Nesky Aerospace. Business Continuity Plan



NESKY AEROSPACE

BUSINESS CONTINUITY PLAN.

Nesky Aerospace. Business Continuity Plan

Table of Contents ………………………………………………………………………… 2

Executive Overview ……………………………………………………………………… 3

Document Change Control ………………………………………………………………. 4

Introduction ……………………………………………………………………………… 5

Risk Assessment Matrix …………………………………………………………………. 6

Critical Business Function ………………………………………………………………. 9

Company Organizational Chart ………………………………………………………… 10

Nesky Aerospace. Business Continuity Plan

**EXECUTIVE OVERVIEW**

At NESKY, we are a diverse team of designers, engineers and researchers. We manufacture, we produce, and we test. We work alongside our customers and partners to develop a robust business strategy that involves engineering, digital technology, research and development and supply chain management that helps us to dream, design and deliver solutions that redefine the future of the airline and airport operations as well as passenger experiences.

Progress defines the future and the future defines us.

This Business Continuity Plan is to maintain the company’s business functions in the event of a disruption and an emergency, and it applies to its subsidiaries, all employees and all locations.

This document provides a framework, guidance and concept of operations to support the company’s business to continue operating during & after a disruption, restoring the critical business functions to its normal operations as well as outlines the approach for supporting the company’s critical business functions, the order of succession, communication methods & notification procedures, defines the roles & responsibilities of the employees, provisions for alternate work locations, and the plan for maintaining and restoring access to vital records, all in the event of any of loss of access to parts of or the entire facility, loss of services due to an exodus of employees and loss of services due to equipment or systems failure.

Nesky Aerospace. Business Continuity Plan

**Document Change Control**

This is expected to maintain the integrity, accuracy and reliability of our critical documents by managing any modifications, revisions or updates to the documents and ensure our compliance with regulations and standards.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Project Name** | **Requested By** | **Date of Request** | **Change/Review** | **Review No.** | **Approved By** | **Approval Date** |
| Manufacturing Employee System | Nick S. | 07/26/24 | Movement of planning from one unit to another. | 636-073/AL | Adrian W. | 10/01/24 |
| Patch Management | Fulton D. | 04/08/24 | Introduction of semi-automatic patching from the use of fully automatic tools. | 999-042/IT | Alan N. | 04/25/24 |
| Database Management | Luke G. | 02/29/24 | The use of parameterized queries and input validation to prevent SQL injections. | 999-024/IT | Josh P. | 04/01/24 |
| Resource Management | Aricelli M. | 11/21/23 | Splitting of the HR department into two units of Employee Relations and Career Advice & Promotions. | 724-113/HR | Haley G. | 01/31/24 |

Nesky Aerospace. Business Continuity Plan

**INTRODUCTION**

**Overview**

Continuity Planning ensures the company’s business can continue or immediately resume the functions that support the mission, comply with legal requirements, and support the safety of lives & assets, in every situation. This includes natural, technological, and man-made incidents, as well as incidents that result in loss of access to parts of or an entire facility or loss of service due to equipment or systems failure. The benefit of continuity planning includes the ability to predict response actions, improve the business performance of its critical business functions, and ensure prompt recovery.

**Plan Scope & Applicability**

The scope of this plan covers Nesky Aerospace. The plan is applicable after the verification of the safety of everyone present within the facility at the time of any incident that will make the facility inaccessible is ascertained. It can be active at any time before, during, or after business hours, with or without warning.

**Plan Objectives**

The Nesky Aerospace Business Continuity Plan objective is to expedite the resumption of critical operations and business functions in a timely & organized manner with the assurance of the welfare and safety of everyone and the protection & accessibility of vital records in all situations.

**Plan Assumptions**

The assumptions below were used in creating this Business Continuity Plan:

* There has been an occurrence that affected normal operations.
* The facility has experienced limited or no access.
* Inaccessibility to documents and equipment within the facility.
* Availability of employees to continue operations.

