FLIGHT BITE KNIGHTS

Delivering flavor at mach speed!

Business Continuity Plan

July 2nd, 2025

Table of Contents

DOCUMENT INFORMATION

Date of publication: 6-30-2025
Version number: Version 1.0
Plan owner: Corneil Sanders

Business Continuity Plan Team and Document Distribution List

The following individuals should be notified by email of any changes to this plan:

Name	Position	Contact
Corneil Sanders	CEO	tasteslikechicken@gmail.com
Julie A. Child	Head of Operations	queencusine@aol.com
Jordan Ramzi	HR	notasoupnazi@gmail.com

ABOUT THE COMPANY

Flight Bite Knights is an online food ordering and delivery service that primarily uses drones for its deliveries and can venture to areas that are often inaccessible to other delivery services.

EXECUTIVE SUMMARY

Flight Bite Knights ensures uninterrupted service to customers relying on drone deliveries, especially in geographically challenging locations. This Business Continuity Plan outlines the necessary strategies, impact analysis, and disaster recovery steps to maintain operations during disruptions like cyberattacks, drone failures, natural disasters, or system outages. This plan also addresses breach of airspace rules, privacy violations, noise regulations.

Objectives of the plan

This document serves as a reference tool for the actions required immediately following an incident or emergency that threatens to disrupt normal business operations.

This plan will help staff to respond to incidents by:

- Respond to incidents
- Maintain critical operations during a disruption.
- Ensure safety of customers, staff, and drone equipment.
- Restore full functionality within targeted recovery time.
- Minimize financial, reputational, and legal impacts.

Scope of the plan

The plan illustrates the actions that can be taken to minimize the disruption to normal business operations caused by the following events:

- Physical Incidents:
  - Drone Malfunction or Crash
  - Theft or Physical Tampering
  - Regulatory Non-Compliance
  - Environmental Hazards

- Cyber Incidents:
  - Drone Hijacking (GPS Spoofing / Signal Jamming)
  - Customer Data Breaches
  - Mobile App or Backend Exploits
  - Cloud or Platform Downtime (Denial of Service)

OVERVIEW

To create the best recovery procedures following an incident, a quantitative and qualitative Business Impact Analysis (BIA) was conducted.

The Business Impact Analysis is important as it sets out clearly and in written form what the critical elements of your business are, how long the business can go without them, how quickly you need to recover them, and the prioritization of recovery. It can be found following this chapter of definitions.

GLOSSARY

[This table provides a consistent and commonly agreed set of definitions for terms used in the plan. Customise this list to suit your business.]

Business Continuity Plan	A document containing all the information required to ensure that your business is able to resume critical business activities should a crisis/disaster occur.
Business Continuity Planning	A process that helps develop a plan document to manage the risks to a business, ensuring that it can operate to the extent required in the event of a crisis/disaster.
Business Impact Analysis	The process of gathering information to determine basic recovery requirements for your key business activities in the event of a crisis/disaster.
Recovery Point Objective (RPO)	The maximum acceptable data loss, expressed as a period of time, from the last good backup to the point of failure.
Recovery Time Objective (RTO)	The time from which you declare a crisis/disaster to the time that the critical business functions must be fully operational in order to avoid serious financial loss.
Resources	The means that support delivery of an identifiable output and/or result. Resources may be money, physical assets, or most importantly, people.
Risk Management	The process of defining and analysing risks, and then deciding on the appropriate course of action in order to minimize these risks, whilst still achieving business goals.

BUSINESS IMPACT ANALYSIS (BIA)

Qualitative Impact Analysis

Business Function	Impact If Disrupted	Description
Drone Dispatch & Navigation	**Severe**	Inability to deliver orders leads to revenue loss, reputational damage, and customer churn.
Online Ordering Platform	**High**	Customers cannot place orders, resulting in immediate loss of sales and long-term trust.
Payment Gateway	**High**	Inability to process payments halts all revenue.
Vendor Communication Systems	**Moderate**	Restaurant order delays and errors lead to inefficiencies.
Customer Service	**Moderate**	Poor communication during disruption worsens customer dissatisfaction.

