# University Parking System: Privacy Policy

for

Master of Science

Information Technology

Kassandra Vega Lucero

University of Denver College of Professional Studies

April 13, 2025

Faculty: Nathan Braun, MBA

Dean: Michael J. McGuire, MLS

Table of Contents

# Internal Policy

## Introduction

The University Parky System's internal policy outlines how the team should manage and protect sensitive data collected by the parking system as of April 13, 2025.  The policy aims to ensure regulation compliance, ethical data practices, and protection of user information.

## Application Overview

The University Parking System is a parking management system that assists in completing a variety of services such as customer registrations, car registrations, issuance of permits and customer IDs, tracking parking lot vacancies and transactions, maintaining a record of the accrued charges, as well as executing commands for registrations. This parking service application collects, stores, and processes sensitive customer data. This requires strict control over data access and privacy protections.

## Data Collection

The system can collect data, which is categorized into customer information, vehicle information, parking lot details, and logs for accrued charges and command execution. Customer information includes the customer's name, street address (primary and secondary), city, state, zip code, phone number, and the cars registered to the customer. Vehicle information includes the license plate number, the type of car (COMPACT or SUV), the permit ID  and its expiration, and the assigned owner of the vehicle. Parking lot details include the parking lot type, vehicle entry and exit times, and the parking lot statistics for vacancies and general usage. The parking lot charge accrual logs maintain information on the amounts charged, to whom they are charged, and from which parking lot. The command execution logs include data on the parameters users submit and the responses generated by the system-based parameter command execution.

## Privacy Implications

The data collected in the University Parking System poses several privacy implications. The initial privacy implication is Personally Identifiable Information (PII). The data with a PII impact includes the customer's name, address, and phone number. Other information can lead to identifying other customer details. Vehicle License plates can be linked to customers. The entry and exit time records and parking charges can allow others to infer their typical parking habits and patterns and the usual charges they accumulate when using the parking lots. The command logs can contain sensitive data passed as an entry or included in the generated responses.

## Data Access and Uses

All data is accessed, stored, and managed, and system and data access is restricted to reduce the risk of misusing it and ensure confidentiality. Parking Office employees have limited access to customer and vehicle details to complete daily operations, including issuing permits and creating customer profiles. System Administrators have full access to the system. Their access is used for auditing, troubleshooting, and monitoring compliance. Also, aiding system debugging, developers can access encoded data to test and perform maintenance. Auditors also access system logs during compliance auditing to ensure adherence to privacy regulations.

## Purpose of Data Collection

The data collected using the University Parking System enhances parking lot services. The parking management system improves the efficiency of parking lot management and customer service and aids in permit enforcement using customer and vehicle data. Data collected on parking lots and their charges are used to optimize the parking lot capacities and allocate the bills due for rendered services. That collection is used during debugging and maintenance to enhance the system's features and functionality.

## Data Security

The data collected is secured to prevent data being misused and accessed by unauthorized parties. Data encryption is used for data storing and while in transit. Encryption allows for only roles-based access to specific data types. Before allowing access to each role, the individuals will complete extensive training on data security. With restricted access to data, data is protected from unauthorized changes or loss during processing, storage, and during transit. All activity is logged for audits, and transaction charges are allocated to the proper individual for the parking services rendered. Logs and data are retained only for as long as needed, usually resulting in three months past their permit expiration or until the customer requests that the data is deleted, whichever comes first. In the scenario of unauthorized access to the data, especially those resulting in data misuse or data breaches, team members must report the incident immediately to administrators for prompt action.

## Conclusion

This internal policy is a guideline for employees and team members to ensure that the data collected in the University Parking System is used responsibly, securely, and ethically. Violating the policy will result in disciplinary action which can include legal repercussions.

# External Policy

## Introduction

The University values your business and your privacy. We are committed to protecting your personal information. Hence, this policy explains how we collect, use, and protect your data when you use our University Parking System. The policy is effective as of April 13, 2025, and by using our parking system, you agree to the data collection and privacy practices outlined below.

## Parking System Overview

This policy is for the parking system you have shown interest in using. The parking system is used by the University to manage parking lots through the issuance of permits for its customers. The system also records parking transactions with entries and exits as well as the charges accrued by using the parking lots.

## Data Collection

The University Parking System collects the following data types to provide our parking services to our community members. Your personal information is collected, including your name, street address (primary and secondary), city, state, zip code, and phone number. Along with personal data, data on your vehicle is also collected, including the license plate, the type of car, and permit information. Your parking lot usage data, such as the entry and exit times and their parking lot statistics, will also be collected. This data collection leads to the collection of the charges you accrue with dates and times.

## Your Rights for Data Collection

With data collection, you have the right to know what data we collect from you and why the data is collected. You may choose not to provide certain information; however, doing so can limit some of the features of the parking system, such as issuing permits and using the parking lots. You can also request that your data be deleted from our system by contacting the parking office administration office. The deletion of your data can invalidate your parking permit if it is required data for permit issuance.

## Accessing and Updating Your Data

You can access your data by visiting a parking office, logging in to the portal, or contacting the parking office administration office. To update your user data, you can also go into a parking office or log in to the parking system portal.

## Data Security

Due to the high value of your information and our desire to keep it safe, we have several security measures to ensure protection. Your data is encrypted both during the transmission and storage in the databases. Activity logs are maintained for all system activities to have a record of access and prevent unauthorized use. They are also used to support the auditing of logs. Only authorized personnel will have access to your sensitive data based on their roles and only after thorough training in the protection of user data. Discovering any unauthorized access is reported immediately to administrators for immediate action.

## Security Violations

In the unlikely event of a privacy breach, the administrative office's immediate action includes notifying affected users. Based on their indicated preference, affected users will be notified promptly via SMS or mail. The notification will include details on the breach, including what information is compromised and the date of the incident. Depending on the data compromised and the nature and impact of the breach, affected users may be entitled to compensation as laws allow.

## Third-Party Access

We understand your information is personal. We do not sell or share your personal data to third parties for marketing purposes. However, if we partner with third-party agents for system improvements or analytics, your data is encoded for animosity before sharing.

## Contacting Us

If you have any questions about this policy on data collection while using the University's Parking System or if you want to exercise your data collection rights, you may contact us via email at parkingadminoffice@university.edu, by phone at (123)555-1234, or by visiting us at the Parking Administration Office located at 1234 University Boulevard, Denver, CO 80204.

## Conclusion

This policy is designed to inform users of the University's Parking System by being transparent about how data is collected. It is also meant to ensure data security and respect your privacy. Thank you for your business and for trusting us with your information.