**Non-Functional Requirements**

**For**

**Airlines Website:**

# **Performance**:

## Page Load Times:

* The website should load pages within 2-3 seconds for users with a broadband connection
* The homepage, including static content and dynamic content, should be fully interactive within 3 seconds when accessed on a 4G mobile network.

## Search Response Times:

* Search queries on the website should return results within 5 seconds under normal load conditions.
* During peak times, the search response should not exceed 10 seconds.
* The system should handle data processing and transactions (e.g., booking a flight) within an acceptable timeframe that does not detract from the user experience, and this will be determined during the User Acceptance Testing.

# **Scalability:**

* The website should maintain its performance benchmarks as the number of connected users increases to a specified target (e.g. 10,000 connected users), also, should be capable of scaling up resources automatically to meet increases in demand without manual intervention (Back End).
* Data Fetching: the database and application servers should handle an increase in transaction volumes in accordance with the growth of the user base or data size

# **Portability:**

* The website should be fully functional on personal computers including desktops and laptops across platforms such as Windows (Windows 10 and above), macOS (macOS Catalina and above), and Linux distributions (Ubuntu, Fedora).
* The website must operate effectively on mobile devices such as smartphones and tablets with Android (Android 10.0 and above) and iOS (iOS 13 and above) operating systems.
* For wearable technologies, the website should display and function correctly on devices like Apple Watch (watchOS 6 and above) and Samsung Galaxy Watch (Tizen 4.0 and above) through their web browsing capabilities.
* The site should be tested for compatibility with the major web browsers like Chrome, Firefox, Safari, and Edge, as well as ensuring functionality on previous versions.

# **Compatibility:**

* The Website should not conflict with the operation of other applications, nor should it be negatively impacted by other software running on the same device.
* It must adhere to industry-standard protocols and data formats to ensure the compatibility with third-party services and APIs.
* The website should integrate smoothly with different payment gateways, reservation systems, Frequent Flyer system, and customer relation management systems without conflicts.

# **Reliability:**

* The website should have a high mean time between failures, in other words, operating an average of 10,000 hours before a failure occurs.
* Critical failures that cause system outages should be rare, not exceeding a defined threshold (1 Critical per 2 months).

# **Maintainability:**

* The website should be designed to facilitate easy updates and bug fixes, ideally without significant downtime (e.g. using rolling updates).
* The code should be well-documented and adhere to coding standards to ease updating efforts.

# **Availability:**

* The website should aim for high availability, with a target uptime percentage (99.9% uptime excluding scheduled maintenance).
* The website should feature redundancy and failover processes to minimize downtime.
* Scheduled maintenance windows should be minimized and occur during off-peak hours, with advance notice provided to users.

# **Security:**

## Data Encryption:

Sensitive data stored in databases should be encrypted at rest.

## Authentication and Authorization:

* Multi-factor authentication should be implemented for an additional layer of security.
* The principle of least privilege should be applied, ensuring users have the minimum access necessary to perform their tasks.

## Security Compliance:

Regular security audits should be conducted, and the website should have a certification of compliance and security where necessary.

## Vulnerability Management:

* If it’s possible, the website should undergo regular security vulnerability assessments.
* Patches and updates for the website and its dependencies should be applied in a timely manner to mitigate known security risks.

## Incident Response:

* An incident response plan should be in place, detailing steps to be taken in the event of a security breach.
* Regular simulations of breaches should be conducted to ensure preparedness.

## User Data Protection:

* Personal user data should be stored according to privacy standards and should only be used for intended purposes as agreed by the user.
* Users should have the ability to manage their data, including viewing and updating their information.

# **Usability:**

* The user interface UI should be intuitive and user-friendly, requiring minimal training or technical knowledge to navigate and use effectively.
* Employees and users feedback should be gathered regularly to inform improvements in UI/UX design.
* Accessibility should be a priority, ensuring the website is usable by individuals with disabilities.