Introduction

April 7, 2023

Palmetto's Choice Diamond Commercial (PCDC) Airline is the Lowcountry's premier choice of airline for your travel destination. PCDC has options for everyone! For our elite customers we provide the most luxurious first-class seats that make you feel as if you are on a private flight. If you are looking for a more economical choice, we provide comfortable seating with plenty of coveted legroom. For all passengers, the in-flight entertainment options along with appetizing snack and meal choices on every flight will be sure to make all travelers believe they are already on vacation. PCDC Airline's customer service and attention to details are what makes tickets high in demand and fills every flight.

With every flight being sold out, PCDC strives to maintain an on-time flight schedule to keep customers happy and coming back. We pride ourselves in having minimal flight cancellations as well as an expedient check-in process since we know how valuable our customer's time is and want to get you from point A to point B as quickly as possible. We hope to see you on one of our flights soon and remember the sky's the limit when you fly with PCDC Airlines!

April 7, 2023

Blue Team,

Welcome to the Palmetto's Choice Diamond Commercial (PCDC) Airline team, where you will oversee the information technology department that maintains all the airline's online functions. Your team will be responsible for ensuring all on ticketing and check-in services are operational.

As new employees of PCDC's support team, each of you will complete various roles of system administrator duties ensuring continuous service to our clients 24/7. This includes the API interfaces, financial and customer databases, maintaining the flight schedule display, internal communication systems leveraged, and many other critical system production functions. The databases will possibly contain Personal Identifiable Information (PII) and customer's personal financial information that must be protected at all times.

Your team must ensure Confidentiality, Integrity, and Availability is maintained using secured, encrypted data transmission protocols, firewalls, VPN tunneling for remote desktop support, and professional communication to multiple clients as needed on a day to day basis.

As the risk of data breaches, ransomware, phishing, and denial of service attacks continue to grow, it is paramount the security of our infrastructure be of the utmost importance to preserve our ticket sales and flight schedule. PCDC has hired your team to ensure PCDC's databases are secured, company and client information is protected, and professional service is always provided. Unfortunately, the previous team abruptly vacated their positions, so we cannot guarantee the current state of any service or of the network diagram.

PCDC is confident your team will help our airline not only maintain but improve our excellent customer service record. We are excited to have you as part of our exceptional team!

Welcome to Palmetto's Choice Diamond Commercial (PCDC) Airline!

Regards,

Mr. Michael Scott
CEO

TABLE OF CONTENTS

LIST OF APPENDICES

1.0 ACCOUNT INFORMATION

1.1 Initial Password List

At the start of the day, your team will be provided with your initial username and password information for all assigned assets.

1.2 Password Changes

Changes of domain user accounts need to be reported to the Gold Team. Please submit password changes to the Gold Team Ticketing service to lessen service check downtime. Failure to promptly report changes to domain user accounts can negatively impact service checks from the competition scoring engine.

1.3 Email Access

Blue Teams will access their web-based email through the following web address: **http://mail.blueXX.pcdc.local** which is in scope. Any email from @pcdc.local is out of scope from the Red Team. Kelly Kapoor (Kelly.Kapoor@blueXX.pcdc.local) is the Help Desk Lead for PCDC Airlines, so she will be receiving various messages throughout the day.

2.0 NETWORK OVERVIEW

Your assigned network consists of virtual machines that are accessed via standard remote access protocols (RDP and SSH) from the assigned AWS Workspace. Usernames and passwords for all assets will be provided in the Initial Password List at the start of competition. An old network diagram was found and is located in Appendix A. Your network will consist of a mix of Windows and Linux operating systems.

2.1 Flight Schedule Display

The flight schedule is displayed using a Raspberry Pi. This device is subject to Red Team attacks and must be protected at all times.

2.2 Backups and Recovery

Teams do not have access to create backups of VMs, nor to recover a VM. Recovery requests can be submitted via a ticket to the Gold Team Help Desk. Select ***Request*** as the ticket category and use the following format:

SUBJECT: Recovery Request
BODY:
Team #: _____
Request: _____
Justification: _____

Please note that recovery comes with a **substantial cost** and reverts the machine to its initial operating condition.

