Area: Finance

Policy Name: Information Security

Policy Statement: To ensure the safety and protection of cardholder data, Salina Tech will adhere to secure handling of sensitive cardholder data including but not limited to magnetic strip data, Cardholder name, Primary Account Numbers, expiration date, and service code.

Procedures: 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.

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

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

Strict control must be maintained over the storage and accessibility of media that contains cardholder data. Only the Vice President of Administrative Services or approved designates will have access to media containing cardholder data.

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 data will be destroyed when over 180 days old. Exceptions to the rule must be approved by the Vice President of Administrative Services.

Contact: Vice President of Administrative Services

Related Form(s):

Adopted: September 22, 2014

Updated: