Foodie’s Business Continuity Plan

[**Purpose 3**](#_9y101arc3xgl)

[**Critical Business Activities Identification 4**](#_ueaycnbneiqk)

[**Business Continuity Risk Assessment 5**](#_9p6p8ufgxj57)

[**Business Continuity Plan Development 32**](#_ioe1dqqdeid4)

[**Regular Review and Ongoing Maintenance 39**](#_n5wdkxor0fkp)

# Purpose

The purpose of Foodie's Business Continuity Plan is to provide a structured and comprehensive strategy that ensures the continued delivery of our services in the event of unforeseen disruptions. This plan emphasizes the significance of maintaining and resuming our business operations. It's designed to guarantee the continuity of vital functions related to our food delivery and ordering operations during and after significant incidents or disasters. A main goal of Foodie's BCP is to protect our employees, customers, and information assets, from data to infrastructure. By minimizing possible service interruptions, this BCP aims to quickly restore services to full operation, providing a clear action plan to avoid unplanned or rushed responses.

# Critical Business Activities Identification

**What is Foodie’s critical business activity:**

Considering Foodie is a company that provides food delivery service, the constant availability of food delivery services, food safety and health regulations are essential. Any business activity that can affect the continuity of these business areas can be considered as critical business activity.

**Foodie’s critical business activities include:**

* Mobile App food ordering process: The core business activities for a food delivery service company. Customers should be able to easily browse menus, select items, and place orders. Any disruption here may directly affect revenue and business continuity.
  + Relevant information assets identified in Foodie’s TRA:
    - Asset A: Main data center
    - Asset B: Order Transaction Records
    - Asset F: Payment and transaction data
    - Asset H: Backend system log
    - Asset P: Foodie’s source code
    - Asset T: Network
* Payment Processing: Customer’s payments need to be securely and effectively processed. Disruptions in this process will potentially cause reputational damage and loss of customer’s trust.
  + Relevant information assets identified in Foodie’s TRA:
    - Asset A: Main data center
    - Asset F: Payment and transaction data
    - Asset H: Backend system log
    - Asset P: Foodie’s source code
    - Asset T: Network
* Delivery process and route optimization: Timely deliveries directly impact customer satisfaction. A failure in the dispatch system can lead to chaotic operations, with drivers being unassigned or assigned inefficient routes. Such disruptions can halt or slow down the entire delivery process, affecting the business's day-to-day operations.
  + Relevant information assets identified in Foodie’s TRA:
    - Asset A: Main data center
    - Asset J: Delivery driver data
    - Asset H: Backend system log
    - Asset L: GPS Route Tracking system
    - Asset U: Employee training and awareness
* Inventory and Restaurant’s menu Management: If inventory isn't managed correctly or items could be out of stock, this could lead to canceled orders, frustrated customers, and potential loss of business.Without proper menu management, there might be delays in food preparation due to missing ingredients. This can lead to longer delivery times, impacting customer satisfaction and the efficiency of delivery personnel.
  + Relevant information assets identified in Foodie’s TRA:
    - Asset A: Main data center
    - Asset D: Menu and Restaurant Data
    - Asset N: Supply Chain data
* Technology and Infrastructure Management: Foodie heavily rely on technology and infrastructure for their day-to-day operations. From processing orders, managing inventory, to ensuring timely deliveries, all operations are technology-driven.
  + Relevant information assets identified in Foodie’s TRA:
    - Asset A: Main data center
    - Asset G: Computers or other tech equipment
    - Asset T: Network

# Business Continuity Risk Assessment

Information assets that are critical to the business continuity of Foodie’s operations have been identified in the previous section. By summarizing the risk assessment and business impact analysis conducted in Foodie’s TRA table, this section will identify potential threats and vulnerabilities of these critical information assets that could interrupt Foodie's operations, evaluate their potential impact, and establish the foundation upon which our Business Continuity Strategy is built.

**What risks would be considered to have a critical impact on business continuity:**

According to the WWMD table, risks that are high or critical are considered intolerable. That means if the loss of risks result in more than 50% of the daily delivery services affected or a single total financial loss of more than 5,000$ , those risks would be considered to have a critical impact on business continuity. How time sensitivity affects those losses will also be taken into account. A business continuity plan will be developed to mitigate them accordingly.

* **Asset A Main data cente**r:
  + Risk scenario A1: An outsider breaks into the main data center and steals the critical server hardware to disrupt the operations of Foodie.
    - Single total loss:
      * 1h: Cost of stolen assets, estimated to be 1500$
      * 1d: 1500$
      * 1w: 1500$
    - Time or resources:
      * 1h: One staff redirected from their usual duties to address the issue
      * 1d: Potential initiation of backup systems
      * 1w: Continuous and minor operation disruption"
    - Political:
      * 1h: None
      * 1d: Potential stakeholder disappointment
      * 1w: Increased regulatory attention
  + Risk scenario A2: Natural disasters damage the power supply in the main data center, resulting in the dysfunction of servers.
    - Single total loss:
      * 1h: Damaged properties: 5000$
      * 1d: Major service disruption: 11000$
      * 1w: Extended service disruption and infrastructure rebuild: More than 20000$
    - Time or resources:
      * 1h: Initial damage assessment and temporary controls by IT team
      * 1d: Senior management involvement in crisis resolution. External resources and help might be needed
      * 1w:Continuous engagement of the IT team and senior management
    - Political:
      * 1h: Minor complaints on unavailable service from social platform
      * 1d: Negative press coverage
      * 1w: Reputational damage and Shareholder Concerns
  + Risk scenario A3: A cyber criminal hacks the servers in the main data center and gains unauthorized access to sell critical data of Foodie.
    - Single total loss:
      * 1h: Legal consultations and discovery costs: around 1000$
      * 1d: Incident Response Costs: around 5000$
      * 1w: Vulnerability assessments, and enhancements to security infrastructure: More than 7000$
    - Time or resources:
      * 1h: Initial incident response by IT team
      * 1d: Complete incident response
      * 1w: Potential involvement of senior management and engaging external experts
    - Political:
      * 1h: Regulatory authorities could be alerted
      * 1d: Stakeholder Pressure
      * 1w: Potential fines or stricter regulations
  + **Based on BIA, A2 and A3 will most likely have a critical impact on the business continuity.**
* **Asset B Order Transaction Records:**
  + Access to order transaction records without authorization can result in a data breach. This can lead to the theft of important client information such as credit card numbers, addresses, and phone numbers.
    - Single total loss:
      * 1h: Potential loss due to unauthorized access: $10,000
      * 1d: Potential loss from data being sold or used maliciously: $50,000.
      * 1w: Costs associated with credit monitoring and identity theft protection for affected customers: $25,000.