Quantitative Impact Analysis

Business Function	Daily Revenue Impact	Downtime Tolerance	RTO	RPO
Drone Delivery	**$25,000**	2 hours	1 hour	15 minutes
Ordering Platform	**$15,000**	1 hour	30 minutes	15 minutes
Payment Gateway	**$10,000**	15 minutes	10 minutes	0 minutes
Customer Support	**$2,000**	4 hours	2 hours	30 minutes
Restaurant Partner Portal	**$5,000**	3 hours	1 hour	30 minutes

RISKS, IMPACT, AND RECOVERY STRATEGIES

Being an online drone-based food delivery service, Flight Bite Knights operates at the intersection of physical logistics and digital infrastructure. This has led to some amazing moments of ingenuity; however, it also exposes us to unique and overlapping physical and cyber risks.

PHYSICAL RISKS

Drone Malfunction or Crash

Causes

Hardware failure, software bugs, battery issues, extreme weather, birds, signal interference.

Impacts

Property damage, injury, food loss, legal liability, reputational damage.

Severity Rating Medium

Likelihood of Occurrence Low

Recovery Strategies

Routine maintenance and pre-flight diagnostics. Redundant systems (e.g., fail-safes, emergency landing). Use weather forecasting integrations and auto-abort in bad weather. Avoid high-risk areas with geofencing.

Theft or Physical Tampering

Causes

Drones can be stolen, hijacked, or tampered with when landing or in low flight zones.

Impacts

Lost inventory, data breach (if onboard systems store info), customer distrust.

Severity Rating Critical

Likelihood of Occurrence Low

Recovery Strategies

Use tamper-proof casings and GPS-based live tracking. Limit landing to secure and verified delivery zones. Equip drones with cameras and sirens to deter theft. Rapid geofencing lock-down if drone goes off-course.

Regulatory Non-Compliance

Causes

Breach of airspace rules, privacy violations, noise regulations.

Impacts

Legal penalties, grounded operations, reputational risk.

Severity Rating High

Likelihood of Occurrence Low

Recovery Strategies

Work closely with aviation authorities (e.g., FAA, EASA). Utilize real-time compliance monitoring tools. Build a robust flight permission and logging system.

Environmental Hazards

Causes

Lightning, wind gusts, bird strikes, tree collisions.

Impacts

Drone damage, public safety risks.

Severity Rating Medium

Likelihood of Occurrence Low

Recovery Strategies

Build drones with rugged, weather-resistant materials. Include LiDAR/obstacle detection. Use AI-powered weather and flight path prediction.

CYBER RISKS

Drone Hijacking (GPS Spoofing / Signal Jamming)

Causes

Attackers spoof GPS signals or jam communication.

Impacts

Loss of control, crash, rerouting to steal goods, data breaches.

Severity Rating Critical

Likelihood of Occurrence Low

Recovery Strategies

Use encrypted control signals and anti-jamming tech. Integrate inertial navigation systems (INS) as backup. Constant telemetry monitoring with automated alerts.

Customer Data Breaches

Causes

API vulnerabilities, weak access controls, poor encryption.

Impacts

Legal/regulatory fines, customer trust loss, lawsuits.

Severity Rating High

Likelihood of Occurrence Low

Recovery Strategies

End-to-end encryption of customer and delivery data. Role-based access control and regular audits. Use secure authentication protocols (OAuth2, MFA).

Mobile App or Backend Exploits

Causes

Code injection, exposed APIs, outdated libraries.

Impacts

Service disruption, impersonation, price manipulation.

Severity Rating Critical

Likelihood of Occurrence Low

Recovery Strategies

Regular penetration testing and code reviews. Secure DevOps (DevSecOps) practices. API gateway with rate limiting and threat detection.

Cloud or Platform Downtime (Denial of Service)

Causes

DDoS attacks, cloud service outages, DNS poisoning.

