

Cardholder Data Security Policy

The following set of guidelines must be followed by every employee when working Cardholder Data (the full credit card number and expiration date):

1. Employees must treat Cardholder Data as highly confidential and exercise caution when working with this information.
2. Employees must label any material that contains Cardholder Data as “Confidential”.
3. Employees must shred all printouts that include Cardholder Data when finished working with them.
4. Employees must store all printouts that include Cardholder Data in a locked drawer or cabinet.
5. Employees are prohibited from removing any Cardholder Data from the premises in any format including verbal, printed, or electronic format or transmission (including email between locations).
6. Employees are prohibited from copying / storing any files that contain Cardholder Data to any portable data storage device (cd-rom, floppy disk, external hard drive, etc.).
7. If employees are required to electronically store Cardholder Data for authorized use, they must store it on the secured confidential data drive.
8. Employees must delete any stored Cardholder Data as soon as reasonably practical following any authorized use.
9. Employees are required to report any violations of the foregoing to their supervisor immediately.
10. Violations of any of the aforementioned policies may result in termination and / or prosecution under Federal and State laws.

I have read and understand the foregoing and agree to comply with this policy.

Employee Signature

Date

Employee Name (please print)