* + - Time or resources:
      * 1h Approximately 8 hours of immediate response and investigation by IT and security teams.
      * 1d: Including external forensic analysis, legal consultation, and notification efforts, totalling around $200,000.
      * 1w: Ongoing efforts for the week, including continuous monitoring, forensic analysis, and improving security measures, requiring approximately 160 hours of work
    - Political:
      * 1h: Reputation: Initial damage to public perception.
      * 1d: Increased negative publicity.
      * 1w: Continued reputational damage, Potential legal actions and more substantial fines.
  + Risk scenario B2: Disruptions in the supply chain (e.g., ingredient shortages, transportation issues) can affect food availability and delivery times.
    - Single total loss:
      * 1h: Immediate response costs: $10,000

Potential loss in sales: $5,000

* + - * 1d: Continued disruption costs: $20,000

Additional sales losses: $15,000

* + - * 1w: Prolonged disruption costs: $50,000

Extended sales losses: $30,000

Potential reputation damage: $10,000

* + - Time or resources:
      * 1h: Approximately 4 hours to assess the initial disruption and begin taking corrective measures.
      * 1d: Continued efforts to manage the disruption, monitor the situation, and engage with suppliers. Approximately 8 hours of work per day.
      * 1w: Ongoing efforts to manage and resolve the supply chain disruption throughout the week, requiring 40 hours of work.
    - Political:
      * 1h: Initial concerns and inquiries from customers, suppliers, and partners.
      * 1d: Ongoing reputational damage as the disruption persists.
      * 1w: Potential legal actions and regulatory fines, especially if contract obligations are not met.
  + Risk scenario B3: Unauthorized or fraudulent financial transactions, including embezzlement or internal fraud by employees.
    - Single total loss:
      * 1h: Initial response costs: $20,000
      * 1d: Continued investigation costs: $40,000

Potential ongoing loss due to fraudulent transactions: $20,000

* + - * 1w: Legal and regulatory penalties: $50,000

Reputational damage: $40,000"

* + - Time or resources:
      * 1h: Approximately 4 hours for initial detection and response, including identifying the fraudulent activity and taking immediate action.
      * 1d: Ongoing efforts to investigate the fraudulent transactions, stop further activity, and implement security improvements.
      * 1w: Continued efforts over the week to address the situation, recover funds, and manage the fallout.
    - Political:
      * 1h: The negative impact on the company's image may begin to develop within the first hour.
      * 1d: Ongoing reputational damage as the fraudulent activity persists.
      * 1w: potential legal actions and regulatory fines, especially if contract obligations are not met.
  + **Based on BIA, B2 and B3 will most likely have a critical impact on the business continuity.**

* **Asset F Payment and Transaction Data**:
  + Risk scenario F1: False positives, resource intensiveness, privacy problems, alert fatigue, insider threats, and data management are among dangers that monitoring systems face. Process optimisation, compliance, data anonymization, prioritizing essential warnings, and dealing with insider threats are all critical for successful monitoring.
    - Single total loss:
      * 1h: $100-$2,000(estimated range based on investigation and mitigation costs)
      * 1d: $1,000-$20,000(estimated range based on the potential for data breaches and more extensive incident response)
      * 1w: $10,000-$200,000(estimated range, considering regulatory fines, legal actions, and reputational damage)
    - Time or resources:
      * 1h: This may require a small team or individual staff member to take initial actions.
      * 1d: A dedicated security or monitoring team, possibly involving IT staff, would need to coordinate efforts during this time frame.
      * 1w: A well-coordinated team, potentially including external experts, may be involved throughout the week to make substantial improvements.
    - Political:
      * 1h: Impact is likely to be minor and mainly internal.
      * 1d: Over the course of a day, the political impact could escalate as internal discussions become more pronounced.
      * 1w: Reputational concerns could grow, impacting relationships with clients, partners, and shareholders.
  + Risk scenario F2: To protect client data and ensure system integrity, the organization undertakes security assessments, addressing issues such as phishing, harmful ads, data breaches, insecure landing pages, and a lack of encryption.
    - Single total loss:
      * 1h: $1,000-$10,000(estimated range based on the potential for detecting and mitigating security issues such as phishing attempts and harmful ads.
      * 1d: $5,000-$50,000(estimated range, including the cost of addressing and recovering from data breaches or more substantial security incidents within a day)
      * 1w: $20,000-$200,000(estimated range, considering the possibility of extended data breaches and reputational damage.
    - Time or resources:
      * 1h: it would generally involve continuous monitoring, preliminary and security assessments.
      * 1d: Over the course of a day, addressing security issues like phishing, harmful ads, data breaches and insecure landing pages.
      * 1w: Comprehensive security assessments and addressing these issues would necessitate an even more significant allocation of resources.
    - Political:
      * 1h: Minor internal discussions about ongoing security assessments and potential issues within the organization.
      * 1d: Internal concerns may escalate, and there could be discussions within the organization.
      * 1w: Shareholders and stakeholders could express greater interest and concern if the issues persist.
  + Risk scenario F3: Data must provide a secure mobile app that uses robust authentication, validation, and frequent security audits to safeguard client data and ensure integrity.
    - Single total loss:
      * 1h: $100-$5,000(estimated range, focusing on the cost of maintaining robust authentication, validation, and conducting periodic security audits within the first hour)
      * 1d $500-$10,000 (estimated range, including potential incident response costs if security issues are detected and need immediate attention within a day)
      * 1w: $1,000-$20,000 (estimated range, considering the ongoing cost of security measures, including audits and maintaining the security infrastructure over the course of a week)
    - Time or resources:
      * 1h: During the first hour, a small team or individual staff member should be continuously monitoring the app's security, addressing any immediate issues, and performing routine checks.
      * 1d Over the course of a day, a dedicated security team or personnel should provide continuous monitoring and address any emerging security concerns.
      * 1w Maintaining security requires comprehensive efforts, including ongoing monitoring and the security team plays a central role in these activities over the week.
    - Political:
      * 1h: Minor complaints on social platforms about temporarily unavailable service may lead to minor reputational concerns and social media discussions.
      * 1d: Negative press coverage highlighting security issues can result in more significant reputational damage.
      * 1w: Shareholder concerns become more prominent as the situation persists.

:

* **Asset H Backend system log:**
  + Risk scenario H1: An immature employee misuses the software that controls backend system logs, and causes the data being altered or deleted. Thus resulting in the loss of availability and integrity of such data.
    - Single total loss:
      * 1h: Investigation costs: 200$
      * 1d: Service disruption and data recovery costs: 1500$
      * 1w: Potential major service disruption. Need of system auditing: 2500$
    - Time or resources:
      * 1h: Initiation of backup data and systems
      * 1d: In-depth Analysis by IT teams
      * 1w: Conduct employee training and resource redirection
    - Political:
      * 1h: None
      * 1d: Complaints from other department in the organization
      * 1w: Major complaints from certain stakeholders
  + Risk scenario H2: To disrupt the operations of Foodie, a hacker organizes a DDOS attack on the server that stores backend system logs, resulting in the loss of availability of such data.
    - Single total loss:
      * 1h: Immediate mitigation costs: 1000$
      * 1d: Major delivery service disruption: 3000$
      * 1w: Critical delivery service disruption: more than 5000$
    - Time or resources:
      * 1h: Immediate response by IT teams
      * 1d: Continued operational disruptions mitigation
      * 1w: Significant IT resources to mitigate the attack and restore data. Major update to the IT security measures. External experts are needed
    - Political:
      * 1h: Minor internal concerns and reputational damage
      * 1d:Major internal concerns. Major customer's complaints on social media platforms
      * 1w: Serious concerns raised by internal and external stakeholders. Loss of faith from customers
  + Risk scenario H3: To gain insights into system operations for malicious purposes, a hacker accesses and steals the backend system logs stored in the server, resulting in the loss of confidentiality of such data.
    - Single total loss:
      * 1h: Investigation costs: 700$
      * 1d: Legal consultations to assess potential regulatory penalties: 2000$
      * 1w: Loss of major data confidentiality: 4000$
    - Time or resources:
      * 1h: Potential temporary lockdown of system
      * 1d: In-depth data confidentiality assessment
      * 1w: Continued re-allocation of IT and managerial resources towards post-breach activities
    - Political:
      * 1h: None
      * 1d: Regulatory team's involvement and employee's concerns
      * 1w: Senior management concerns about data security policies and controls
  + **Based on BIA, H2 will most likely have a critical impact on the business continuity.**
* **Asset J Delivery Drivers data**
  + Risk scenario J1: Internal employees or other parties may inappropriately access and misuse driver data, resulting in privacy violations and legal consequences.
    - Single total loss:
      * 1h: Immediate Investigation Costs: From $2,000 to $5,000, depending on the complexity of the incident and the need for external expertise.
      * 1d: Data Recovery Expenses: From $2,000 to $5,000 for data recovery, especially if they have effective backup solutions in place.
      * 1w: Enhanced Security Measures: The costs of implementing enhanced security measures could vary but might fall in the range of $2,000 to $7,000
    - Time or resources:
      * 1h: Initial Communication: Notify key stakeholders, such as legal counsel and the incident response team, to initiate the response process.
      * 1d: Privacy Notifications: Notify affected drivers and regulatory authorities within the first day to comply with data protection laws. This may require printing, mailing, and communication costs.
      * 1w: Incident Response Plan Enhancement: Over the course of the first week, refine the incident response plan based on lessons learned from the incident to enhance future responses.
    - Political:
      * 1h: Immediate Concerns: In the initial hour, the focus is on containing the incident and assessing the immediate political implications. The organization's leadership and management should become aware of the incident. Political discussions and initial decisions may take place internally.
      * 1d: Reputation Damage: Within the first day, news of the incident may start to spread, potentially causing reputational damage. Customers, drivers, and the public may express concern and demand accountability.
      * 1w: Internal Changes: The organization may undergo internal changes or restructuring to prevent similar incidents in the future. This could involve changes in leadership, policies, and security measures.
  + Risk scenario J2: Attackers may manipulate drivers into divulging sensitive information or bypassing security protocols through social engineering techniques.
    - Single total loss:
      * 1h: Containment (Cost: $1,000 - $5,000): Isolating affected systems or data involves technical measures, such as temporarily disabling compromised accounts, which may require technical expertise or external assistance.
      * 1d: Data Assessment: Assess the extent of data exposed and the potential impact. ($1,000 - $5,000)
      * 1w:
        + Root Cause Analysis: Over the course of the week, conducting a root cause analysis to prevent similar incidents can involve costs ranging from $2,000 to $7,000 for forensic analysis and security improvements.
        + Enhanced Security Measures: Investment in enhanced security measures, such as access controls and monitoring tools, may range from $2,000 to $8,000, depending on the specific needs and scale of the hub.
    - Time or resources:
      * 1h: Allocate resources for monitoring systems or security software to detect the social engineering incident and promptly identify unauthorized access.
      * 1d: Data Assessment - Allocate internal staff time for assessing the extent of data exposed and the potential impact of the incident. Minimal external costs are involved.
      * 1w: Security Training:Develop a long-term driver training program on recognizing and responding to social engineering attempts. This includes training materials, staff time, and possibly external trainers.
    - Political:
      * 1h: Immediate Awareness - Within the first hour, senior management and key stakeholders should be informed about the incident.
      * 1d: Internal Communications - Within the first day, engage in internal communications addressing the incident. This includes discussions with affected employees, and internal stakeholders. Clear and transparent communication is crucial to manage internal political concerns.
      * 1w: Political and Legislative Impact - Depending on the nature and scale of the incident, it may lead to political discussions and debates on data protection laws and regulations. There may be calls for increased regulations or government oversight in response to such incidents.
  + Risk scenario J3: Stolen Devices: Delivery drivers often use mobile devices for work, and if these devices are lost or stolen, sensitive driver and customer data may be exposed.
    - Single total loss:
      * 1h:
        + Immediate Notification (Cost: $100 - $500): Quickly informing relevant internal stakeholders about the incident, including the IT department and management, which may require minimal external costs.
        + Immediate Identification (Cost: $500 - $2,000): Detecting the loss or theft of devices may require monitoring systems or remote device management tools. The cost can vary based on the sophistication of the tools and the number of devices to track.
      * 1d: Data Assessment: Internal staff time and possibly external experts (cost: $1,000 - $5,000) to assess the data exposure and potential impact.
      * 1w:
        + Device Replacement (Cost: $2,000 - $10,000): The cost of replacing lost or stolen devices and ensuring they have adequate security measures.
        + Security Training (Cost: $2,000 - $7,000): Develop a long-term security training program for drivers and staff to prevent future incidents.
    - Time or resources:
      * 1h: Immediate Identification and Containment - In the first hour, it's crucial to identify the stolen devices, remotely lock or wipe them (if possible), and change access credentials to prevent unauthorized access. This response primarily involves technical measures and staff time
      * 1d: Data Assessment - Over the course of the day, assess the potential impact of the incident, particularly the sensitivity of data exposed.
      * 1w: Security Training
        + Develop a long-term security training program for drivers and staff to prevent future incidents.
        + Incident Documentation Review - Review incident documentation to identify areas for improvement in incident response and reporting procedures.
    - Political:
      * 1h: Immediate Awareness - Within the first hour, ensure that the Foodie leadership and management are informed of the incident. Internal discussions may take place.
      * 1d: Internal Communications - Within the first day, engage in internal communication addressing the incident. This includes discussions with affected employees and internal stakeholders. Clear and transparent communication is essential to manage internal political concerns.
      * 1w: Political and Legislative Impact - Monitor and engage with any political discussions and debates related to data protection laws. Ensure that the Foodie's perspective is considered in potential legislative changes and proactively communicate with political stakeholders.

**Asset K Marketing campaigns**

* + Risk scenario K1: Monitoring systems face risks like false positives, resource intensiveness, privacy concerns, prioritizing critical alerts, and addressing insider threats are crucial.
    - Single total loss:
      * 1h: Investigation cost: 1000$
      * 1d: system failiur cost for all 3000$
      * 1w: For new system 4000$
    - Time or resources:
      * 1h:Respond by staff at a time
      * 1d: System lockdown
      * 1w:Replace security
    - Political:
      * 1h:None
      * 1d:Concern among IT team
      * 1w:Complain from share holder
  + Risk scenario k2: The company conducts security audits to safeguard customer data and maintain system integrity, addressing risks such as unsecured landing pages.
    - Single total loss:
      * 1h: Maintanance cost: 400$
      * 1d: Restore system integrity: 2000$
      * 1w: Landing new system: is 3500$
    - Time or resources:
      * 1h:Regular check by the team
      * 1d: Internal security analysis
      * 1w:Ongoing system monitoring
    - Political:
      * 1h:Regulation will be alerted
      * 1d: High pressure from users
      * 1w:Deploy reputation loss
* Risk scenario k3: TNeed to develop a secure mobile app to protect customer data and maintain integrity, utilizing strong and regular security audits.
  + Single total loss:
    - 1h: Investication cost: 1000$
    - 1d: Recovery cost: 2000$
    - 1w: New system integration: 4000$

Time or resources:

* + 1h:General checkup
  + 1d:System updated
  + 1w:Replace and improve security system
  + Political:
    - 1h:None
    - 1d: Concerns among shareholders
    - 1w: Concerns among IT team
* **Asset L GPS Route Tracking system**
  + Risk scenario L1: Malicious users can manipulate the real-time GPS data and route tracking system. It can cause the order missing or delay.
    - Single total loss:
      * 1h: Investigation cost: 500$
      * 1d: API configuration and system recovery cost: 4000$
      * 1w: New API configuration and restart: 5000$
    - Time or resources:
      * 1h: Response by technical staff on time
      * 1d: Most functions not working and the system barely lockdown
      * 1w: Replace the API and improve the security monitoring.
    - Political:
      * 1h: Minor internal concerns and discussions.
      * 1d: Major concerns surrounding customers and internal.
      * 1w: Major complaints from stakeholders.
  + Risk scenario L2: Malicious users can manipulate the real-time GPS data and route tracking system. It can cause the order missing or delay.
    - Single total loss:
      * 1h: Investigation cost: 1000$
      * 1d: Deploy the high-protection networking shield: 3000$.
      * 1w: Sensitive data loss: 8000$.
    - Time or resources:
      * 1h: Immediate response and system check by IT staff.
      * 1d: Internal security analysis and complete incident approach
      * 1w: Potential security configuration and continual efforts over a longer period to recover data and confirm data loss.
    - Political:
      * 1h: Regulation will be alerted.
      * 1d: high pressure from the public and stakeholders
      * 1w: Deeply reputation loss and regulatory further investigation.
* Risk scenario L3: The outside attacker intercept the GPS system data, result in data breach. The data can be sold on the dark web by hacker to gain huge money.
  + Single total loss:
    - 1h: Investigation cost: 1000$
    - 1d: Partly services offline in the short term: 2000$.
    - 1w: Potential major services disruption: 3800$.
  + Time or resources:
    - 1h: Update system security configuration.
    - 1d: Exports and regulations consultation and analysis.
    - 1w: Ongoing system monitoring and analysis over the week.
  + Political:
    - 1h: Regulation will be alerted.
    - 1d: Major concerns on reputational damage
    - 1w: Pressure from the stakeholders and the public.