2.3 Active Defense

While this term is still being defined in industry (some say it includes offensive capabilities and others say it does not). We are referring to Defending Forward – countering of preventing a perceived cyber-attack by taking the fight to your adversary with the goal of taking away their ability to perform offensive cyber operations against you. This is not permitted under any circumstances. Teams should keep their actions within their own assigned assets, unless explicitly permitted by Mr. Green, Chief Information Systems Officer (CISO).

2.4 Incident Reporting

Accurate incident reports that can be verified will net your team a modest number of points in the end-of-day team assessment. Incident reports must contain a description of how and what occurred (including source and destination IP addresses, timelines of activity, passwords cracked, access obtained, damage done, etc), a discussion of what was affected, and a remediation plan. Overly inaccurate Incident Reports, especially abuse of Incident Reports, will net no points and may result in a loss of points.

Written reports must be coherent and professional. Should you recognize that an incident has occurred, you may escalate an incident response report by submitting a ticket to the Gold Team Help Desk. Select ***Incident*** as the ticket category and use the following format:

SUBJECT: Incident Reporting
BODY:
Team #: _____
Time(s) of Incident: _____
Asset(s) Affected: _____
Source (IP Address) of Attack: _____
Description of Attack/Incident: _____
Remediation/Plan to Resolve: _____

2.5 Firewall Requests

The perimeter firewall will be managed by the PCDC, Inc Gold Team. All requests to modify the perimeter firewall must be submitted to the Gold Team via the Help Desk Ticketing system and by selecting the ticket category ***Request***.

2.6 Competition World Share

Files may be made available here for the teams to utilize throughout the competition including, but not limited to the initial default password list distribution.

The share can be accessed via \\share.pcdc.local\worldshare.

2.7 Out of Band Virtual Machine

The AWS Workspace is the out of band virtual machine denoted on the network diagram. It is fully out of scope from the Red Team.

2.8 Out of Band Email

Blue teams will be given a Stemrocks account that will be used for email, chat and Gold Team Help Desk access. This account is out of scope for the Red Team. This account will be used for inject distribution, submitting injects and access to the Gold Team Help Desk. The Stemrocks site can be reached at:

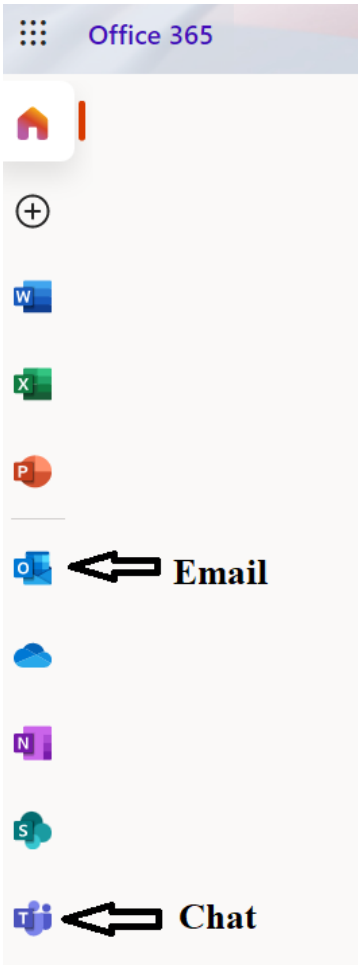
https://portal.office.com

Account format is:

HS-blueXX@stemrocks.org
COL-blueXX@stemrocks.org
PRO-blueXX@stemrocks.org

Passwords will be provided the day of competition.

Once logged in, select the Outlook application icon from the left side of the site for access to email. Select the Teams application icon for access to chat. Icons may not appear in the same order as displayed in this image.