Nesky Aerospace. Business Continuity Plan

**RISK ASSESSMENT**

This is for the identification and evaluation of the risks associated with our operations, practices and processes. It will allow us to determine the likelihood of the risks occurring and the impact it will have on our business if it happens.

The risks identified over the cause of doing business are:

1. Project Management risks – (a) Poor project plan

(b) Employee unavailability

(c) Inaccurate estimates

(d) Poor communication

1. Engineering risks – (a) Changes in regulations and standards

(b) Accidents in manufacturing processes

(c) Defective parts, poor quality parts from vendors

3. Political & Economic risks – (a) Volatility in politics

(b) Inflation rate

4. Supply chain risks – (a) Poor quality of products

(b) Delayed delivery

5. Customer satisfaction

6. Cyber risks – threats, vulnerabilities, attacks

**RISK MATRIX**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **LOW** | **MEDIUM** | **HIGH** |
| **Unlikely** |  |  | 3 |
| **Possible** | 1, 2 | 4 |  |
| **Likely** | 6 |  | 5 |

Nesky Aerospace. Business Continuity Plan

1. **Project Management Risks**

The likelihood of this occurring is once every six months because we review an existing project or take on new projects in six months.

Our assets are in the range of $800000 to $1300000, therefore the approximate asset value is $1000000.

The exposure factor is low because of the efforts we put into managing the risks, which makes the impact minimal as well. The estimate for this is about 10 percent.

Therefore: -

The annualized rate of occurrence of project management risks is – 2/1 = 2.

The Single Loss Expectancy = Asset Value (AV) \* the Exposure Factor (EF)

= 1000000 \* 0.1 = $100000. There will be about a hundred thousand dollars loss experienced if there is any occurrence of a poor project plan, employee unavailability, inaccurate estimates or poor communication.

The Annualized Loss Expectancy = SLE \* ARO

= $100000 \* 2 = $200000.

1. **Engineering Risks**

The likelihood of engineering risks is once every year. ARO = 1/1 = 1.

The exposure factor is 40%, hence Single Loss Expectancy = 1000000 \* 40%. = $400000.

ALE = SLE \* ARO = 400000 \* 1 = $400000.

1. **Political & Economic Risks.**

The likelihood of occurrence is every four years. ARO = ¼ = 0.25.

Its exposure is high since we can absolutely do nothing about it. = 80%

SLE = 1000000 \* 0.8 = $800000.

ALE = 800000 \* 0.25 = $200000

1. **Supply Chain Risks.**

With the implementation of lean manufacturing and Just In Time, product defects are very low with the probability of escaping to the market even lower, hence the likelihood of a risk has been pecked to about one occurrence every year and the exposure is about five percent. Therefore ARO = 1/1 = 1 and SLE = 1000000 \* 0.05 = $50000.

ALE = ARO \* SLE = 1 \* 50000 = $50000.

Nesky Aerospace. Business Continuity Plan

1. **Customer Satisfaction.**

This is a critical factor in our risk assessment because of its likelihood of happening and the impact it will have on our reputation. The occurrence has been found to be like one every month. Therefore, ARO is twelve. The exposure factor is 85% which makes the SLE to be

1000000 \* 0.85 = $850000.

ALE = 850000 \* 12 = $10200000.

1. **Cyber Risks.**

The likelihood of occurrence in the organization is once every three years, with the impact very high if it happens and an exposure factor of 50%.

Therefore ARO = 1/3 = 0.33

SLE = 1000000 \* 0.5 = $500000.

ALE = 500000 \* 0.33 = $165000.

Nesky Aerospace. Business Continuity Plan

**Part 1. Issue-Specific Security Policies.**

1. BYOD
   * Issue Statement: The use of personal devices on the company’s network can cause breach of data and unauthorized access to the network.
   * Company’s Position: It is only permitted to use personal devices on the company’s network after strict compliance with the security controls as dictated by the security department.
   * Applicability: This policy applies to all employees, vendors, contractors and every other third-party user who accesses the company’s network using their personal devices.
   * Roles and Responsibilities: (a) Employees are to ensure personal devices comply with every security requirement. (b) The IT and Security departments will implement and enforce security controls for personal devices. (c) The management at all levels should monitor compliance and deal with violations on time and decisively.
   * Compliance: Compliance to the security requirements of the use of personal devices is non-negotiable with violations punishable with disciplinary actions, including termination of network access privileges and up to termination of employment.

