**Skybot Web Portal**

*Software project*

| **Project name** | **Date** | **Version** | **Author** |
| --- | --- | --- | --- |
| Skybot Web Portal | 03.07.2024 | 1.0 | Oleksandra Solodka |

**Table of Contents**

# 1. Introduction

1.1 Purpose

1.2 Scope

1.3 Definitions, Acronyms and Abbreviations

2. Overall Description

3. Test coverage

3.1 Functional Testing

3.2 Performance Testing

3.3 Security Testing

3.4 Usability Testing

4. Test Environment

4.1 Operating Systems

4.2 Mobile

4.3 Browsers

5. Entry criteria/Exit criteria

6. Risks and Contingencies

**Software Requirements Specification**

**1. Introduction.**

Skybot is a company in the sale and servicing of electric transport. The company aims to develop, test and implement a B2C portal that will enhance its customer engagement and streamline its online sales and service operations. As part of our commitment to delivering reliable solution, we are tasked with creating a test plan to ensure the new portal meets all functional and non-functional requirements.

### **1.1 Purpose**

The purpose of this test plan is to outline the testing strategy, objectives and scope for the Skybot B2C portal. The primary goals of the testing effort are to ensure the quality, functionality, performance, and security of the portal. This involves identifying and addressing defects early in the development cycle to ensure a seamless user experience upon launch.

In the context of this project, testing is crucial for validating that the portal meets all specified requirements and provides a reliable and user-friendly platform for Skybot's customers. Effective testing will help mitigate risks, enhance customer satisfaction, and support Skybot’s business objectives by delivering a high-quality product that aligns with their brand values and operational goals.

**1.2 Scope**

The scope of this test plan covers the testing activities for the Skybot B2C portal development project. This includes testing the portal’s functionality, performance, security and user experience.

**1.3 Definitions, Acronyms and Abbreviations**

B2C - Business-to-Consumer

SQL injection - is a type of cybersecurity vulnerability that occurs when an attacker injects malicious SQL (Structured Query Language) code into a query input.

XSS - Cross-Site Scripting is a type of cyber attack that involves injecting and executing malicious JavaScript code on a web page or web application through inadequate handling of input data.

CSRF (Сross-Site Request Forgery) - a type of security exploit where an attacker tricks a user's web browser into making an unwanted request to a web application for which the user is authenticated

**2. Overall Description**

The Skybot B2C portal project is an initiative to develop an online platform that facilitates the sale and servicing of electric transportation products directly to consumers. The primary goal of this portal is to enhance Skybot's customer engagement, streamline online sales processes, and provide exceptional post-purchase support. This project encompasses the design, development, testing, and implementation of a user-friendly and secure web portal that meets the diverse needs of Skybot's customers. The website should be responsive on various mobile devices and desktops with a minimalist design. Users should be able to view each product, add items to their cart, place orders, write reviews and upload photos or videos, as well as schedule service appointments after purchasing a product and book test drives.

**3. Test coverage**

**3.1 Functional Testing:**

* + User registration and login processes.
  + Product catalog browsing and searching.
  + Detailed product descriptions and specifications.
  + Shopping cart functionality.
  + Order placement and checkout process.
  + Payment processing and confirmation.
  + User reviews and feedback mechanisms.
  + Appointment scheduling for test drives.
  + Service center appointment scheduling.

**3.2 Performance Testing:**

* + Load testing to evaluate portal performance under expected user load.
  + Stress testing to determine the portal's ability to handle peak loads.
  + Response time and throughput analysis.

**3.3 Security Testing:**

* + Verification of secure user authentication and authorization.
  + Testing for vulnerabilities such as SQL injection, XSS and CSRF.
  + Ensuring secure payment processing and data protection.

**3.4 Usability Testing:**

* + Evaluation of user interface design and navigation.
  + Testing the mobile version of the portal for responsiveness and usability.
  + Accessibility testing to ensure compliance with accessibility standards.

**3.5 Exclusions from the Scope:**

* Testing of any third-party integrations not developed by the Skybot team.
* Performance testing under extremely rare or unrealistic conditions.
* Any future features or enhancements not included in the current project phase.

### 

### **4. Test Environment**

#### **4.1 Operating Systems:**

Windows 10\11, Ubuntu 20+, MacOS Monterey

**4.2 Mobile:**

iOS, Android

#### **3.3 Browsers:**

* ***Desktop Browsers:***
  + Google Chrome, Mozilla Firefoх, Microsoft Edge, Safari
* ***Mobile Browsers:***
  + Google Chrome (latest version and two previous on Android)
  + Safari (on iOS,macOS)
  + Samsung Internet Browser (latest version on Android)

**5. Entry criteria/Exit criteria**

| **Entry criteria** | **Exit criteria** |
| --- | --- |
| * Business Requirements signed off by stakeholders * Change Requests are well documented and approved * Release Test Plan has been defined and approved * Acceptance Testing has been completed successfully | * All changes/updates have been tested and verified * Regression testing completed fully * All required test documentation is completed * Test report and signed off document provided * No Defects with Severity 1&2,   Defects 3&4 Severity are defined as non-high priority for release |

**6. Risks and Contingencies**

|  | **Security Vulnerabilities** | **Performance Issues** | **Compatibility Challenges** | **Data Integrity and Backup** | **Scope Creep and Timeline Delays** |
| --- | --- | --- | --- | --- | --- |
| **Risk** | Potential for cross-site scripting (XSS) or cross-site request forgery (CSRF) attacks due to inadequate input validation and security controls | Poor performance under heavy traffic load, slow response times | Incompatibility with different browsers, devices, or operating systems | Loss of critical data due to software bugs, hardware failure, or human error | Changes in project scope, requirements, or unforeseen technical challenges |
| **Impact** | Compromise of user data, unauthorized transactions, reputational damage | User dissatisfaction, loss of sales opportunities | Poor user experience, reduced accessibility | Disruption of business operations, potential legal and financial repercussions | Project delays, increased costs, resource allocation issues |
| **Contingency** | Implement strict input validation, use security libraries/frameworks, conduct regular security audits and penetration testing. | Perform load testing, optimize code and database queries, use content delivery networks (CDNs), and scale infrastructure as needed. | Test across multiple browsers (Chrome, Firefox, Safari, Edge), devices (desktop, mobile), and operating systems (Windows,Linux macOS, iOS, Android). | Implement regular automated backups, utilize redundancy in storage solutions, and employ transactional integrity checks in the database. | Establish clear project scope and requirements from the outset, conduct regular reviews and prioritize tasks based on impact and urgency |