Bristol Service Intl.

Information Security Policy

Overview
This policy is intended to relay the importance of security and protecting cardholder data.

Purpose

- To establish the Bristol Service Intl.'s policy for the secure handling of sensitive card holder data including but not limited to magnetic strip data, Cardholder name, Primary Account Numbers (PAN's), expiration date, and service code
- To establish the policies and procedures to manage the relationship(s) with Service Providers.

Scope
This policy applies to all employees and systems of Bristol Service Intl.

Policies to Restrict Physical Access to Cardholder Data

The importance of protecting cardholder data is paramount. Allowing data theft or destruction, inadvertently sharing confidential information, infecting system networks with viruses, misuse of company resources, allowing the theft of company property, and allowing the compromise of private or confidential company or client information are all very real examples of what might result from a security compromise.

1.0 All paper that contains cardholder data is to be identified and physically secured in a locked drawer. No electronic cardholder data will ever be stored.

2.0 Strict control is to be maintained over the internal or external distribution of any kind of media that contains cardholder data

- Media is classified and clearly marked as confidential
- Media is sent by secured courier or other delivery method that can be accurately tracked

3.0 Management approval is to be obtained prior to moving any and all media containing cardholder data from a secured area.

4.0 Strict control must be maintained over the storage and accessibility of media that contains cardholder data. Only senior management, or their designators, will have access to media containing cardholder data.

5.0 Media containing cardholder data is to be destroyed when it is no longer needed for business or legal reasons.

- Paper materials are to be shredded, incinerated, or pulped so that cardholder data cannot be reconstructed.
- The general rule is that media containing cardholder date will be destroyed when over 180 days old. Exceptions to the rule must be approved by senior management.