Data Encryption Policy

# 1.0 Overview

This policy addresses encryption policy and controls for confidential other sensitive data that is at rest (including portable devices and removable media), data in motion (transmission security), and encryption key standards and management.

# 2.0 Purpose

The purpose of this policy is to provide guidance to 7 Bridges Marketing, LLC’s employees and affiliates on the use of encryption to protect information resources that contain, process, or transmit confidential and sensitive information. Additionally, this policy provides direction to ensure that a foundation is available for meeting the information security standards established by 7 Bridges Marketing, LLC’s customers.

# 3.0 Scope

This policy applies to all 7 Bridges Marketing, LLC. employees and affiliates, including vendors, contractors as well as customers. This policy also applies to all equipment that is owned or leased by 7 Bridges Marketing, LLC, as well as all equipment that communicate electronically with 7 Bridges Marketing, LLC’s equipments.

# 4.0 Policy

# 4.1 Encryption Strength

* All encryption mechanisms implemented to comply with this policy must support a minimum of, but not limited to the industry standard, AES 128-bit encryption.
* The use of proprietary encryption algorithms are not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by 7 Bridges Marketing, LLC’s IT management team.

#### 4.2 Data at Rest

* Confidential sensitive data at rest on computer systems owned by and located within 7 Bridges Marketing, LLC controlled spaces and networks should be protected by at least one of the following:
  + Encryption
  + Firewalls with strict access controls that authenticate the identity of individuals accessing the data
  + Other compensating control such as complex password
* Password protection should be used in combination with all controls including encryption.

Note: hard drives that are not fully encrypted, e.g., have encrypted partitions, virtual disks, or are unencrypted, but connect to encrypted USB devices may be vulnerable to information spillage from the encrypted region into the unencrypted region. The hard drive’s unencrypted auto-recovery folder may retain files that have been saved to the encrypted portion of the disk or USB. Full disk encryption avoids this problem.

#### 4.3 Portable Devices

Portable devices represent a specific category of devices that contain data-at-rest. Many incidents involving unauthorized exposure of confidential data are the result of stolen or lost Portable Computing Devices. The best way to prevent these exposures is to avoid storing confidential data on these devices. As a general practice, confidential or sensitive data should not to be copied to or stored on a portable computing device. However, in situations that require confidential or sensitive data to be stored on such devices, encryption and password protection must be used to reduce the risk of unauthorized disclosure in the event that the device becomes lost or stolen.

Confidential or sensitive information stored on portable devices including laptops, personal digital assistants(PDAs) must be encrypted using products and/or methods in accordance with 7 Bridges Marketing, LLC’s Data Encryption Policy.

Portable devices including laptops, personal digital assistants(PDAs) should not be used for the long-term storage of any Confidential or sensitive information.

Portable devices including laptops, personal digital assistants(PDAs) that store or transmit confidential or sensitive information must have the proper protection mechanisms installed, including antivirus and/or firewall software, with unneeded services and ports turned off and subject to needed applications being properly configured.

Removable media including CD-ROMs, floppy disks, backup tapes, external hard drives and USB memory drives that contain confidential or sensitive information must be:

* + encrypted and stored in a secure, locked location.
  + transported using in a secure manner
  + in the possession of the authorized user at all times (e.g., must not be checked as luggage while in transit).

Data owners and users of portable computing devices and non-7 Bridges Marketing, LLC owned computing devices containing confidential and sensitive data must acknowledge how they will ensure that data are encrypted and how encrypted data will be accessible by the owner in the event that an encryption key becomes lost or forgotten. Methods to meet this requirement include, but not limited to, the following.

* Maintaining an accessible copy of the data on a server managed by 7 Bridges Marketing, LLC.
* Use of whole-disk encryption technologies that provide an authorized systems administrator access to the data in the event of a forgotten key.
* Escrowing the encryption key with a trusted party designated by the data owner and 7 Bridges Marketing, LLC’s IT management

#### 4.4 Transmission Security

Users will follow 7 Bridges Marketing LLC’s Acceptable Use Policy when transmitting data and must take particular care when transmitting or re-transmitting Confidential or sensitive data (e.g., citizen personal identification information) received from business partners, affiliates or clients.