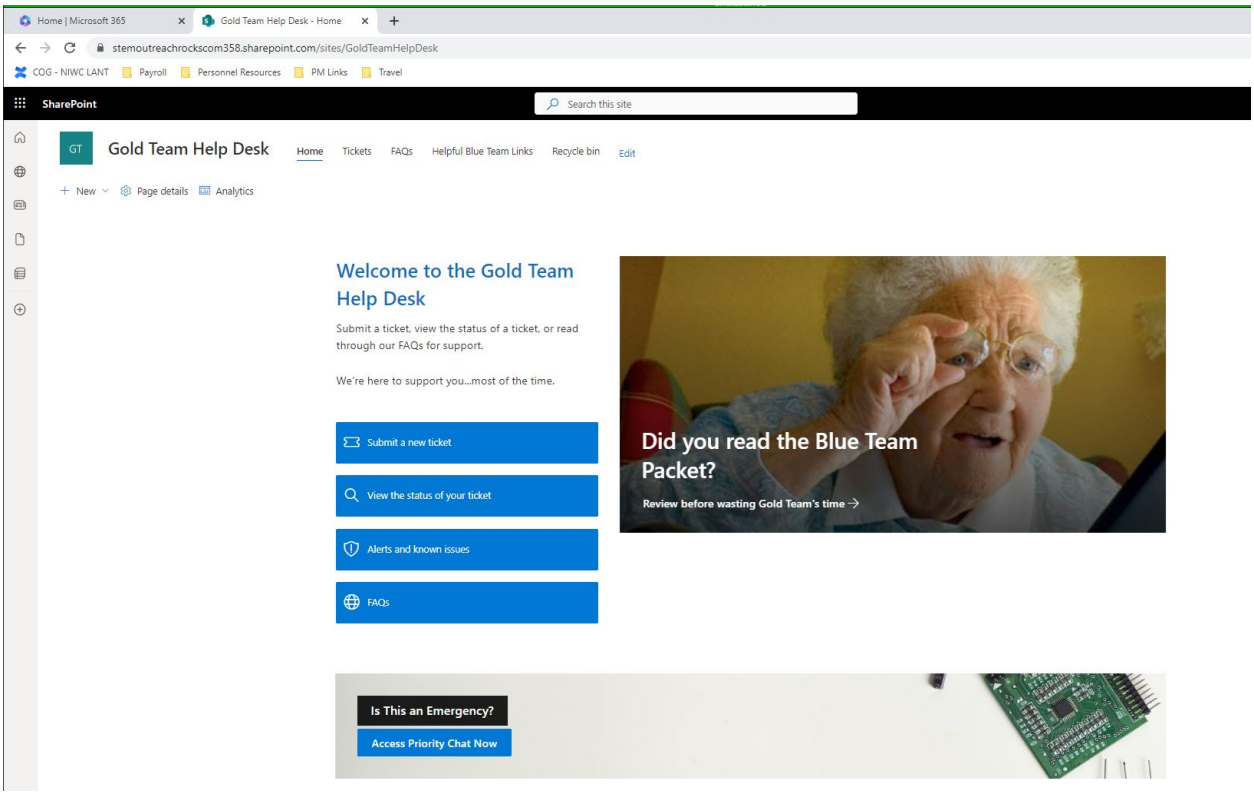


2.9 Gold Team Help Desk

There will be an online Help Desk system provided for teams to request assistance from the Gold Team. The Help Desk can be reached at:

https://stemoutreachrockscom358.sharepoint.com/sites/GoldTeamHelpDesk.

The Gold Team Help Desk will respond as soon as possible to your ticket. The Help Desk chat function will also be available to use as needed.



3.0 TEAM ASSESSMENT

Employee performance is assessed at the end of each day. A single score is given to each team of employees.

3.1 Scoring

Scoring is based on keeping required services up, controlling/preventing unauthorized access, completing business tasks, a.k.a. injects, from colleagues, supervisors, and other departments throughout the day, and continuing to provide critical business products/services. Teams accumulate points by successfully completing these injects and maintaining services. Teams lose points by violating service level agreements, usage of recovery services, and successful penetrations by hackers, a.k.a. the red team.

Any team action that interrupts the scoring system is exclusively the responsibility of that team and will result in a lower score. Any team member that modifies a competition system or system component, with or without intent, in order to mislead the scoring engine into assessing a system or service as operational, when in fact it is not, may be suspended or fired. **Validation of this act will come with a significant points penalty** as it gives the Blue Team an unfair points advantage for a service that is not actually up.