**Asset M Marketing campaigns**

* + Risk scenario M1: Attack vector identification detects vulnerabilities in gaining sensitive user data. Security teams investigate, and implement mitigation measures.
    - Single total loss:
      * 1h:Cost of loss user data: 5000$
      * 1d:20000$
      * 1w:30000$
    - Time or resources:
      * 1h:Staff redirected the issue
      * 1d: Potential backups
      * 1w:Continues issues
    - Political:
      * 1h:None
      * 1d:Stakeholders disappointment
      * 1w:Media attractions
* Risk scenario M2: May shares user data without consent, data collection, strong anonymization, vendor evaluation, audits, and user education.
  + Single total loss:
    - 1h: Stolen data collection 15000$
    - 1d: Major services: 20000$
    - 1w: Extended services: 50000$
  + Time or resources:
    - 1h:Immediate response by team
    - 1d:Functions may not work
    - 1w: Improver the security
  + Political:
    - 1h:Will be alerted
    - 1d: High pressures from the team
    - 1w: Major complaints from shareholder
* Risk scenario M3: Company faces reputational damage from restaurant quality control failure, social media monitoring, and compensation.
  + Single total loss:
    - 1h:cost of quality control: 1000$
    - 1d:1500$
    - 1w:1500$
  + Time or resources:
    - 1h:Initial response will handle by team
    - 1d: Further losses will been calculated
    - 1w: IT team will inform total loss to authority
  + Political:
    - 1h:None minor concerns
    - 1d:Major concerns among customers
    - 1w: Pressure from media
* **Asset N Supply Chain data**
  + Risk scenario N1: Suppliers and third-party partners in the supply chain may have weak cybersecurity practices, making them susceptible to cyberattacks.
    - Single total loss:
      * 1h:
        + Containment (Cost: $2,000 - $7,000): Implementing measures to contain the incident, such as isolating compromised systems, may require technical resources and external assistance.
        + Internal Communication (Cost: $2,000 - $5,000): Costs related to internal communication and notifying relevant stakeholders about the incident.
      * 1d:
        + Data Assessment (Cost: $2,000 - $10,000): Assessing the extent of data exposure and potential impact may involve internal staff time and, in some cases, external experts (cost: $1,000 - $3,000).
        + Communication Plan (Cost: $2,000 - $7,000): Preparing a communication plan for internal and external stakeholders, involving staff time and possibly external communication support.
      * 1w:
        + Enhanced Security Measures (Cost: $10,000 - $20,000): Invest in security enhancements for the supply chain, including third-party assessments, access controls, and vendor security requirements. Costs may vary based on the scale of implementation.
        + Security Training (Cost: $5,000 - $15,000): Developing a long-term security training program for suppliers and third-party partners to improve their cybersecurity practices. Costs include training materials, staff time, and possibly external trainers.
    - Time or resources:
      * 1h:
        + Immediate Identification - Within the first hour, identify any ongoing or potential cyberattacks targeting suppliers and partners. This may involve monitoring systems and security alerts.
        + Containment - If a cyberattack is identified, take immediate containment measures to limit the damage and prevent further access to sensitive data.
        + Notification to Leadership - Notify the Foodie's leadership and management about the situation. Initiate discussions on how to proceed (internal communication).
      * 1d: Data Assessment - Over the course of the day, assess the extent of the cyberattack and potential data exposure. Internal staff time and potential external experts are involved.
      * 1w: Enhanced Security Measures - Invest in improving the cybersecurity practices of suppliers and third-party partners. This may include security assessments, access controls, and security requirements in contracts.
    - Political:
      * 1h: Within the first hour, ensure that the Foodie's leadership and management are informed of the situation involving suppliers and third-party partners with weak cybersecurity practices. Emphasize the potential risks and political implications.
      * 1d: Internal Communications - Within the first day, establish internal communication channels to address the incident with affected employees, internal stakeholders, and the leadership. Highlight the significance of the cybersecurity weaknesses among partners and the potential political impact. Emphasize transparency to manage internal political concerns.
      * 1w: Monitor and engage with any political discussions and debates related to data protection laws specifically in the context of supplier and partner cybersecurity practices. Ensure the Foodie's perspective is considered in potential legislative changes and proactively communicate with stakeholders.
  + Risk scenario N2: Attackers may attempt to steal sensitive supply chain data, including product designs, customer information, or trade secrets.
    - Single total loss:
      * 1h:
        + Immediate Identification (Cost: $7,000 - $20,000): Rapid identification of the incident may require monitoring systems and security software. Costs can vary based on the sophistication of monitoring tools.
        + Containment (Cost: $7,000 - $15,000): Implementing measures to contain the incident, such as isolating compromised systems, may require technical resources and external assistance.
      * 1d:
        + Data Assessment (Cost: $7,000 - $15,000): Assess the extent of data exposure and potential impact. This may involve internal staff time and, in some cases, external experts.
        + Communication Plan (Cost: $5,000 - $10,000): Prepare a communication plan for internal and external stakeholders, involving staff time and possibly external communication support.
      * 1w:
        + Enhanced Security Measures (Cost: $15,000 - $50,000): Invest in security enhancements specific to protecting sensitive supply chain data, including security assessments, access controls, and vendor security requirements. Costs may vary based on the scale of implementation.
        + Security Training (Cost: $10,000 - $25,000): Develop a long-term security training program for employees and partners to improve their cybersecurity practices, with a focus on safeguarding sensitive supply chain data.
        + Incident Response Plan Improvement (Cost: $17,000 - $15,000): Refine the incident response plan based on lessons learned from the incident and enhance it for future readiness, focusing on protecting sensitive supply chain data.
    - Time or resources:
      * 1h:
        + Within the first hour, the IT and security teams work to identify the breach, using existing monitoring systems and security software
        + Immediate containment measures are initiated, isolating compromised systems and preventing further unauthorized access
        + A brief communication is made to the Foodie's leadership to apprise them of the situation, emphasizing the need for immediate action.
      * 1d:
        + Throughout the day, a thorough assessment is carried out to gauge the scope of data exposure and potential consequences. Simultaneously, a comprehensive communication plan is devised to ensure transparency and trust among both internal and external stakeholders.
      * 1w:
        + Significant investments are dedicated to improving security through measures such as security assessments, access controls, and vendor security requirements. Additionally, a comprehensive, long-term security training program is designed for employees and partners to enhance their cybersecurity practices, with a particular emphasis on protecting sensitive supply chain data.
    - Political:
      * 1h: Within the first hour, inform the Foodie's leadership about the breach. Highlight the potential political implications and the need for swift action. Clear communication with leadership is vital to ensure they are aware of the situation.
      * 1d: During the first day, worries within the organization can grow as employees, stakeholders, and leadership want to feel secure and well-informed. There might be meetings about how this affects the organization's image and its position in the industry.
      * 1w: Rebuilding trust with customers and the public becomes a significant political priority. The startup must take measures to assure affected parties that their information and trade secrets will be safeguarded in the future. Failing to do so can have lasting political consequences.
  + Risk scenario N3: Threat actors may use phishing emails or social engineering tactics to deceive employees or suppliers into revealing sensitive information or login credentials.
    - Single total loss:
      * 1h: Immediate Identification and Mitigation Cost: $3,000
      * 1d:
        + Investigation and Communication Cost: $7,000
        + Employee and Supplier Training Cost: $4,000
      * 1w:
        + Ongoing Monitoring and Security Enhancements Cost: $7,000
        + Rebuilding Trust Cost: $10,000
    - Time or resources:
      * 1h: In the first hour, Foodie should allocate resources for immediate identification and mitigation of the phishing attack. This includes investing in cybersecurity tools, analysis, and incident response efforts to stop the attack.
      * 1d: In the first day post-incident, a thorough investigation is launched to assess data exposure, while communication and public relations activities are initiated to inform stakeholders. Simultaneously, immediate training programs are implemented for employees and suppliers to recognize and prevent phishing attacks, with associated costs for training materials and staff time.
      * 1w: Throughout the first week, there is a focus on continuous system monitoring and security improvements to mitigate future phishing attacks, involving investments in security assessments and access controls. Additionally, substantial efforts and costs are directed towards rebuilding trust with customers, suppliers, and the public through communication, compensation, and marketing initiatives to reassure those affected by the incident.
    - Political:
      * 1h: In the first hour, top leadership becomes aware of the incident and its potential political implications, such as concerns about data security and potential data breaches. Immediate awareness is crucial for quick political decision-making.
      * 1d: Over the first day, internal political concerns may intensify as employees, stakeholders, and leadership seek reassurance and transparency. There could be discussions on how the breach affects the organization's reputation and its political standing within the industry.
      * 1w: Be prepared for potential political consequences, such as meetings for changes in leadership related to oversight of cybersecurity. Strategies should be developed to address these political outcomes while minimizing adverse effects.
* **Asset O Logistical Information**
  + Risk scenario O1: Attackers may use phishing emails, pretexting, or social engineering tactics to trick employees into revealing login credentials or other sensitive information. This can compromise logistical systems and data.
    - Single total loss:
      * 1h: Immediate Identification and Mitigation Cost: $3,000
      * 1d:
        + Investigation and Communication Cost: $7,000
        + Employee and Supplier Training Cost: $4,000
      * 1w:
        + Ongoing Monitoring and Security Enhancements Cost: $7,000
        + Rebuilding Trust Cost: $10,000
    - Time or resources:
      * 1h: Within the first hour, the IT and security teams work diligently to identify the nature and scope of the breach, assessing the extent of potential data exposure and system compromise.
      * 1d: Over the first day, a comprehensive investigation is launched to determine the full extent of data exposure and assess the damage to logistical systems. Communication efforts, including notifying affected employees and stakeholders, are essential.
      * 1w: Throughout the first week, the startup intensifies efforts on ongoing monitoring of systems and security enhancements. This involves continuous allocation of time and resources to strengthen the security posture and prevent future incidents.
    - Political:
      * 1h: In the first hour, top leadership becomes aware of the incident and its potential political implications, such as concerns about data security and potential data breaches. Immediate awareness is crucial for quick political decision-making.
      * 1d: Over the first day, internal political concerns may intensify as employees, stakeholders, and leadership seek reassurance and transparency. There could be discussions on how the breach affects the organization's reputation and its political standing within the industry.
      * 1w: Be prepared for potential political consequences, such as meetings for changes in leadership related to oversight of cybersecurity. Strategies should be developed to address these political outcomes while minimizing adverse effects.
  + Risk scenario O2: Unauthorized access to logistical information can lead to data breaches, compromising sensitive data related to shipments, routes, schedules, and inventory levels. This can result in financial losses, legal issues, and damage to reputation.
    - Single total loss:
      * 1h: Immediate Identification and Mitigation Cost: $3,000
      * 1d: Investigation and Communication Cost: $5,000
      * 1w: Ongoing Monitoring and Security Enhancements Cost $5,000 - $15,000
    - Time or resources:
      * 1h: Within the first hour, Foodie will allocate resources to identify and mitigate the breach, which includes expenses for monitoring systems and security software to stop the unauthorized access.
      * 1d: Over the first day, a comprehensive investigation is conducted to understand the extent of data exposure and assess system vulnerabilities. Communication efforts to inform affected parties, employees, and stakeholders are vital and incur costs related to communication materials and public relations efforts.
      * 1w: Throughout the first week, the startup focuses on ongoing monitoring of systems and security enhancements to prevent future unauthorized access. This includes investments in security assessments, access controls, and vendor security requirements.
    - Political:
      * 1h: Within the first hour, the Foodie's leadership becomes aware of the breach and acknowledges the potential political implications. Immediate concerns arise about the security of sensitive logistical data, which can impact the Foodie's reputation and raise questions about data protection.
      * 1d: Over the first day, internal political concerns may intensify as employees, stakeholders, and leadership seek reassurance and transparency. Questions about how the breach affects the Foodie's reputation and potential legal issues emerge.
      * 1w: Foodie may face financial and legal consequences related to the data breach. Legal costs, fines, and potential lawsuits may contribute to the political and financial impact.
  + Risk scenario O3: Employees, contractors, or drivers with access to logistical information may intentionally or inadvertently misuse or expose the data.
    - Single total loss:
      * 1h: Immediate Identification and Mitigation Costs: From $2,000 to $5,000, depending on the complexity of the incident and the need for external expertise.
      * 1d: Investigation and Communication: From $3,000 to $7,000.
      * 1w: Ongoing Monitoring and Security Enhancements: The costs of implementing enhanced security measures and ongoing monitoring could vary but might fall in the range of $5,000 - $12,000
    - Time or resources:
      * 1h: Within the first hour, Foodie will initiate efforts to detect any unauthorized or unintended data exposure. This may involve analyzing access logs and monitoring systems, consuming significant time and attention from IT and security teams.
      * 1d: Over the first day, a comprehensive investigation is launched to understand the extent of data exposure, assess system vulnerabilities, and determine if data misuse was intentional. This investigation is resource-intensive and requires substantial time from IT and security personnel.
      * 1w:
        + Throughout the first week, the startup focuses on ongoing monitoring of systems, security enhancements, and stricter access controls to prevent future data misuse or exposure. This continuous process requires both time and resources.
        + If data misuse led to financial losses or legal penalties, the startup will need to allocate resources for compensating affected parties or covering legal costs.
    - Political:
      * 1h: Within the first hour, the Foodie's leadership becomes aware of the breach and acknowledges the potential political implications. Immediate concerns arise about the security of sensitive logistical data, which can impact the Foodie's reputation and raise questions about data protection.
      * 1d: Over the first day, internal political concerns may intensify as employees, stakeholders, and leadership seek reassurance and transparency. Questions about how the breach affects the Foodie's reputation and potential legal issues emerge.
      * 1w: Foodie may face financial and legal consequences related to the data breach. Legal costs, fines, and potential lawsuits may contribute to the political and financial impact.
* **Asset Q Regularity Guidlines:**
  + Risk scenario Q1: The company fails to follow safety standards and guidelines, leading in the delivery of dangerous or contaminated food to clients
    - Single total loss:
      * 1h: Legal consultations and discovery costs: around 1500$
      * 1d: Incident Response Costs: around 4500$
      * 1w: Vulnerability assessments, and enhancements to security infrastructure: More than 6000$
    - Time or resources:
      * 1h: Initial incident response & check by IT team
      * 1d: Complete incident response
      * 1w: Potential involvement of senior management
    - Political:
      * 1h: Minor problems
      * 1d: Stakeholder Pressure
      * 1w: Potential fines
  + Risk scenario Q2: The organization fails to protect client data, resulting in data breaches and privacy providers.
    - Single total loss:
      * 1h: Immediate mitigation costs: 1000$
      * 1d: Major delivery service disruption: 3000$
      * 1w: Critical delivery service disruption: more than 5000$
    - Time or resources:
      * 1h: Immediate response by IT teams
      * 1d: Continued operational disruptions mitigation
      * 1w: Significant IT resources to mitigate the attack and restore data. Major update to the IT security measures. External experts are needed
    - Political:
      * 1h: Minor problems
      * 1d: Stakeholder Pressure
      * 1w: Pressure form the public
  + Risk scenario Q3: Laws and regulations regulating the food delivery industry change unexpectedly, resulting in noncompliance.
    - Single total loss:
      * 1h: Investigation cost 1000$
      * 1d: 3000%
      * 1w: loss 4500$
    - Time or resources:
      * 1h: Initial incident response & check by IT team
      * 1d: Complete incident response
      * 1w: Monitoring
    - Political:
      * 1h: Minor problems
      * 1d: Stakeholder Pressure
      * 1w: Major problems from stackholders
* **Asset R Employee code of conduct :**
  + Risk scenario R1: An employee obtains illegal access to consumer data and utilizes it for personal advantage or shares it with third parties.
    - Single total loss:
      * 1h: Estimated cost 500-1500$
      * 1d: 2500$
      * 1w: data loss 4500$
    - Time or resources:
      * 1h:Response by technical staff
      * 1d: analysis security problems
      * 1w: Update systems
    - Political:
      * 1h: None
      * 1d: major concerns on reputation
      * 1w: reputation loss
  + Risk scenario R2: A firm employee files a complaint alleging discrimination harassment, or a hostile work environment
    - Single total loss:
      * 1h: Estimated cost: 700$-2500$. For Initial maintenance and access costs.
      * 1d:$5000- $9000. For Maintenance, and system availability.
      * 1w: For Ongoing maintenance, data backup, cost 7000$-13000$
    - Time or resources:
      * 1h:Potential temporary breakdown of system
      * 1d: For dedicating resources would involve a small team or individual staff member ensuring maintenance, data backups, and system availability.
      * 1w: Potentially involving a dedicated team
    - Political:
      * 1h: None or minor concerns inside
      * 1d: Major concerns on reputational damage
      * 1w: Pressure from the stakeholders and the public.
  + Risk scenario R3: Failure to follow safety requirements by delivery drivers results in accidents, injuries, and damage to corporate and consumer property.
    - Single total loss:
      * 1h: Investigation costs: 100$
      * 1d: Containment Costs: 500$
      * 1w: System Restoration: 1000$
    - Time or resources:
      * 1h: Potential system downtime
      * 1d: Might affect the productivity of employee.
      * 1w: Continuous monitoring
    - Political:
      * 1h: None
      * 1d: Potential Stakeholder Concerns
      * 1w: Regulatory investigation
* **Asset P Foodie’s APP source code**
  + Risk scenario P1: The user of Foodie provides the home address when they order food through APP. A MitM attacker can capture this address infomation data.
    - Single total loss:
      * 1h: Investigation cost: 500$
      * 1d: Deploy the high-protection networking shield: 3000$
      * 1w: Sensitive data loss: 8000$
    - Time or resources:
      * 1h: Immediate response and system check by IT staff.
      * 1d:Internal security analysis and complete incident approach.
      * 1w: Potential security configuration and continual efforts over a longer period to recover data and confirm data loss.
    - Political:
      * 1h: Regulation will be alerted.
      * 1d: high pressure from the public and stakeholders.
      * 1w: Deeply reputation loss and regulatory further investigation.
* Risk scenario P2: The gain the password or code of Foodie's APP. The hacker can apply brute force attacks that attacker use multiple world password library to try the all password combinations until get correct one.
  + Single total loss:
    - 1h: Investigation cost: 200$
    - 1d: Inadequate hashing or MD5 Method: 2000$
    - 1w: Sensitive data loss: 6500$
  + Time or resources:
    - 1h: Immediate response and system check by IT staff.
    - 1d:Internal security analysis and complete incident approach.
    - 1w: Monitoring the system status by the security team and risk assessment team.
  + Political:
    - 1h: None or minor concerns.
    - 1d: Potential stakeholder pressure
    - 1w: Increased stakeholders pressure and the public.
* Risk scenario P3: To access the admin protal of Foodie, the hacker will use SQL injection in the login form page which has an administrative portal. To grant fully control of the Foodie's platform.
  + Single total loss:
    - 1h: Database damage cost: $5000
    - 1d: Major database structure damage: 8000$
    - 1w: Re-design the database and deploy high shield:12000$
  + Time or resources:
    - 1h: Immediate response by database admin staff.
    - 1d: Senior database engineers and the security team start addressing further issues and enhancements.
    - 1w: Continuous engagement of the security team and CTO CIO.
  + Political:
    - 1h: Regulation will be notified.
    - 1d: Potential stakeholder pressure.
    - 1w: Major complaints from stakeholders.
* **Asset S Vendor contracts :**
  + Risk scenario S1: One of the key suppliers fails to satisfy contractual obligations, causing supply chain interruptions and affecting the company's ability to deliver orders.
    - Single total loss:
      * 1h: Estimated cost: 700$
      * 1d: Deploy the high-protection networking shield: 3500$
      * 1w: Sensitive data loss: 7000$
    - Time or resources:
      * 1h: Immediate response and system check by IT staff
      * 1d: Internal security analysis and complete incident approach
      * 1w: Potential efforts over a longer period to recover data and confirm data loss
    - Political:
      * 1h: Regulation will be alerted
      * 1d: high pressure from the public and stakeholders
      * 1w: Deeply reputation loss and regulatory further investigation.
  + Risk scenario S2: A vendor or partner who handles client data shares it with third parties without proper authorisation, potentially resulting in data breaches and privacy violations.
    - Single total loss:
      * 1h: Investigation cost 1000$
      * 1d: 3000%
      * 1w: loss 4500$
    - Time or resources:
      * 1h: Initial incident response & check by IT team
      * 1d: Complete incident response
      * 1w: Monitoring
    - Political:
      * 1h: Minor problems
      * 1d: Stakeholder Pressure
      * 1w: Major problems from stakeholders
  + Risk scenario S3: A supplier is discovered to be involved in unethical or environmentally hazardous methods, causing the food delivery company's reputation to suffer.
    - Single total loss:
      * 1h: Investigation costs: 500$
      * 1d: Service disruption : 2500$
      * 1w: Potential major service disruption. Need of system: 3500$
    - Time or resources:
      * 1h: Initiation of backup data and systems
      * 1d: In-depth Analysis
      * 1w: Conduct employee training and resource redirection
    - Political:
      * 1h: None
      * 1d: Complaints from other department in the organization

**Asset V Marketing campaigns**

* + Risk scenario V1: Cyberattacks targeting Executive Leadership Insights systems could expose confidential information, potentially causing reputational damage, investor loss.
    - Single total loss:
      * 1h: Damage information: 2000$
      * 1d:1000$
      * 1w:1000$
    - Time or resources:
      * 1h: Initial response from IT team
      * 1d: Management will interfere
      * 1w: Fully integrated by the team
    - Political:
      * 1h:Minor complain
      * 1d: stakeholder’s disappointing the fact
      * 1w: Reputational damage
  + Risk scenario V2: Employees accessing Executive Leadership Insights may intentionally or accidentally leak sensitive information legal consequences, and loss of trust among stakeholders.
    - Single total loss:
      * 1h:Leak information: 6000$
      * 1d: 7000$
      * 1w:8000$
    - Time or resources:
      * 1h: One member will identify the issue
      * 1d: Management interfere
      * 1w: Continues operation disruption
    - Political:
      * 1h:Negative press conference
      * 1d: stakeholder disappointment
      * 1w: Increased bad approach
  + Risk scenario V3: Physical breaches expose confidential information, damage reputation, and lead to legal consequences.
    - Single total loss:
      * 1h:Confidential information costs:8000$
      * 1d: Major damage: 10000$
      * 1w: Extended services : 15000$
    - Time or resources:
      * 1h: Temporally controls by IT team
      * 1d: Seniormanagement involvement
      * 1w: Continues involvement of the whole team
    - Political:
      * 1h:Authorized alert the fact
      * 1d: Negative press coverage
      * 1w: Reputation damage

# Business Continuity Plan Development

To ensure uninterrupted service to our customers and reduce the risk of business disruptions, this section will outline comprehensive business continuity strategies tailored to address potential impacts arising from identified critical information assets and its scenarios.