Impacts

Delivery delays, order loss, revenue loss.

Severity Rating High

Likelihood of Occurrence Low

Recovery Strategies

Use CDN and DDoS protection (e.g., Cloudflare, AWS Shield). Multi-cloud redundancy and offline flight modes. Build in failover paths and queuing systems.

CHECKLIST – IMMEDIATE ACTIONS FOLLOWING INCIDENT OR EMERGENCY

1. Incident: Drone malfunction or crash

Action: Determine location, enable auto-abort and emergency landing features.

Confirm:
- Who completed the task(s):
- Time:
- Date:
- Other relevant information:

2. Incident: Theft or Physical tampering

Action: Enable cameras, stealth GPS tracking, and sirens.

Confirm:
- Who completed the task(s):
- Time:
- Date:
- Other relevant information:

3. Incident: Regulatory Non-compliance

Action: Contact the proper authorities. After determining location, enable real-time compliance tools.

Confirm:
- Who completed the task(s):
- Time:
- Date:
- Other relevant information:

4. Incidident: Environmental Hazards (Lightning strikes, high winds, unexpected collisions, animal interference)

Action: Enable auto-abort and emergency landing features. Ensure LiDAR/obstacle detection is enabled. If possible, get damage report.

Confirm:
- Who completed the task(s):
- Time:
- Date:
- Other relevant information:

5. Incident: Drone Hijacking (GPS Spoofing / Signal Jamming)

Action: Enable auto-abort and emergency landing. Activate all anti-theft features. Sirens, lockdown mode, etc. Scan systems. After recovery, reestablish signal and continue delivery.

Confirm:
- Who completed the task(s):
- Time:
- Date:
- Other relevant information:

6. Incident: Customer Data Breaches

Action: Notify key personnel. Lock all affected accounts and systems. Run diagnostic scans. After securing data and accounts, update authentication process and firewalls.

Confirm:
- Who completed the task(s):
- Time:
- Date:
- Other relevant information:

7. Incident: Mobile App or Backend Exploits

Action: Isolate compromised system, determine the extent of the damage, mitigate countermeasures, strengthen authentication.

Confirm:
- Who completed the task(s):
- Time:
- Date:
- Other relevant information:

8. Incident: Cloud or Platform Downtime (Denial of Service)

Action: Contact server providers. Analyze attack, implement mitigation strategies, reroute traffic, limit requests, adjust firewall settings, disable impacted applications, assess damage. Recover from backups. Finally, restart systems and services.

Confirm:
- Who completed the task(s):
- Time:
- Date:
- Other relevant information:

COMPANY COMMUNICATION POLICY AND PROCEDURES

For Staff and Suppliers of Flight Bite Knights
Effective Date: 7/2/2025
Last Reviewed: 6/30/2025

1. Purpose

This policy outlines the communication standards, expectations, and procedures for internal and external communication at Flight Bite Knights. It is designed to ensure consistent, clear, and professional communication among staff, suppliers, and partners to support operational efficiency and excellent customer service.

2. Scope

This policy applies to:

- All employees of Flight Bite Knights (full-time, part-time, and contract)
- All suppliers and service providers with whom we have an agreement

3. Objectives

- Promote clear and timely communication
- Foster collaboration between staff and suppliers
- Protect confidential and sensitive information
- Minimize miscommunication and operational delays
- Maintain a consistent brand voice and professionalism

4. Communication Channels

Channel	Purpose	Audience
Email	Formal communication, documentation, reporting	Staff, Suppliers, Management
Internal Messaging (e.g., Slack, Teams)	Real-time updates, coordination, quick questions	Staff
Company App/Portal	Shift schedules, delivery updates, announcements	Staff (Drivers, Dispatchers)
Phone/VoIP	Urgent issues, escalations, customer service	Staff, Suppliers, Customers
Video Calls (Zoom, Meet)	Meetings, training sessions, supplier check-ins	Staff, Suppliers
SMS/WhatsApp	Backup or emergency communication	Staff, Select Suppliers

5. Communication Responsibilities

5.1. Staff

- Respond to internal messages and emails within 24 hours (or sooner if marked urgent).
- Use approved communication tools only.
- Keep tone professional and courteous in all written and verbal interactions.
- Report communication breakdowns or issues to their manager.