3.2 Injects

If a business task, a.k.a. inject, requires multiple files for fulfillment, please compress the files into a single file in .zip format. This ensures that each inject has only one upload. Please name inject emails/files in the following format:

<teamNumber>_<injectNumber>_<injectTitle>

Injects and services are weighted evenly; it is disadvantageous to ignore injects.

There will be **NO** partial credit for late injects, so make a point to fulfill injects on-time. Inject responses that are turned in on-time will be allowed at least partial credit.

If an inject is directed to be submitted to the Gold Team Help Desk, select the ticket category ***Inject*** when creating the ticket.

4.0 ADDITIONAL INFORMATION

4.1 Blue Team Tools and Supplies

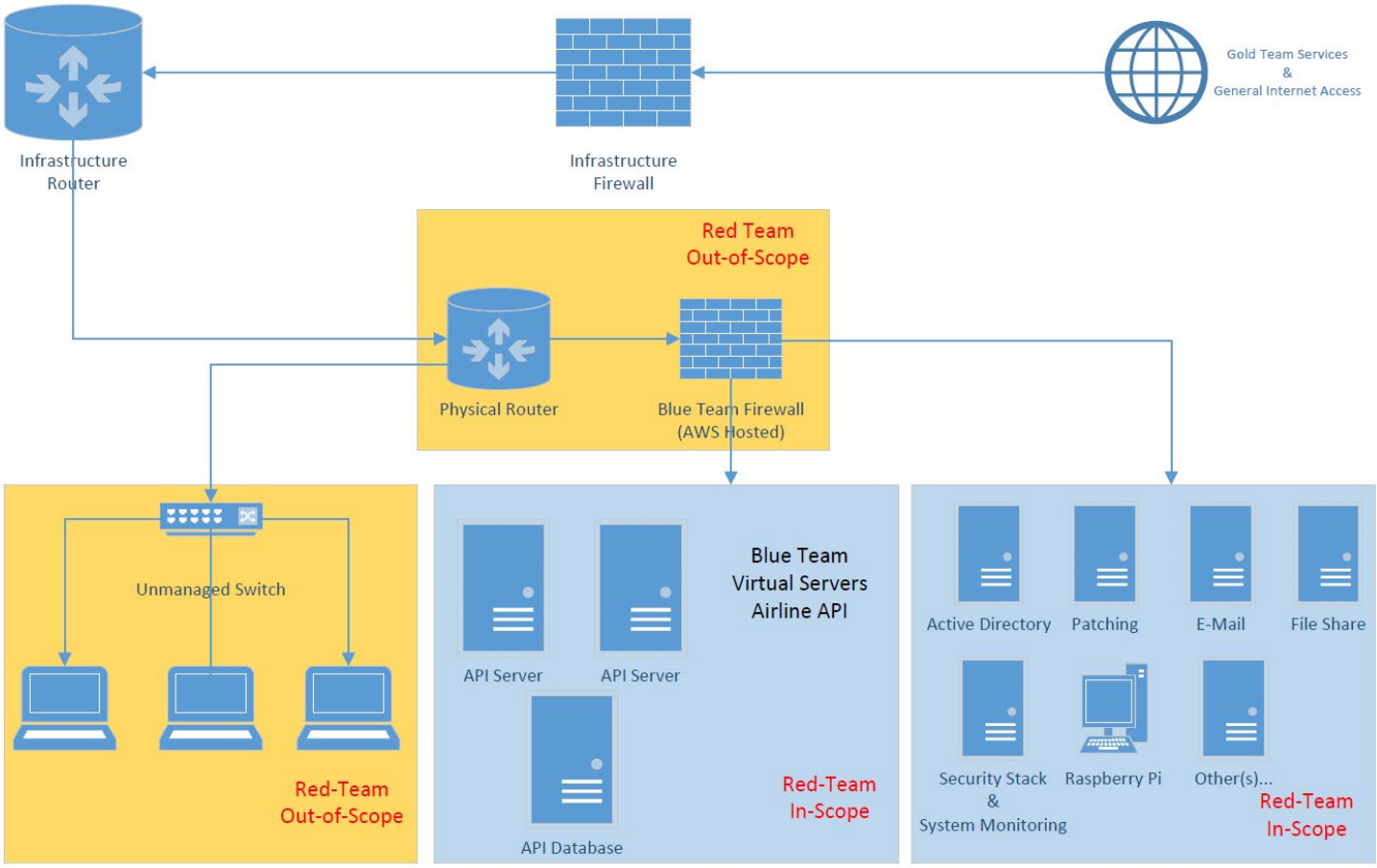
At the start of competition there will be supplies provided that could include notepads, pens, mouse pads, dry erase board markers and erases, and network cable tools. Please be sure to leave these on the team tables at the end of the day.