* **Asset A Main data center:** 
  + Key Functions: Hosting critical server hardware, data storage, and service operations.
  + Primary Asset Owner:CIO
  + Procedure for Critical Scenario A2:
    - Immediate: Initiate emergency power systems, secure all critical server hardware.
    - Short-term: Evaluate damage extent, engage emergency repair teams, and begin recovery from backups.
    - Long-term: Establish secondary power sources, contract with emergency repair services, and conduct drills for natural disaster scenarios..
  + Procedure for A3:
    - Immediate: Initiate system lockdown, notify Incident Response Team and legal department.
    - Short-term: Assess the scope and impact of the breach, communicate with affected stakeholders, and implement initial countermeasures.
    - Long-term: Strengthen server defenses, undergo periodic security evaluations, and partner with cybersecurity experts for continuous monitoring and advanced defense mechanisms.
* **Asset H Backend system log:**
  + Key Functions: Monitor and store server transaction records, system operations, and security logs.
  + Primary Asset Owner: CIO
  + Procedure for Critical Scenario H2:
    - Immediate: Activate DDoS mitigation tools, inform the cybersecurity team.
    - Short-term: Collaborate with cybersecurity firms to trace the origin, update firewall and defense systems.
    - Long-term: Regularly evaluate and bolster DDoS defense mechanisms, conduct periodic penetration testing.
* **Asset J Delivery Drivers data**
  + Key Functions: Optimizing routes, enhancing customer service, and ensuring driver safety. It helps minimize delivery times, offers accurate tracking, and serves as proof of delivery. This data aids in evaluating driver performance, efficient work scheduling, and accurate compensation. It supports inventory management, customer communication, and maintaining a positive customer experience. Compliance with regulations and safety standards is monitored, while insights from the data drive continuous improvement. In the event of incidents, the data is invaluable for investigations. Overall, driver data is the backbone of a well-organized and customer-focused food delivery hub.
  + Primary Asset Owner: COO
  + Procedure for Scenario J1:
    - Immediate: As soon as unauthorized access is suspected or detected, the incident should be documented and reported to the designated authority, such as the information security officer or incident response team.
    - Short-term: Isolate the affected systems, servers, or data sources from the network to prevent further unauthorized access and potential data compromise. Notify the affected delivery drivers whose data may have been accessed. Provide guidance on what steps they should take to protect their information, such as changing their passwords or monitoring their accounts for suspicious activity.
    - Long-term: Identify the root causes of the breach, including any vulnerabilities or weaknesses in security controls, processes, or employee behavior that allowed the unauthorized access to occur. Consider implementing data encryption to protect sensitive driver data both at rest and during transit.
  + Procedure for Scenario J2:
    - Immediate: Report the phishing attack to relevant authorities and regulatory bodies, if required by data protection regulations. Engage the incident response team or designated personnel to handle the incident and assess the potential risks and impact.
    - Short-term: Scan the compromised device for malware or any residual threats. Remove any identified malicious software and ensure the device is secure. Immediately change the compromised user's login credentials, including passwords and access keys, to prevent further access by the attacker.
    - Long-term:
      * Implement continuous security awareness and training programs for all employees, with a focus on recognizing and avoiding phishing attempts.
      * Enforce MFA for accessing sensitive systems and data, ensuring an additional layer of security beyond passwords.
      * Conduct regular simulated phishing exercises to test and improve employees' ability to identify and report phishing emails.
      * Strengthen access controls to limit user privileges, ensuring that employees have access only to the data and systems required for their roles.
  + Procedure for Scenario J3:
    - Immediate: Immediately change any access credentials associated with the stolen device, such as login passwords, access keys, or PINs. Communicate the incident to relevant personnel within the organization to ensure everyone is aware of the situation and can provide support as needed.
    - Short-term: If the stolen device has remote management capabilities (e.g., mobile phones, tablets), use these features to remotely lock the device and initiate a data wipe to erase all. Determine if there are recent backups of the data that was on the stolen device and restore it to a replacement device if available.
    - Long-term: Provide ongoing training and education to all delivery drivers on security best practices, emphasizing the importance of securing their devices and data. Enable tracking and geolocation services on devices to assist in locating and recovering stolen devices. Use remote management and tracking capabilities for all devices to facilitate remote locking and data wiping in case of theft or loss.
* **Asset N Supply Chain data**
  + Key Functions: Key functions of supply chain data in Foodie include inventory management, cost control, quality assurance, supplier relationship management, demand forecasting, and customer communication, all of which are essential for efficient operations and customer satisfaction.
  + Primary Asset Owner: COO
  + Procedure for Scenario N1:
    - Immediate:
      * Immediately contact the vulnerable suppliers and third-party partners to notify them of potential weaknesses and encourage them to take immediate action.
      * If feasible, isolate or limit connections with the vulnerable vendors until their security weaknesses have been addressed to prevent potential threats from spreading.
    - Short-term:
      * Implement a formal third-party risk assessment process to evaluate the cybersecurity practices and vulnerabilities of all suppliers and third-party partners.
      * Establish formal cybersecurity agreements and contracts with suppliers and partners, outlining their responsibilities for maintaining robust security practices.
    - Long-term:
      * Assess the security practices of third-party vendors and partners who have access to supply chain data, ensuring they adhere to robust security standards.
      * Provide ongoing training and awareness programs for employees and contractors to maintain a security-conscious culture.
      * Conduct periodic security audits and risk assessments to identify evolving threats and vulnerabilities.
      * Continuously refine the incident response plan to improve the organization's ability to address data theft incidents effectively.
  + Procedure for Scenario N2:
    - Immediate: Immediately isolate the affected systems or data repositories where the theft occurred to prevent further unauthorized access. Activate the incident response team to investigate and mitigate the data theft incident, identifying the scope and source of the breach.
    - Short-term:
      * Encrypt sensitive supply chain data at rest and during transmission to protect it from theft or unauthorized access.
      * Implement 2FA for critical systems and user accounts to enhance security.
    - Long-term:
      * Provide ongoing training and awareness programs for employees and contractors to maintain a security-conscious culture.
      * Conduct periodic security audits and risk assessments to identify evolving threats and vulnerabilities.
      * Continuously refine the incident response plan to improve the organization's ability to address data theft incidents effectively.
  + Procedure for Scenario N3:
    - Immediate:
      * User Account Lockdown - If an employee or supplier has fallen victim to the phishing attempt, immediately lock or disable their account to prevent further unauthorized access.
      * Report the phishing attack to relevant authorities and regulatory bodies, if required by data protection regulations. Engage the incident response team or designated personnel to handle the incident and assess the potential risks and impact.
    - Short-term:
      * Phishing Simulations - Implement regular phishing simulation exercises to continuously test and reinforce employees' and suppliers' ability to detect and respond to phishing attempts.
      * Multi-Factor Authentication (MFA) - Require the use of MFA for email and other critical systems to enhance security.
    - Long-term:
      * Comprehensive Security Training - Offer ongoing, in-depth security training that includes practical guidance on recognizing and responding to phishing attempts and social engineering tactics.
      * Extend security education and awareness programs to vendors, suppliers, and partners who have access to supply chain data.
* **Asset O Logistical Information**
  + Key Functions: Logistical information in Foodie serves as a critical tool for optimizing delivery routes, enabling real-time tracking of delivery vehicles, and providing proof of delivery with time and location stamps. These functions enhance the efficiency and reliability of food deliveries, ensuring customer satisfaction and effective delivery operations.
  + Primary Asset Owner: COO
  + Procedure for Scenario O1:
    - Immediate: Notify the IT and security teams about the phishing incident, providing them with details of the attempted attack.
    - Short-term: Conduct a malware scan on the affected user's device to ensure that no malicious software has been installed.
    - Long-term: Conduct regular security audits and assessments to identify vulnerabilities and areas for improvement in the organization's security posture.
  + Procedure for Scenario O2:
    - Immediate:
      * Immediately revoke access for any unauthorized users or accounts that have gained access to logistical information.
      * Lock or disable accounts that are suspected of unauthorized access until they can be thoroughly reviewed and verified.
    - Short-term:
      * Two-Factor Authentication (2FA) - Require 2FA for all users to add an extra layer of security to the login process.
      * Regular User Access Reviews - Conduct periodic reviews of user access privileges to ensure that only authorized personnel have access to logistical data.
      * Data Encryption - Encrypt logistical information both at rest and during transmission to protect it from unauthorized access.
    - Long-term:
      * Identity and Access Management (IAM) System - Implement an IAM system that offers centralized control over user access and enables advanced access policies.
      * User Behavioral Analytics (UBA) - Utilize UBA tools to monitor user behavior and detect anomalies that could indicate unauthorized access or insider threats.
  + Procedure for Scenario O3:
    - Immediate: Immediately review and restrict access to logistical information to only those with a legitimate need. Revoke or modify permissions for users who do not require access.
    - Short-term: Have all employees, contractors, and drivers sign confidentiality agreements that legally bind them to protect logistical information.
    - Long-term: Data Classification and Labeling - Implement RBAC to ensure that employees, contractors, and drivers have access to logistical data based on their specific job roles.
* **Asset P Secure Foodie’s source code:**
  + Key Functions: Securing the source code of Foodie’s application.
  + Primary Asset Owner: CTO
  + Procedure for Critical Scenario P3:
    - Immediate: isolate the affected system from the network to prevent further unauthorized access and potential data breaches.
    - Short-term: make a complete backup of your database and affected systems to preserve evidence and facilitate recovery.Identify the specific areas of your code that are vulnerable to SQL injection.
    - Long-term: Implement a Web Application Firewall to help prevent future SQL injection attacks, same time continuously monitor the system for any suspicious events.
  + Procedure for Critical Scenario P2:
    - Immediate: Isolate affected systems or network segments to prevent the attacker from further intercepting or manipulating data. Determine whether a MitM attack has occurred by analyzing network traffic, logs, and other sources of information.
    - Short-term:change the credentials and key to ensure the authentication mechanisms are secure. Examine network and system logs to trace the source of the MitM attack and identify the affected systems.
    - Long-term: Ensure that all affected systems, network equipment, and software are up to date with the latest security patches and updates.Require strong authentication methods, such as multi-factor authentication.
* **Asset L GPS Route Tracking System:**
  + Key Functions: Securing the GPS route tracking system.
  + Primary Asset Owner: CTO
  + Procedure for Critical Scenario L1:
    - Immediate:Isolate and disable the affected APIs or systems to prevent further unauthorized access to GPS data.
    - Short-term: Consult with legal counsel to understand your obligations regarding data breaches, conduct a forensic analysis to determine the extent of the breach, identify vulnerabilities that were exploited, and establish a timeline of events.
    - Long-term: implementing stricter data retention policies, and anonymizing or pseudonymizing user data where possible. Implement robust security measures for your GPS route tracking APIs.

# 

# 

# 

# Regular Review and Ongoing Maintenance

To ensure that the Business Continuity Plan (BCP) remains current, effective, and aligned with Foodie's operational landscape and strategic objectives.

1. Frequency of Review: The BCP will undergo a formal review annually. However, reviews can be triggered by significant changes in business operations, after the occurrence of a disaster or a major incident.
2. Stakeholders Involved:
   1. CEO (Chief Executive Officer) 47905085 Hasanul Banna
   2. CFO (Chief Financial Officer) 48038679 Deepanshu Chandna
   3. CTO (Chief Technology Officer) 44379455 Yuchen Yang
   4. CSO (Chief Security Officer) 47765305 Shweta Hooda
   5. COO (Chief Operation Officer) 47901306 Jacqueline Dela Rosa
   6. Head of Governance 48089133 Md Shimul Hossain
   7. CIO (Chief Information Officer) 46139206 Guangye Li
3. Documentation: All changes, updates, and reviews will be documented and archived.

| Entry # | Date & Time | Updated by | Reasons for update | Change description |
| --- | --- | --- | --- | --- |
| 1 | 19/10/2023 | CIO: Guangye Li | To make what critical business activities and critical loss of risks more clear. | Add descriptions of “What is Foodie’s critical business activity” and “What risks would be considered to have a critical impact on business continuity” |
| 2 | 20/10/2023 | COO: Jacq Dela Rosa | Added BCP for Operations | Add BCP details for Operations |
| 3 | 20/10/2023 | HOG: Md Shimul Hossain | Added BCP | Added details of BCP |
| 4 | 20/10/2023 | CEO: Hasanul Banna | Added BCP operations | Elaborate the BCP details |
| 5 | 20/10/2023 | CTO:Yuchen Yang | Update critical loss of identified risk scenario, also provide business continuity strategies for Foodie | Add business continuity strategies tailored to address potential impacts arising from identified information assets L, P |
| 6 | 20/10/2023 | CFO: Deepanshu Chandna | To make critical business activities and potential risks more clear | Elaborating BCP details for different aspects of the business. |