X-PHY Deepfake Detector – User Acceptance Testing (UAT) Guide

UAT Introduction

This document outlines the **User Acceptance Testing (UAT)** process for the **X-PHY Deepfake Detector** desktop application.

The purpose of this UAT phase is to allow users to **validate the available features**, **verify key user flows**, and **confirm expected application behavior** for the functionality included in this phase.

This guide defines what is **in scope** for the current UAT phase. Any functionality not explicitly covered here should be considered **out of scope** for this phase.

UAT Expectations

This UAT phase focuses on validating the **core user flows and primary functionality** of the X-PHY Deepfake Detector application. The objective is to confirm that **end-to-end workflows**, system behavior, and detection outcomes operate as expected.

During this phase, emphasis is placed on **functional correctness and flow completion** rather than enhanced visual design or UI refinements. The user interface is fully functional and suitable for UAT purposes. **UI enhancements and visual improvements will be addressed in subsequent phases.**

Feedback during this UAT is encouraged primarily on:

- Functional behavior

- Completion of defined user flows

- System responses and notifications

- Detection results and outcomes

UI-related feedback can be shared; however, it will be reviewed separately from functional acceptance criteria.

In-Scope Functionality

The following features and user flows are included in the scope of this UAT phase:

Installation

- End-to-end installation flow is included.

- All functional installation steps are covered.

- Due to limitations of the default installer framework, some UI elements may not align with final design expectations. This will be addressed in a future phase with a **WPF-based installer**.

Sign Up / Create New Account

- New users can create an account by providing all mandatory details.

- Email verification is enforced via a **one-time password (OTP)** sent to the user's registered email address.

Sign In

- Users can sign in using their registered **email address and password**.

- Successful sign-in grants access to the application dashboard.

Trial Period

- A default **30-day trial period** is automatically assigned to newly created user accounts.

Subscription Purchase

- Users can purchase subscriptions with durations of **1 month, 6 months, or 12 months**.

Detection

- Users can initiate deepfake detection from the dashboard.

- Active media sources are identified automatically.

- Users can select a media source, choose the detection type, and start detection.

- During detection:

    - The application minimizes automatically

    - The selected media source comes to the foreground

    - Detection start and detection completion notifications are shown

---

Out-of-Scope Functionality

The following features and flows are **not included** in this UAT phase:

1. Corporate user sign-in and related flows

2. Forgot username and forgot password flows

3. Results section and results history

4. User profile section

5. Settings section

6. Support page

7. Floating launcher functionality

8. Background execution and system tray run module

9. AI manipulation detected notifications

10. User interface (UI) enhancements and visual refinements

These items should not be considered part of the acceptance criteria for this UAT phase.

Issue Reporting Guidelines

All issues identified during UAT should be logged in the **defect log section of the provided UAT sheet**.

Each issue should include:

- A brief description

- Steps to reproduce

- Expected versus actual behavior (where applicable)

This will help ensure efficient tracking and resolution.