Forno Test Plan

The purpose of this test plan is to ensure the functionality, usability, security, and performance of the Restaurant Reservation Website.

This test plan covers the testing activities for the core features of the Restaurant Reservation Website, including user registration, reservation creation, modification, and cancellation, as well as system performance and security.

1. Objectives:

   - To verify that all features work as intended.

   - To identify and address any potential security vulnerabilities.

   - To evaluate the performance of the website under normal and peak loads.

2. Test Items:

   A) Features to be tested:

   - User Registration

   - Reservation Creation

   - Reservation Modification

   - Reservation Cancellation

   - System Performance

   - Security

3. Test Environment:

   A) Hardware:

   - Servers, database, and network infrastructure.

B) Software:

- Web browsers (Chrome, Firefox, Safari, Edge).

- Operating systems (Windows, macOS, Linux).

- Database management system.

- Web server software (XAMPP).

- Security testing tools.

4. Test Cases:

A) User Registration:

- Verify that users can register with valid information.

- Validate the email confirmation process.

- Test password reset functionality.

B) Reservation Creation:

- Confirm that users can create reservations for a specified date and time.

- Validate the inclusion of required details (name, contact, party size).

- Test reservation confirmation email.

C) Reservation Modification:

- Ensure users can modify reservations with valid credentials.

- Confirm that modified reservations reflect accurately in the system.

D) Reservation Cancellation:

- Verify that users can cancel reservations with valid credentials.

- Confirm the cancellation process sends appropriate notifications.

E) System Performance:

- Evaluate website response time under normal load conditions.

- Test the scalability of the system under peak load conditions.

- Identify and address any performance bottlenecks.

F) Security:

- Perform penetration testing to identify vulnerabilities.

- Ensure secure communication (HTTPS).

- Validate user authentication and authorization mechanisms.

5. Test Schedule:

A) Testing will be conducted in multiple phases:

- Phase 1: Unit testing and component testing (3 weeks).

- Phase 2: Integration testing (2 weeks).

- Phase 3: System testing (2 weeks).

- Phase 4: Security testing (1 week).

- Phase 5: Performance testing (2 weeks).

6. Responsibilities:

A) Testing Team:

- Conduct all test activities according to the test plan.

- Document and report all defects.

B) Development Team:

- Provide necessary support during testing.

- Address and fix reported defects promptly.

7. Risks and Contingencies:

A) Risks:

- Unexpected server downtime.

- Security vulnerabilities.

B) Contingencies:

- Have a backup server environment ready.

- Regularly update security protocols.

8. Approval:

This test plan requires approval from the project stakeholders before testing begins.

9. Revision History:

Document any changes made to the test plan throughout the testing process.