infrastructure. An independent assessment was conducted for compliance with the MPAA best practices, and achieved the highest maturity rating possible, indicating that the TBoxCloud infrastructure is compliant with all applicable MPAA infrastructure controls across all the TBoxCloud services under review. While the MPAA does not offer a "certification", media companies can use this report to complete their own risk assessment and audit of MPAA-type content on TBoxCloud hosted services.

DIGICERT

SSL Certificate Encryption & Authentication

Strong 2048-Bit SSL Certificate Encryption

SSL Certificates from DigiCert provide the strongest 2048-bit and SHA-2 encryption available. TBoxCloud uses digiCert WildCard Plus SSL to further protect its sub-domains, integration connection points, and data transport.

Additional Questions

If you have additional questions that are not addressed above, please review our legal section at www.tboxcloud.com/legal or contact our legal department at legal@tboxcloud.com.