NPS2001C
Milestone 1

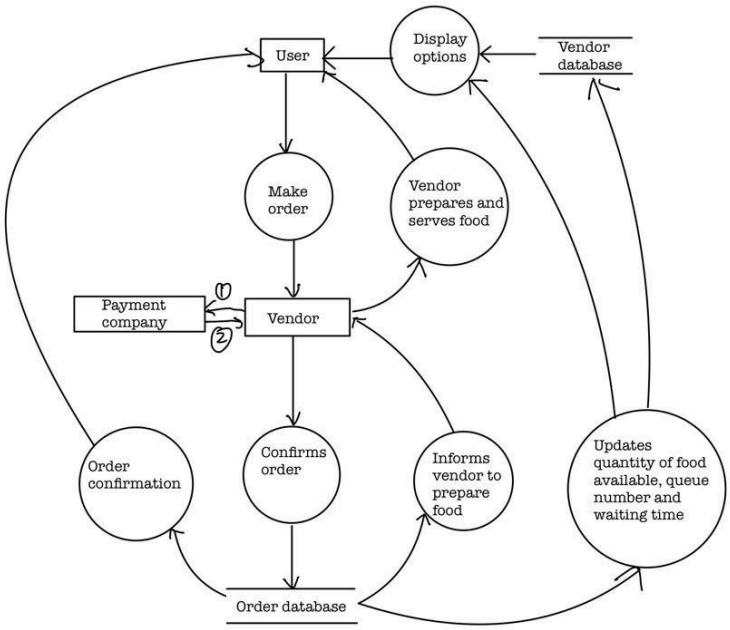
Chong Zhao Yang, Shun Pyae Phyo,
Ho Jia Wen, Jane, Han Xin Ping

Group Milestone 2: Data Report

Question 1 - What data does your app need to function and how will your app process it?

The app requires data such as store name, name of food item, price of food item, and availability of food item from vendors. In making the order, the app would obtain data such as the timing of the order, location/store ordered from, name of food item ordered, price of food item ordered, picture of food item ordered, quantity of food item ordered, total cart amount, and number of food items ordered in queue in front of the individual.

When making payment, the app would then obtain data such as username and password (optional to do so) for login, name and phone number and/or email to inform the user that their order is ready. These are the data that the app requires to function.



Question 2 - What are the issues related to data privacy and security for your app and how will your app deal with them?

Data privacy issues

A data privacy concern would be user content and transparency. In obtaining personal information such as names, phone numbers, and emails, individuals might not feel comfortable sharing their personal information to make the order. These are information that individuals can be identified with.

One possible data security issue for our app is attacks during data transfers. When data is being transmitted from the user to the server, the data will be transmitted as plaintext. As such, there is the risk of attacks during the transmission process which allow external parties to access personal information of the individuals.

Data security issue

Another possible security issue for the app is attacks on servers. When data is stored in servers, they are not encrypted. As such, attacks could be targeted directly to servers to obtain the personal information of individuals.

Mitigations for data privacy issues

We will mitigate data privacy issues by obtaining user consent when collecting personal information and fully disclose the personal information that we will be collecting (I.e. name, email address,

phone number). We will also state that all information will be used for order tracking only. Users would also have the option to decide which information they would prefer to share (consent preference) and are able to use a pseudonym for the order.

Risk Assessment

	Severity			
Likelihood		Mild	Moderate	Severe
	Unlikely	Low	Low	Moderate
	Likely	Low	Moderate	High
	Near certain	Moderate	Moderate	High

System: Food Ordering and Live Wait Timing App			
Threat Event	Likelihood	Severity	Risk Level
Loss of Confidentiality: The system and its data is compromised by hackers, or released publicly without approval	**Unlikely:** The app only handles non-financial identifiable information like mobile numbers and email addresses, making it less attractive to attackers compared to apps with sensitive financial data.	**Moderate:** While the exposed data (mobile numbers, email addresses) is identifiable, it lacks the financial sensitivity of credit card information or health records. This information, though not publicly available, can be misused for targeted marketing or scams, but doesn't directly grant access to financial accounts.	**Low**
Loss of Integrity: The system and its data can no longer be trusted, or made to be incomplete or incorrect	**Unlikely**: The app's lack of financial information diminishes the incentive for malicious actors, making targeted attacks less probable. Additionally, appropriate data integrity controls like encryption and access restrictions can further decrease the risk of successful tampering.	**Severe**: Tampering with food item details, prices, or availability could lead to misinformation, customer dissatisfaction, and potential financial losses for both users and vendors.	**Moderate**
Loss of Availability: The system and its data no longer exists, no longer responds to valid queries from users, or cannot be retrieved by an authorized user	**Unlikely:** The app could face system failures due to hardware malfunctions, software bugs, or targeted attacks such as DDoS. While such events are relatively rare, they can still occur, especially if proper safeguards are not in place.	**Severe:** System downtime could disrupt users' ability to place orders, leading to dissatisfaction, loss of revenue for vendors, and damage to the app's reputation. Moreover, in a university setting, where students and staff rely on timely food orders, any disruption to service could impact productivity and satisfaction.	**Moderate**
Overall Risk:			**Moderate**

How to Mitigate Security Risks

We will deal with data security issues by implementing encryption protocols such as Secure Sockets Layer (SSL) or Transport Layer (Security) during data transfer from the user to the server. We will also adopt encryption methods of data stored on the server and restrict access to this data. Lastly, we will also work with third-parties that meet stringent security standards to allow transactions to pass through their payment gateways.