Parking Services
UNIVERSITY OF COLORADO **BOULDER**
www.colorado.edu/pts

Parking Services
1050 Regent Drive, UCB 502
Boulder, CO 80309
(303) 735-PARK (7275)

PS CREDIT CARD INFORMATION SECURITY POLICY

Effective Date:	March 1, 2025
Topic:	Credit Card Information Security Policy
Prepared by:	Tracy Humphrey, Asst Dir Finance
Approved by:	Tom McGann, Director, Parking Services (PS)
Applies to:	All PS employees

POLICY

1. It is the policy of this department to protect the security and confidentiality of all payment cardholder information, at all times, and in whatever forms such information is received. The security and confidentiality of cardholder information is the responsibility of every employee in this department, whether or not directly involved in processing payment transactions, and each employee is expected to be familiar with the methods used to protect cardholder information.

2. Access to credit card numbers is restricted to employees who need to know the credit card numbers for the conduct of PS business and will not be collected or retained for any other purpose.

3. Credit card payments may be received in person, over the phone, or through secured electronic means (web, parking meters, etc). PS discourages customers from sending credit card numbers via fax or through the mail. PS does not accept credit card numbers via email.

4. Credit card information received by PS for business purposes will not be sent via fax, email, conveyed via phone or removed from the office or written down while in the field (while working an event, for example).

5. It is prohibited to store or retain the full credit card number or cardholder track data in any electronic form whatsoever, including in spreadsheets, databases, word processing documents, emails, on websites, or by any other electronic means or in any electronic file. Cardholder track data will not be stored or retained from point-of-sale devices and/or manual recording (paper, etc.).

6. Credit card numbers received over the phone can be copied manually to a piece of paper. The word “confidential” will be displayed somewhere on this paper. If the credit card number is received by mail/fax, it must be marked as confidential. It is the responsibility of the employee who receives the information to keep the paper under their control, or secured in an authorized storage location. Once the credit card number is no longer needed to complete the transaction, the credit card number is to be shredded in a crosscut paper shredder.

7. Copies of the credit card number will not be made.

8. Credit card receipts will show only the last four digits of the credit card number on both customer and merchant copies.

9. All third parties, vendors, or contractors that handle cardholder information on behalf of PS will follow this policy in its entirety and are obligated and bound to protect the confidentiality and security of all such cardholder information they may have access to.

10. Employees, third parties, vendors and contractors with the potential of being exposed to sensitive cardholder information will be required to read and sign the PS Credit Card Information Security Policy. New PS employees will have thirty (30) days from the date of employment to read and sign the form.

11. PS will verify service providers’ PCI DSS compliance status once a year.

12. PS will conduct training for new employees responsible for handling credit card information during the onboarding process. PS employees are required to review all relevant credit card security policies/procedures and sign the PS Credit Card Information Security Policy on an annual basis.

13. The PS Director will ensure that this policy is reviewed at least annually and whenever PS business practices and procedures change. A current copy of this policy will be forwarded to the CU Treasurer’s Office whenever changes are made.