The Griffin Framework for Digital Trust & Safety

Document ID: GFDTS-2025-01

Version: 1.0

Effective Date: October 24, 2025

Preamble

This document establishes the mandatory baseline for all digital services and applications operating within the jurisdiction. The Griffin Framework is designed to protect user privacy, ensure equitable access for all individuals, and mandate baseline security practices to foster a safe and trustworthy digital ecosystem. Compliance is not optional.

Article 1: Data Handling & User Privacy

Section 1.1: Logging of Personally Identifiable Information (PII)

The logging of Personally Identifiable Information (PII) to persistent, non-secure storage (such as plain text log files or non-encrypted databases) is strictly prohibited. All PII *must* be anonymized or masked before being logged.

For the purposes of this framework, PII includes, but is not limited to:

- User email addresses
- Phone numbers
- Government-issued identification numbers
- Full names when associated with other personal data
- Precise physical addresses

Section 1.2: Data Encryption in Transit

All data transmitted between a client application (e.g., a web browser or mobile app) and a server *must* be encrypted using industry-standard, secure protocols. The minimum acceptable standard is Transport Layer Security (TLS) version 1.2. Connections over unencrypted protocols like HTTP are a critical violation.

Article 2: User Interface & Accessibility

Section 2.1: Image Accessibility and Text Alternatives

To ensure all users, including those utilizing screen-reading technology, can perceive content, all non-decorative <img> elements rendered within the user interface *must* possess a descriptive alt attribute. An image without an alt attribute is considered a compliance failure unless it is explicitly marked for decorative purposes.

Section 2.2: Interactive Target Sizing

All interactive elements, including but not limited to buttons, links, and form inputs, *must* have a minimum target size that is sufficient for users with motor impairments. The minimum acceptable target size is **44 by 44 CSS pixels**.

Article 3: Application Security & Secrets Management

Section 3.1: Prohibition of Hardcoded Credentials

The direct embedding of sensitive credentials, including but not limited to API keys, database passwords, OAuth client secrets, or private certificates, within source code files is a critical violation. Source code is defined as any file that is committed to a version control system.

Section 3.2: Secure Credential Storage

All credentials necessary for the application's operation *must* be loaded from a secure external source at runtime. Acceptable sources include:

- Environment variables injected by a secure hosting platform.
- A dedicated secrets management service (e.g., HashiCorp Vault, AWS Secrets Manager).

END OF DOCUMENT