* Confidential or sensitive information transmitted as an email message must be encrypted.
* Any confidential or sensitive information transmitted through a public network (e.g., Internet) to and from vendors, customers, or entities doing business with 7 Bridges Marketing, LLC must be encrypted or be transmitted through a tunnel that is encrypted with virtual private networks (VPN) or secure socket layers (SSL).
* Transmitting unencrypted confidential or sensitive information through the use of web email programs is prohibited.
* Transmission of data files through any Instant Messaging (IM) or online peer-to-peer (P2P) file sharing programs is prohibited.
* Wireless (Wi-Fi) transmissions that are used to access 7 Bridges Marketing, LLC owned portable computing devices or internal networks must be encrypted using the IEEE 802.11i (WPA2) or better.
* Encryption is required when users access confidential or sensitive data remotely from a shared network.
* 7 Bridges Marketing, LLC. permits the secure encrypted transfer of documents and data over the Internet using file transfer programs such as “secured FTP” (FTP over SSH). Only authorized 7 Bridges Marketing, LLC. users can initiate secure FTP transactions and will use the following procedures:
* To use the transmitting server securely, each authorized user must have a logon ID and password with a designated directory. Users should not have access to shared directories unless required for business reasons. Anonymous FTP is not permitted.
* All accounts and keys must be managed by 7 Bridges Marketing, LLC.’s IT personnel from within 7 Bridges Marketing, LLC’s corporate network.
* All files contained within an account’s directory must be deleted a maximum of seven days after they are made available for retrieval.
* All transactions and transfers must be logged, and reviewed for prohibited activity.
* Plain FTP does not provide encrypted transmission and should not be used on any Internet-facing systems or where confidential data is being transmitted.

#### 4.5 Encryption Key Management

Effective key management is the crucial element for ensuring the security of any encryption system. Key management procedures must ensure that authorized users can access and decrypt all encrypted data using controls that meet operational needs and comply with data retention requirements..

7 Bridges Marketing, LLC’s key management processes and systems are characterized by the following security precautions:

* 7 Bridges Marketing LLC uses procedural controls to enforce security and availability of encryption keys so that they are protected when in storage and can be made available when needed. These controls apply to persons involved in encryption key management or who have access to security-relevant encryption key facilities and processes, including IT personnel and/or contractor personnel. 7 Bridges Marketing, LLC will verify backup storage for Key passwords, Files, and related backup configuration data to avoid single point of failure and ensure access to encrypted data.
* To ensure separation of duties and two person control, no single individual is authorized to generate a new CA key pair.
* Background checks and clearance procedures in place for the personnel involved with confidential and sensitive data as well as encryption keys.
* Complete regular training on key management requirements and procedures
* Encryption Keys shall be stored on primary and backup media protected with password and labeled appropriately. The on premise copy shall be stored under lock and key in a fire-proof cabinet under the jurisdiction of authorized personnel from Information Technology Dept. The off-site backup copy shall be escrowed, in addition to all other procedures described in this document.
* Specific personnel shall be authorized to recover the keys from the escrow company, who will require a minimum of two signatures on the authorization for recovery of the keys.
* Sanctions against personnel for unauthorized actions, unauthorized use of authority, and unauthorized use of 7 Bridges Marketing, LLC systems, resulting in written reprimand or dismissal.
* Written acknowledgement of receipt of this policy from each individual involved in key management.
* Private keys must be kept confidential
* Keys must be randomly chosen from the entire key space, using hardware-based randomization.
* Key-encrypting keys are separate from data keys. No data ever appears in clear text that was encrypted using a key-encrypting key, e.g., a key-encrypting-key is used to encrypt other keys, securing them from disclosure.

Keys that are transmitted are sent securely to well-authenticated parties.

# 5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.