4.2 Scripting

Scripting during the competition is allowed, and teams are encouraged to write their own scripts. All team written scripts should be submitted to the Gold Team Help Desk for review and approval prior to use. Any resources or tools pulled down from the internet to assist with scripting should be publicly available and free of cost. The use of scripts or tools not created by the team should be submitted to Gold Team by opening a Help Desk ticket, including the citation for the tool or resource used if applicable. Failure to notify Gold Team of script or tool usage that was not provided by the Gold Team or the use of non-public resources may incur a penalty.

If the blue team has written a script in advance of the competition, it may only be brought into the competition typed and printed on a sheet of paper or hand-written in a notebook. It must be submitted to the Gold Team Help Desk including any sources used for approval.

Appendix A Network Diagram



Appendix B PASSWORD TRACKER

Username	Password	Account Description

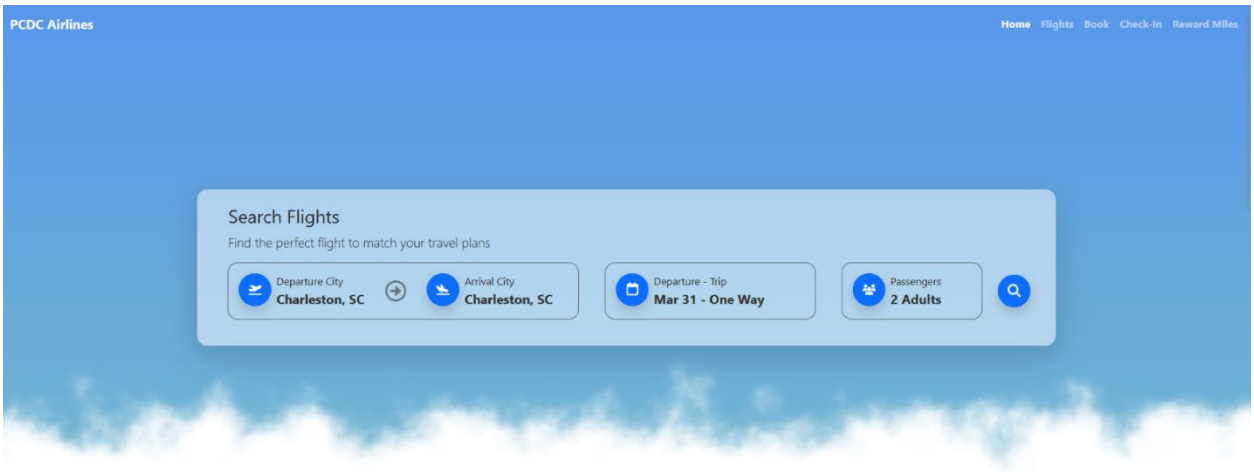
Appendix C ORGANIZATION CHART

This list only contains the PCDC Airline department leads and does not include all PCDC Airline employees. All employee accounts at the start of competition are valid accounts.

