NESKY Aerospace design and deliver solutions that redefine the future of the airline and airport operations as well as passenger experiences.

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 & development and supply chain management.

**MISSION STATEMENT.**

At Nesky Aerospace, we are committed to excellence, integrity and innovation in every aspect of our business; product development, manufacturing, customer service and community engagement by providing defense and security solutions that safeguard people and nations, ensuring peace and stability in an ever-changing world and through our work, inspire the next generation of scientists, engineers and dreamers. (Boeing.com)

**WEB APPLICATION.**

Our web application runs on the windows operating system with regular updates as needed and a monthly maintenance on the server side and can be assessed from any device through a web browser with an internet connection on [www.nesky.org](http://www.nesky.org).

**SERVERS.**

Our servers provide powerful computing, designed to manage, store and process our data in local data centers and cloud to run other services like email, Active Directory, databases, DNS and applications in other computers which are known as clients. Our servers host applications, manage our data resources and facilitate communication between clients.

**DEPARTMENTS.**

Nesky Aerospace has five departments

* Enterprise Operations
* Engineering
* Digital Technology
* Human Resources
* Finance.

**ROUTERS and SWITCHES.**

These devices in our corporate network control data flow between devices and enable access for users and services. While the routers connect the internal network to the internet, the switches connect our different devices for the purpose of communication between a department and two or more departments.

It includes physical and virtual switches, wired and wireless routers.

**REMOTE ACCESS**

The company’s remote access is designed to allow our employees who work from home to connect to the corporate network from their different locations using Virtual Private Network (VPN) and Remote Desktop Protocol (RDP) technologies. Some other essential workers who need to manage our servers and networks at non-office hours and employees who need to access files while in transit can also utilize the remote access technology.

**WIRELESS COMMUNICATION.**

For the purpose of ensuring security to our corporate network, only Wi-Fi is allowed as the only form of wireless communication, and it allows devices within the internal network to connect to the internet after the use of MFA.

**FIREWALL**

Our firewalls are security devices which are both physical and software that are designed and configured to monitor and control incoming and outgoing traffic based on a predefined set of security rules to act as a barrier between our internal network and the internet. The software firewalls are configured with Snort, an intrusion detection and prevention system and a Fortinet proxy firewall to filter requests and send back responses from users to the internet.

**DEMILITARIZED ZONE (DMZ)**

Our DMZ is a logical sub network in our local area network (LAN) that allows a barrier between our trusted corporate network and the internet and within our private and public networks. It acts as a protection layer through which outside users cannot access the company’s data thereby adding an extra layer of security.

**Introducing NIST Cybersecurity Framework.**

The step-by-step guides of NIST CSF are:

* Identify: - we need to carry out the inventory of all resources; hardware, software, data & network and understand the importance of each resource and the potential impact of any risk occurrence. We then establish processes, policies and procedures to manage regulatory and legal requirements.
* Protect: - we protect the resources we identified by implementing strong access control measures, have data backup procedures, protect data through encryption, carrying out regular updates and regular patching and conduct regular training and awareness programs for every employee.
* Detect: - we need to implement continuous monitoring practices and introduce tools to detect threats as they occur, establish processes to analyze unusual activities that will indicate security incidents.
* Respond: - we develop and implement incident response plans, establish means of communication for both internal and external stakeholders during an incident, how to conduct thorough analysis of incidents to understand their impacts and implement measures to reduce incidents and mitigate their effects if incidents occur.
* Recover: - it is required of us to develop and implement recovery plans to restore data and systems affected by security incidents and an effective communication procedure with all stakeholders during the recovery process to assure them of the protection of their interests and maintain trust.

