

## 1. Introduction

The purpose of this document is to define the test strategy for verifying the **Sign-Up feature** of [EchoGPT](#). The goal is to ensure that the sign-up functionality works correctly, securely, and provides a smooth user experience.

### Scope of Testing

#### In Scope:

- Functional testing of Sign-Up form (First Name, Last Name, Email, Send OTP)
- Validation of input fields and error messages
- OTP generation, delivery, and verification
- Navigation (e.g., "Already have an account? Sign In")
- Usability testing of sign-up flow
- Compatibility testing across browsers/devices

#### Out of Scope:

- Post-login functionalities
- Password-related scenarios (not part of current form)
- Backend load testing beyond OTP handling

## 2. Requirements Analysis

### Explicit Requirements

- First Name and Last Name must be at least 2 characters.
- First Name and Last Name cannot be numeric, only spaces, or special characters.
- Email must be in a valid format.
- OTP must be a 6-digit number.
- Checkbox "*I want to receive updates about EchoGPT*" is optional.

### Implicit Requirements

- All error messages should be user-friendly and displayed below the input field.
- OTP should be delivered to the registered email.
- System should prevent duplicate account creation with the same email.
- Sign-In navigation should work correctly.

### Assumptions

- User has a valid internet connection.
- Test data emails are functional and accessible.

- OTP is single-use and expires after a short time (system behavior assumed).

### User Personas

- Students, professionals, and job seekers looking to use EchoGPT services.

## 3. Test Objectives & Success Criteria

### Objectives

- Validate correct functionality of the sign-up process.
- Ensure error handling and field validations are robust.
- Verify OTP flow works as expected.
- Confirm system security against basic invalid inputs.

### Success Criteria

- All **critical test cases** pass.
- No **blocker or high-severity defects** remain open.
- OTP is consistently delivered, validated, and verified.

## 4. Risk Assessment

- **High Risk:** Broken sign-up flow, OTP not delivered, security flaws.

- **Medium Risk:** Incorrect or missing error messages, UI/UX inconsistencies.
- **Low Risk:** Cosmetic issues, minor alignment errors.

## 5. Test Approach

- **Functional Testing:** Positive, negative, edge case scenarios.
- **Usability Testing:** Clarity of error messages, form layout, accessibility.
- **Security Testing:** Invalid data injection, field restrictions, basic spam prevention.
- **Performance Testing:** OTP delivery response time, handling multiple requests.
- **Compatibility Testing:** Chrome, Firefox, Safari, Edge on desktop & mobile.

## 6. Test Environment

- **Browsers:** Chrome (latest), Firefox, Edge.
- **Devices:** Desktop (Windows)
- **Test Data:** Valid/invalid names, emails, OTPs.

## 7. Entry & Exit Criteria

### Entry Criteria:

- Website accessible and functional.

- Test data available.
- Browser/device setup ready.

**Exit Criteria:**

- All high-priority test cases executed.
- All major defects reported.
- Test summary prepared.

**8. Deliverables**

- Test Case Suite (Excel).
- Bug Reports (Excel).
- Test Execution Report (with screenshots).
- Automation Recommendations.
- Executive Summary.