* + Points of Contact: IT Support – infotech.support@nesky.com

Security Administrator – [secure.adminsupport@nesky.com](mailto:secure.adminsupport@nesky.com)

* + Supplementary Information: Refer to the employee handbook BYOD security guidelines or the website <https://nesky.com/onboarding/securityguidelines> for detailed requirements.

1. Internet Access
   * Issue Statement: Indiscriminate and unnecessary internet access can lead to security vulnerabilities and productivity issues.
   * Company’s Position: Internet access is provided for business purposes only, with monitoring and auditing to prevent misuse.
   * Applicability: This policy applies to every user of the company’s internet.
   * Roles and Responsibilities: (a) Employees are to use the internet responsibly and for official purposes only. (b) The IT and Security departments will monitor and filter internet usage. (c) The management will review internet usage reports and address issues.
   * Compliance: Violations to the responsible usage of the internet may result in restricted internet access or one working week suspension or both.
   * Points of Contact: IT Support – infotech.support@nesky.com

Security Administrator – [secure.adminsupport@nesky.com](mailto:secure.adminsupport@nesky.com)

Nesky Aerospace. Business Continuity Plan

* + Supplementary Information: Refer to the internet usage policy document or the website <https://nesky.com/internetusage> for detailed guidelines.

1. Personal Use of Company Equipment
   * Issue Statement: The personal use of the company’s equipment can cause damage to the equipment, reduced productivity, poor quality of products and security risks.
   * Company’s Position: Company’s equipment is to be used strictly for business purposes with any other use outside of business purposes to be authorized by the security administrator and department manager.
   * Applicability: This policy applies to all employees and contractors using the company’s equipment.
   * Roles and Responsibilities: (a) Employees are to ensure non-personal use of the company’s equipment except authorized. (b) The Engineering and Security departments will monitor equipment usage and enforce policies. (c) The management will ensure compliance with the policy and address policy violations.
   * Compliance: Non-compliance may result in disciplinary actions, including loss of equipment privileges.

* + Points of Contact: Engineering Manager – [facilities.support@nesky.com](mailto:facilities.support@nesky.com)

Security Administrator – [secure.adminsupport@nesky.com](mailto:secure.adminsupport@nesky.com)

* + Supplementary Information: Refer to the employee handbook for equipment usage policy or the website <https://nesky.com/equipmentusagepolicy> for guidance.

1. Removal of Company Equipment from the Premises
   * Issue Statement: The removal of company equipment or property from the premises can lead to intellectual theft and loss of privacy.
   * Company’s Position: Permission is only given to authorized contractors to remove company equipment under security supervision.
   * Applicability: This policy applies to all employees and contractors handling company equipment.
   * Roles and Responsibilities: (a) Except authorized and under security supervision, no employee may remove company equipment. (b) The Engineering and Security departments will track and monitor equipment removal. (c) The management will approve equipment removal requests and oversee a proper removal.
   * Compliance: Unauthorized removal of company equipment may result in disciplinary actions, including and up to termination of employment.

* + Points of Contact: Engineering Manager – [facilities.support@nesky.com](mailto:facilities.support@nesky.com)

Security Administrator – [secure.adminsupport@nesky.com](mailto:secure.adminsupport@nesky.com)

Nesky Aerospace. Business Continuity Plan

* + Supplementary Information: Refer to the facility and equipment handling policy document or the website <https://nesky.com/equipmenthandling> for guidelines.

1. Use of Unofficial Software
   * Issue Statement: The use of unofficial software can increase the risk of security breach of the company network, security vulnerabilities and compliance issues.
   * Company’s Position: Only authorized software is permitted for use on the company’s network and systems to ensure security and compliance.
   * Applicability: This policy applies to all employees and third-party users of the company’s network and systems.
   * Roles and Responsibilities: (a) Employees are prohibited from introducing any software and are required to report any use or installation of unofficial software. (b) The IT department will maintain a list of authorized software and monitor installations. (c) The management will enforce the software usage policy.
   * Compliance: Non-compliance of this policy may result in disciplinary actions, including up to termination of access to company devices.