First Name	Last Name	Position	Domain Admin
Michael	Scott	CEO	Yes
Andy	Green	CISO	Yes
Angela	Martin	CFO	No
Oscar	Marinez	Lead Accountant	No
Kelly	Kapoor	Help Desk Lead	No
Larry	Lee	Customer Service Lead	No
Kevin	Malone	Food Services Lead	No
Joe	Ortiz	Marketing Lead	No
Dwight	Shrute	Sales Lead	No
Dylan	Sanders	Executive Assistant	No
Kathryn	Soulis	Lead Enterprise Administrator	Yes
Abigail	Jenkins	Lead Network Administrator	Yes
Keith	Hill	Lead Web Developer	Yes

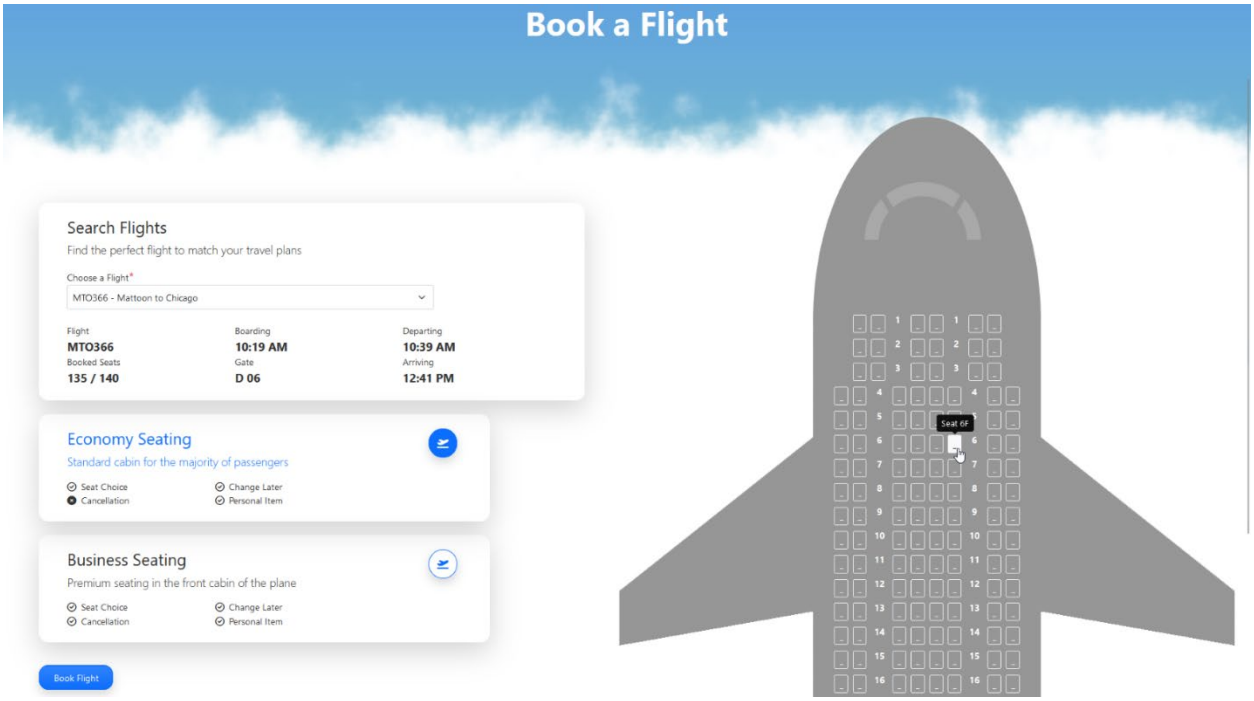
Appendix D PCDC AIRLINES WEBSITE

PCDC Airlines customer ticket sales and flight check-in are performed via a website. The below image displays what customers will see upon browsing to our site.