5.2. Suppliers

- Notify Flight Bite Knights promptly about delays, shortages, or operational issues.
- Use email for order confirmations, delivery notices, and invoices.
- Maintain open lines of communication during operational hours.

6. Confidentiality and Data Protection

- All communication must comply with the company's Data Protection Policy.
- Confidential information (e.g., customer data, delivery routes, pricing) must not be shared without authorization.

7. Communication Protocols

7.1. Incident Reporting

- Staff must report operational issues (e.g., failed deliveries, drone malfunctions) via the internal portal or to the supervisor immediately.
- Suppliers must inform the Supply Manager of any service disruptions or quality issues.

7.2. Feedback and Escalation

- Concerns or disputes should be raised through the appropriate supervisor or manager.
- Escalations must follow the internal chain of command.

7.3. Customer Interaction (Staff Only)

- Be polite, clear, and helpful.
- Never promise what cannot be delivered.
- Direct unresolved issues to the Customer Support Lead.

8. Monitoring and Enforcement

- Communication may be monitored to ensure compliance with this policy.
- Violations may result in disciplinary actions, including termination of contracts or employment.

9. Review and Updates

This policy will be reviewed annually or as needed based on operational or technological changes.

10. Acknowledgment

All staff and suppliers must read and acknowledge this policy before commencing work.

TESTING THE PLAN

Testing the BCP requires some centralized coordination, usually by the BCP coordinator or team. The team or coordinator is responsible for overseeing the accomplishment of targeted objectives and following up with the appropriate areas on the results of the test.

Generally, it is advisable to have the maximum number of personnel that will be involved in implementing the BCP also participate in the test. This participation increases awareness, buy-in, and ownership in achieving successful BCP implementation. It is also advisable to rotate personnel involved in testing to prepare for the loss of key individuals, both during a disaster and as a result of retirements, promotions, terminations, resignations, or re-assignment of responsibilities.

The involvement and oversight of independent staff such as auditors will help to ensure the validity of the testing process and the accuracy of the reporting.

TEST RESULTS

A useful test can only be achieved if the test results are analyzed and compared against stated objectives and acted upon. Management should report the test results and the resolution of any problems to the board. Management reports should consider all the test results.[1]

Test analyses should include:

- An assessment of whether the test objectives were completed
- An assessment of the validity of test data processed
- Corrective action plans to address problems encountered
- A description of any gaps between the BCP and actual test results
- Proposed modifications to the BCP
- Recommendations for future tests

[1] *FFIEC IT Examination Handbook* (March 2003), p. 20.

UPDATING A BUSINESS CONTINUITY PLAN

A Business Continuity Plan is a "living" document; changing in concert with changes in the business activities it supports. The plan should be reviewed by senior management, the planning team or coordinator, team members, internal audit, and the board of directors at least annually.

As part of that review process, the team, or coordinator should contact business unit managers throughout the financial institution at regular intervals to assess the nature and scope of any changes to the institution's business, structure, systems, software, hardware, personnel, or facilities. It is to be expected that some changes will have occurred since the last plan update. Software applications are commercially available to assist the BCP coordinator in identifying and tracking these organizational changes so that the BCP can be updated.

All such organizational changes should be analyzed to determine how they may affect the existing continuity plan, and what revisions to the plan may be necessary to accommodate these changes. The agencies expect that BCP updates will be documented to show that the plan reflects the institution, as it currently exists. Lastly, the financial institution should ensure the revised BCP is distributed throughout the organization. [2]

Scheduled Update	Plan Version

[2] *FFIEC IT Examination Handbook* (March 2003), p. 21.