* + Points of Contact: IT Support – infotech.support@nesky.com

Security Administrator – [secure.adminsupport@nesky.com](mailto:secure.adminsupport@nesky.com)

* + Supplementary Information: Refer to the software usage policy document or the website <https://nesky.com/softwareusage> for guidelines.

1. Design and Development of an Information Security Awareness and Training Program
   * Issue Statement: The lack of security training and company-wide awareness can lead to increased vulnerabilities, social engineering and security incidents.
   * Company’s Position: The company is committed to developing and maintaining a comprehensive information security awareness and training program.
   * Applicability: This policy applies to all employees, vendors and contractors of the company.
   * Roles and Responsibilities: (a) Employees must participate in security awareness and training programs. (b) The Training Coordinators will develop training materials and conduct training and awareness. (c) Management will ensure participation and compliance with training requirements.
   * Compliance: Non-compliance or failure to participate in requisite training will result in disciplinary actions including and up to termination of employment.

* + Points of Contact: IT Support – [infotech.support@nesky.com](mailto:infotech.support@nesky.com)

Security Administrator – [secure.adminsupport@nesky.com](mailto:secure.adminsupport@nesky.com)

Training Coordinators – [education.training@nesky.com](mailto:education.training@nesky.com)

Nesky Aerospace. Business Continuity Plan

* + Supplementary Information: Refer to the Education and Training document or the website <https://nesky.com/management/educationandtraining> for guidelines.

**Part 2. Legal Standard Operating Policies and Procedures.**

**Incident Management Manual**

The purpose and scope of this manual is to present the legal standard operating policies and procedures for systematic handling of incidents for the purpose of business continuity and quick recovery.

Incident Management for legal compliance and operational continuity is crucial for the industry,

aerospace.

There is a commitment to safety and risk management through proper documentation and timely reporting.

Compliance and Regulations.

* + Federal Aviation Regulations (FAR) Part 21 which is the certification procedures for products and parts. It is issued by the Federal Aviation Administration (FAA).
  + International Traffic in Arms Regulations (ITAR) which controls the export and import of defense-related articles and services, including aerospace components. (FAA.gov).
  + ISO 9001 is the international standard that specifies requirements for a quality management system (QMS).
  + RTCA DO-178C provides guidelines for the development of airborne software to ensure safety and reliability and the SAE standards which are developed by the Society of Automotive Engineers which cover various aspects of aerospace engineering.

These documents by FAA and SAE provide guidelines for our best practices and ensure that our Information Security plan includes measures to comply with these standards by adequately allocating resources effectively and investing in advanced security technologies and training programs.

**Incident Types**

* 1. **Fire Evacuation**

**Industry Compliance**

OSHA Standards – Compliance with procedures for reporting a fire, emergency evacuation and employee training.

**Business Operations**

Employee training for employees responsible for critical operations.

Clear markings of evacuation routes and an adequate communication company wide.

**Training & Awareness**

Nesky Aerospace. Business Continuity Plan

Regular fire drills to ensure every employee is familiar with evacuation procedures.

Annual training on the use of fire extinguishers and other emergency equipment.

**Disaster Recovery**

Procedures for accounting for all employees.

Procedures for assessing damage.

Procedures for resuming operations as quickly as possible after an incident.

**Incident Response**

Emergency contact: Security Manager – 512 234 9876

Engineering Manager – 469 678 4321.

Email to external stakeholders, phone calls and text messages to employees.

* 1. **Ransomware Attack**

**Industry Compliance**

FISMA – A timely technical assistance and guidance on detecting and handling ransomware.

**Business Operations**

A secure and accessible backup with regular updates.

Multi-Factor Authentication and Principle of least privilege.

**Training & Awareness**

Training employees in recognition of phishing emails.