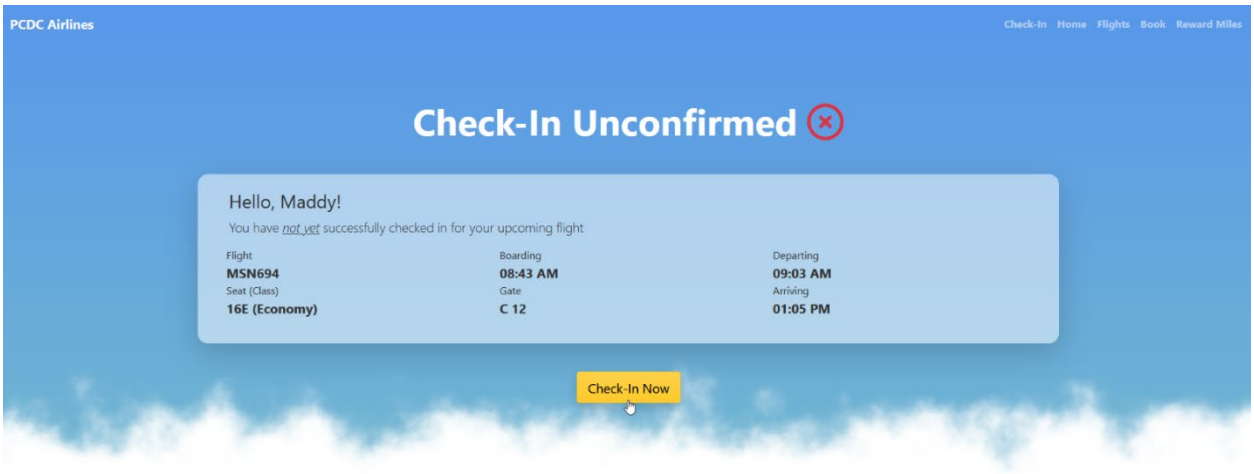
Booking a Flight for Passengers

In order to purchase a ticket for an upcoming PCDC flight, a passenger simply navigates to the PCDC Booking page, selects their flight of interest as well as their preferred seating prior to clicking on the ***Book Flight*** button in the bottom left of the page in order to provide their personal information for booking the flight.



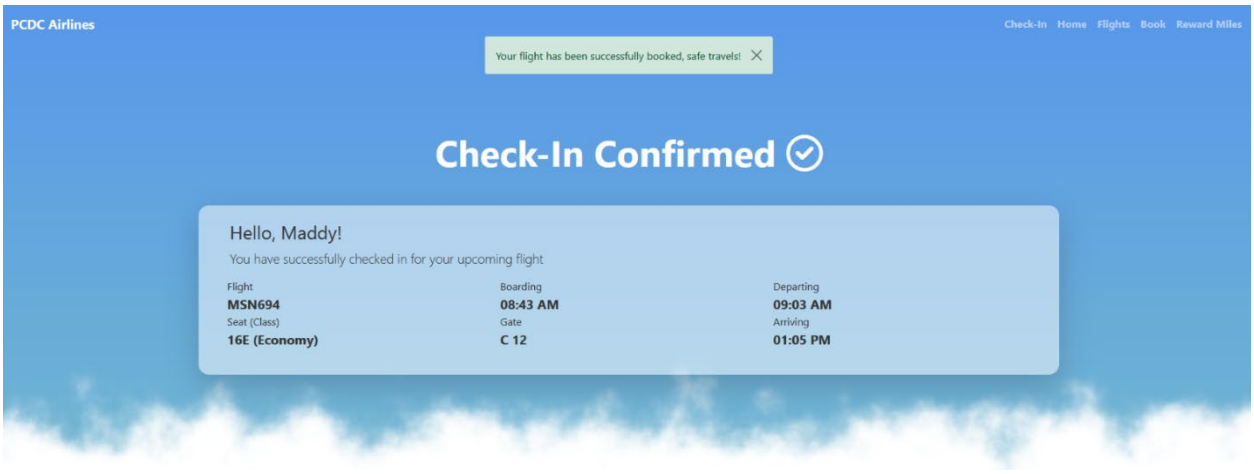
Check-In a Passenger's Booking

Passengers can quickly check-in for their flight by accessing the check-in page of the PCDC Airlines website, provide the ticket number or confirmation code associated with their flight booking, as well as their last name and then they will be redirected to their Check-In Confirmation page.



Here, passengers will be provided updated flight information, seat details, and their confirmation message or ability to check-in for their upcoming flight in order to confirm their seat reservation.

As always, make sure to be on the lookout for the Check-In Confirmed checkmark indicator to ensure your booking is confirmed prior to the flight taking off to make sure your trip goes off without a hitch!



This Page Intentionally Left Blank