ENgrid Framework - PCI Compliance Documentation

Document Version: 1.1
Last Updated: July 25, 2025
Maintained by: 4Site Studios

Overview

ENgrid is the most powerful and user-friendly frontend framework built to boost the performance of donation and advocacy pages in Engaging Networks. In this document, you'll find insights into ENgrid's assets and security practices for PCI compliance assessment.

Developed over more than 5 years of research and continuous improvement, ENgrid has had zero reported security incidents, with no vulnerabilities such as XSS, CSRF, or IDOR ever identified. The framework enhances security by minimizing third-party dependencies and maintaining complete open-source transparency.

Static Assets

ENgrid compiles into four static assets:

- **engrid.js** - Main JavaScript bundle with core framework logic, form enhancements, and accessibility features
- **engrid.min.js** - Minified production version of engrid.js
- **engrid.css** - Main stylesheet with SCSS-compiled CSS using modern layout systems
- **engrid.min.css** - Minified production version of engrid.css

Key Security Considerations

- **Secure by design:** ENgrid is a fully client-side integration using static assets compiled from TypeScript with strict type checking. It includes no server components or databases, never transmits or stores payment data, avoids `eval()` or dynamic script generation, has minimal dependencies, and loads all assets over HTTPS.
- **No external calls:** ENgrid makes no outbound API requests or third-party analytics calls.
- **No sensitive data handling:** ENgrid does not process or store sensitive user information. Payment fields are securely embedded by Engaging Networks via "Very Good Security" (VGS) hosted iframes and tokenization.
- **Strict content policies:** ENgrid supports strict Content Security Policies (CSP) without requiring unsafe directives.
- **Open source transparency:** The full codebase is available for review and security audits, with all changes peer-reviewed and automated security scanning via GitHub Dependabot.

- Source Code: ENgrid GitHub Repository
- Documentation: ENgrid Docs Portal

Input Handling and Validation

While final validation and all payment processing are handled server-side by Engaging Networks, ENgrid performs several front-end input sanitization tasks:

1. Strips out non-numeric characters from donation amount fields
2. Capitalizes name and address fields on submit
3. Honors custom field validators defined in Engaging Networks

Dependencies

ENgrid maintains minimal production dependencies:

- `sanitize.css` (v12.0.1) - CSS normalization
- `tippy.js` (v6.3.1) - Tooltip library
- `shuffle-seed` (v1.1.6) - Array shuffling
- `strongly-typed-events` (v2.0.9) - Event handling

PCI Compliance Notes

ENgrid assets are static JavaScript and CSS files that improve the Engaging Networks user experience without handling or processing any sensitive user data directly.

Key compliance points:

- Static assets only (no server-side processing)
- CSP-compatible with no inline scripts
- Proper input sanitization and XSS prevention
- Continuous dependency monitoring
- Security issues addressed within 24-48 hours
- All code changes tracked and auditable

Reporting Issues

If you identify a potential vulnerability, you can contact us at: 📧 support@4sitestudios.com