**The current risks of threats to our corporate security.**

* Vulnerability exploitation. This is when threat actors and attackers gain unauthorized access to our network through weaknesses in our network.
* Advanced Persistent Threats. This is after a vulnerability has been detected in our network and the attackers stay undetected for a very long time, allowing them to cause significant damage to us.
* Ransomware. This is when attackers get into our network, infiltrate our data, make them unavailable to us then declare a ransom for us to have access to both network and data.
* Social Engineering. This is where deceptive emails and/or messages are used to trick our employees into revealing sensitive company information.
* Insider threats. This is when an employee knowingly or unknowingly misuses their rights or an access to information to cause data breaches or create vulnerabilities. (CISA.gov)

**Plans for the protection of Intellectual Property (IP).**

* We implement a strong access control policy coupled with the encryption of data transmission that restricts access to confidential information and trade secrets to only current and authorized employees.
* We ensure employees that leave the company are removed immediately from the corporate network to prevent any unwanted breach or theft. It also affirms our zero-trust policy.
* We enforce dedicated company device usage and prevent any device or network that is not company specific.
* We need to establish a legal basis for the protection of our confidential information by ensuring incoming and outgoing employees sign a non-disclosure agreement (NDA) and make them aware of the penalties and legal implications of disclosing our IP to competitors or for personal gain.
* We carry out regular IP audits to identify and document all of our IP assets like patents, trademarks, copyrights and trade secrets. We also need to classify them based on their importance and sensitivity.
* We ensure continuous monitoring and surveillance of potential threats by using monitoring tools.
* We regularly educate employees on the importance of IP protection and best security practices.
* We adhere strictly to ISO 27001 and NIST CSF.
* The headlines on our website will read:

***Use of this site or the receipt of information from it does not grant any licenses to any copyrights, patents or any other intellectual property rights or the rights to any of the materials on the site or materials accessed by use of the site.***

**SECURITY MODEL.**

Our security model will be the foundation of our information security. It is the framework for implementing our security measures to protect sensitive data. Our model will be the **Bell-LaPadula** which focuses on confidentiality and access control. It classifies users and data into levels of top secret, secret, confidential and unclassified.

This model ensures that information flow is controlled, with higher level users only able to access lower-level information.

**ACCESS CONTROL MECHANISM and MANAGEMENT.**

Our access control model will be both role-based and attribute-based. The Role-Based Access Control (RBAC) will be based on the assignment of user roles to ensure employees have access to only the information necessary for their job and the Attribute-Based Access Control (ABAC) uses the department of an employee and their location to determine access.

Principle of least privilege will be enforced company-wide with single sign-on to simplify access and the use of Multi-Factor Authentication to enhance security.

The roles in planning and managing the security plan as it impacts cybersecurity are:

* **Board of Directors –** they will be responsible for overseeing the organization’s overall risk management strategy ensuring that the cybersecurity program is adequate and effective and approve cybersecurity budgets.
* **Senior Management –** led by the Chief Executive Officer will be responsible for integrating cybersecurity into the organization’s overall strategy. They will prioritize cybersecurity in business decisions and ensure adequate resources are allocated to cybersecurity efforts.
* **Chief Information Security Officer –** will be most senior employee that is responsible for developing & implementing the organization’s information security program and ensuring alignment with business objectives. He will create & enforce security policies and procedures, oversee incident response (IR) and disaster recovery planning (DRP).
* **IT Management –** the Chief Information Officer will be the head of IT management and will be responsible for the technical implementation and maintenance of cybersecurity measures, the security of IT infrastructure, compliance with policies and regulatory requirements and lead the response to security incidents.
* **Departmental Management –** comprising of the HR, Finance, Quality, Supply Chain, Production, Maintenance, Materials, Facility, IT and Information security managers will be responsible for ensuring that cybersecurity measures, policies and procedures are implemented within their departments, identify and manage security risks within their departments and work with security teams to address vulnerabilities.
* **Security Teams –** they will be responsible for the day-to-day operations of information security, continuously monitor systems for security breaches and vulnerabilities, respond to and mitigate security incidents and initiate training and awareness programs for employees.
* **Employees and end users –** they are the first line of defense against threats by reporting suspicious activities and potential security incidents, be involved in security training and awareness education and adhere to security policies and best practices.

**References.**

Santos, O., 2023. Developing Cybersecurity Programs and Policies. 3rd ed.

Boeing, (n.d.) General Information.

<https://www.boeing.com/company/general-info>

NIST.gov, 2024. Cybersecurity Framework.

<https://www.nist.gov/cyberframework>

CISA.gov, 2025. Cyber Threats and Advisories.

<https://www.cisa.gov/topics/cyber-threats-and-advisories>