

## **Policies that Address Information Security for Contractors and Service Providers**

- 1.0 A list of Service Providers must be maintained. This list will be updated and reviewed by senior management when necessary but at least every 180 days.
- 2.0 A written Agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service provider possess is required from each service provider.
- 3.0 Due diligence is to be performed prior to the engagement of Service Providers. Procedures performed will include when possible:
  - A visit to the Service Providers physical offices to discuss security practices and procedure with their management and staff.
  - A written statement acknowledging their responsibilities to securely process, handle and transmit cardholder data.
  - Written proof that the Service Provider is PCI compliant.
  - Request reliable industry references.
- 4.0 A program is to be maintained to monitor Service Providers' PCI DSS compliance status. On an annual basis a request for a new compliance certificate will be requested.

---

### **Senior Management Approval:**

Printed

Name: **Sandra E. Haven**

Signature:

  
\_\_\_\_\_

Title: **Owner, Bristol Services Intl.**

Date: **1/12/2016**

### **Revision History**