

The Guardian AI Hackathon Compliance Standard (GAHCS) v1.0

Document ID: GAHCS-2025-v1.0

Effective Date: October 25, 2025

Preamble

This document outlines the mandatory compliance standards for all software projects developed during the Guardian AI Hackathon. The purpose of GAHCS is to ensure all projects adhere to a baseline of user privacy, data security, and web accessibility. Failure to address these core tenets will result in a compliance review.

Section 1: User Data & Privacy

Article 1.1: Principle of Explicit Consent

All collection of Personally Identifiable Information (PII) must be preceded by an explicit and affirmative act of consent from the user. PII is defined as, but not limited to, email addresses, full names, phone numbers, and physical addresses. Software must not collect such data without a user actively checking a box or clicking an "I Agree" button. Logging user IP addresses for analytics is permissible but must be declared in a privacy statement.

Article 1.2: Data Security in Transit and At Rest

Any PII transmitted over a network must be encrypted using industry-standard protocols (TLS 1.2 or higher). Any storage of sensitive user data, especially passwords or API keys, must be hashed and salted. Hardcoding secrets, such as API keys, database credentials, or private tokens, directly within the source code is a critical violation of this standard. Such credentials must be loaded from secure environment variables or a dedicated secrets management service.

Article 1.3: Data Minimization and Logging

Developers must ensure that logs do not contain sensitive user information. For debugging purposes, if user data must be logged, it should be anonymized or masked. For example, an email address user@example.com should be logged as u***@e*****.com. Never log raw passwords or session tokens.

Section 2: Web Accessibility & User Interface

Article 2.1: Semantic HTML and Image Accessibility

All user-facing web interfaces must be built with semantic HTML to ensure proper function with assistive technologies. For all (image) elements that convey meaningful content, a descriptive alt attribute must be present. Images that are purely decorative should have an empty alt attribute (alt="").

Article 2.2: Form Labeling and Input Association

All , , and form controls must have a corresponding element. The for attribute of the label must correctly match the id of the input control. This ensures that screen readers can correctly announce the purpose of each form field. Placeholder text is not an acceptable substitute for a proper label.

Article 2.3: Keyboard Navigability and Focus Management

All interactive elements, including links, buttons, and form inputs, must be reachable and operable using only the keyboard. The currently focused element must have a visible focus indicator (e.g., an outline). Custom UI components built with

or elements must be given an appropriate tabindex and ARIA (Accessible Rich Internet Applications) role to be included in the keyboard navigation order.

End of Document