Awareness of the prohibition on the use of unofficial software.

Education on morals and ethics.

**Disaster Recovery**

Isolation of affected device.

Total wipe-off of data.

Data restoration from backup server.

**Incident Response**

Establishment and training of the Incident Response Team.

Professional reporting of security incidents.

* 1. **Power Outage**

**Industry Compliance**

Federal Energy Regulatory Commission (FERC) and NFPA 110.

**Business Operations**

Installation, operations, maintenance and servicing of backup generators and power systems.

Activation of uninterruptible power supply to continue critical operations during power outage.

**Training & Awareness**

Awareness of evacuation procedure during power failure.

Backup of power supply training for incident response team.

Nesky Aerospace. Business Continuity Plan

**Disaster Recovery**

Assess the probable damage to any equipment.

Repair any equipment as required.

If the equipment cannot be repaired, request a replacement.

**Incident Response**

Assess the list of contacts for utility companies and emergency services.

Professional reporting of the outage.

* 1. **Pandemic Situations**

**Industry Compliance**

Guideline compliance from WHO and Center for Disease and Control.

**Business Operations**

Implementation of the existing remote work policies.

Activation of support team for remote work.

Operations to be modified to comply with WHO and CDC.

**Training & Awareness**

Awareness of pandemic response and personal hygiene.

**Disaster Recovery**

The incident response team and emergency responders to ensure the health and safety of all employees.

Business operations to be maintained and supported.

**Incident Response**

Pandemic response team and emergency responders to be maintained.

Nesky Aerospace. Business Continuity Plan

**Part 3. Incident Response.**

An incident response plan has several phases which include Preparation, Detection & Analysis, Containment, Eradication & Recovery and Post-Incident Activity.

Using the NIST SP 800-61 Revision 2 as my guide, the initial phase involves acquiring the necessary tools (such as firewalls, antivirus and IDS/IPS), gathering the resources and establishing a team, defining their roles and responsibilities. The team will be trained, ensuring the team is familiar with the incident response policy. During the preparation phase, based on the results of our risk assessment conducted earlier, we will select and implement a set of controls. From the risks that will remain after implementing the controls, detection will be necessary so that whenever a breach occurs, we will be alerted. The risks or breaches will then be mitigated by containing them. After the incident has been handled, a report of the cause, impact and cost of the incident and the steps to be taken in the future if such an incident is repeated.

Actions to be taken in the event of a:

Ransomware attack on a device.

1. The attack will be identified by using some of the acquired tools, the antivirus and the Intrusion Detection System. The device will then be isolated from the network.
2. The attack will be contained within the device by disabling network access.
3. The ransomware attack will be removed from the device, the latest patches will be applied to the computer.
4. From the backups, which should be checked for non-infections, data should be restored to the computer and tests will be carried out for a probable remnant of the attack or any previously undetected infection.
5. The incident will be reviewed to understand how it occurred, if the response was adequate and how the response can be improved in case of recurrence.

Power Failure.

1. After the outage of power, the systems, computers and operations affected will be determined.
2. There will be a changeover to our backup power supply and communication will be sent out to everyone that needs to know about the power failure.
3. The cause of power outage will be determined while efforts will be made to restore power supply.
4. Every affected system or operations will be checked for proper functionality before returning them to the network or normal functions.
5. The response to the power outage will be reviewed, lessons learned will be documented and identify areas for improving response.

ISP Failure.

1. Network monitoring tools will be used to identify the failure and determine the source of failure.
2. Services, devices and users affected will be determined.
3. A backup or secondary internet connection will be utilized to maintain connectivity.

Nesky Aerospace. Business Continuity Plan

1. Every user will be informed of the failure while internet usage will be managed among users if necessary. Resolution time will be communicated too.
2. If the failure is not internal, the company will work with the provider to resolve the issue.
3. Connection to the internet through the ISP will be restored once the failure has been resolved and ensure connectivity is up for every internet-dependent device and there is proper functionality.
4. Response to this failure will be reviewed and improvements identified.

Nesky Aerospace. Business Continuity Plan

**CRITICAL BUSINESS FUNCTION**

**Overview**

In the aviation industry, airlines and airports work to provide seamless travel experience for the passengers, intertwining their operations to be optimally efficient, cost effective, safe and customer friendly. (Collinsaerospace.com).

At Nesky Aerospace, we support critical aviation needs. We understand the complex ecosystem of airlines and airports and offer products and services to optimize airport operations for passengers, airports and airlines alike.

**Function**

With AirPlan , we transform the use of data into powerful insights that improve airline and airport operations as well as passenger experiences. Airports can manage a variety of resources from a single application on any device on their network.

**Business Process**

As modern travel evolves, passengers expect a faster, easier and more seamless experience. Our all-in-one Airport Operational Database (AODB) and Resource Management System (RMS) offers integrated and intelligent solutions for passenger processing and facilitation, airport operations and baggage management. Our self-service solutions help create a seamless travel experience for a high volume of passengers.

**Lead Point of Contact.** Digital Technology director.

**Vendors and Contractors.** Rockwell and United Technologies Company

Nesky Aerospace. Business Continuity Plan

**COMPANY ORGANIZATIONAL CHART**



Chief Intelligence Officer

Tomi Talabi

Chief Operating Officer

Chief Financial Officer

Human Resources Director

Enterprise Operations Director

Financial Manager

HR Manager

Engineering Director

Digital Technology Director

Maintenance Manager

Quality Manager

Information Technology Manager

Supply Chain Manager

Materials Manager

Information Security Manager

Production Manager

Facility Manager

Security Administrator

Security Auditor

DevSecOps

**References.**

Fani, S. & Subriadi, A., 2019. Business Continuity Plan: Examining of Multi-Usable Framework, (pg. 275-282), Vol. 161, ISSN 1877-0509.

<https://doi.org/10.1016/j.procs.2019.11.124>.

Weinberg, N., 2021. Business Continuity and Disaster Recovery Planning: The Basics.

<https://www.proquest.com/trade-journals/business-continuity-disaster-recovery-planning/docview/2505032966/se-2>

Blass, G., (2022). Extended Downtime: Why You Need to Update Your Business Continuity Plan.*Journal of Health Care Compliance,*(pg. 59-62), Vol 24. <https://lopes.idm.oclc.org/login?url=https://www.proquest.com/trade-journals/extended-downtime-why-you-need-update-your/docview/2698713226/se-2>

Conklin, A., White, G., Cothren, C., Davis, R., Williams, D., 2022. Principles of Computer Security: CompTIA Security+ and Beyond (Exam SY0-601), Chapter 21. (6th ed.)

<https://www.accessengineeringlibrary.com.lopes.idm.oclc.org/content/book/>

Sokolova, V., 2024. Main Risks of Aerospace Engineering Projects: How to Implement Wise Risk Management into Your Organization.

<https://www.epicflow.com/blog/main-risks-of-aerospace-engineering-projects-how-to-implement-wise-risk-management-into-your-organization/>

<https://www.collinsaerospace.com>

FEMA Template, (n.d.).

<https://arlingtonva.s3.amazonaws.com/wp-content/uploads/2019/08/COOP-Template-Business-Continuity.pdf>

ComplianceQuest, 2024. What is Document Change Control?

<https://www.compliancequest.com/document-change-control/>

NIST SP 800-61 Rev. 2, 2012. Computer Security Incident Handling Guide.

<http://dx.doi.org/10.6028/NIST.SP.800-61r2>

CISA.gov, 2023. I’ve Been Hit by Ransomware!

<https://www.cisa.gov/stopransomware/ive-been-hit-ransomware>

Reddit.com, 2022. How to Deal with ISP Failure.

<https://www.reddit.com/r/sysadmin/comments/vtcex7/how_to_deal_with_isp_failure/?rdt=55216>

FAA.gov, 2023. Manufacturing Best Practices.

<https://www.faa.gov/aircraft/air_cert/production_approvals/mfg_best_practice>

SAE.org, 2025. SAE Aerospace Standards.

<https://www.sae.org/standards/aerospace>