LAUGHLIN CONSTABLE
FULL CIRCLE BRANDING™
CHI / MKE / NYC / NJ
LAUGHLIN CONSTABLE
FORM STANDARDS
Last Updated: 8/012/2015

# PROJECT REQUIREMENTS



## Overview

This document outlines the Laughlin Constable (LC) form and data security standards. The requirements are written based upon the boilerplate forms located at http://boilerplate.laughlinreview.com/contact-form.php and http://boilerplate.laughlinreview.com/billing-form.php.

## Form and Data Security Standards

1. **Treat Personally Identifiable Information (PII) as if it were financial information.** By protecting PII as financial information, it ensures that best practice security measures are in place to mitigate a breach.
    1.1. Establish and publish a privacy policy and follow it; use the data for what is stated it will be used for and nothing more.
        1.1.1. Inform customers of what information you will NEVER request from them.
        1.1.2. Provide customers consent and choice (opt-in/opt-out) options.
            1.1.2.1. European, Australian and Canadian targeted communications require a user double opt-in confirmation. A user double opt-in confirmation is highly recommended but not required for United States centric communications.
        1.1.3. Enable customers to access, update and correct their data via one of two options, depending upon the scope of the project and/or existing systems:
            1.1.3.1. User account system
            1.1.3.2. A mailto: link for the user to submit information changes via email.
    1.2. Assess systems and operations to identify all PII being processed, accessed or stored in electronic or physical forms.
    1.3. Collect data only on HTTPS (secure) platforms governed by an active Secure Socket Layer (SSL) certificate.
    1.4. Use POST rather than GET in form implementations.

**Commented [JR1]:** Rene to confirm this stance. Is there supporting documentation available that shows that this is a legal requirement?

**Commented [JR2]:** "Physical forms" is a challenge to address and enforce. LC leadership to review options (insurance coverage, SOW verbiage options, etc.)

1.4.1. POST is the preferred method for submitting forms. If GET is used, the parameters of the form will end up as part of the URL in the address bar, exposing data.

1.5. Encrypt all data in all states (transmission, storage, etc.).

1.5.1. Includes all data being submitted as well as data being sent out or requested. All instances of data transmission and storage must be encrypted.

1.6. If data is not needed, do not collect nor store it.

1.6.1. Only request information essential to conduct business; do not request PII from customers, vendors or employees unless absolutely necessary.

1.6.2. When PII is needed to conduct business, do not store the data unless absolutely necessary.

1.7. Observe URLs for PII. The most common links/pages with PII include profile pages, settings, account, notifications/alerts, messaging/mail, registration/signups, login, and other links that appear to associate with the user's information. Example: site.com/settings/sample@email.

1.7.1. In most cases, the PII in the URL can be replaced with a unique site-specific identifier (USSI). Example: "43231". The USSI should be then be set in the background of the application via a POST request and cookie.

1.8. Email is often used for verification as part of site registration/sign up processes, newsletter signups, forgot password processes, etc. Ensure these verification emails do not include PII within the confirmation/registration link.

1.8.1. For instance, site.com/confirm?email=sample@email.com&token=413203. If the confirmation page's URL does contain PII, data is exposed. Remove the PII from the link and use USSI methods to associate the verification email with the user account.

1.9. During development, use placeholder data.

1.9.1. Actual consumer data should be used only in production.

2. **Protect the actual data and know where it is going.** Most companies have focused data protection strategies on protecting the perimeter where the data is stored, rather than protecting the actual data. Start with an internal data classification audit that walks through data flow for the internal business processes, as well as all external processes with third party vendors, to identify all potentially sensitive data. It is important to realize that if database hosting duties are outsourced, it doesn't mean LC nor the client outsources its liability in the event of a data breach.

2.1. Know the network and have a current network diagram.

2.2. Encrypt connection strings section in production web.config file(s) for .NET projects.

2.3. Assess vulnerabilities through Qualys scans and remediate all Level 5 and other results that are determined to be in need of resolution.

2.4. Implement a strong password policy.

2.4.1. Ensure default passwords are changed on all systems, applications and devices.

2.4.2. Enforce acceptable use and password policy (no sharing).

2.5. Use a robust firewall with strong rules and configuration standards.

2.6. Use capable anti-virus/malware software and update regularly.

2.7. Ensure system security updates and patches are promptly installed.

2.8. Encrypt all PII in transit and storage.

2.8.1. Includes all data being submitted as well as data being sent out or requested. All instances of data transmission and storage must be encrypted.

2.9. Track and monitor all access to network resources and PII.

2.9.1. Tightly control portable devices and remote access.

3. **Apply appropriate protective measures to PII.** Encrypt all data and actively monitor emerging data security solutions as older technologies such as monitoring and access control are no longer sufficient. At a minimum, security firms including industry leader Securosis are confirming that tokenization provides the strongest and most cost-effective data security available today.

4. **Audit data flow, including outsourced partners and vendors with access to customer data.** After understanding the data flow and having classified the data, ensure that any vendors with access to the data comply with LC standards for data security. At a minimum, know what type of security solution the third party provider is using for data transit and data at rest, and when and how frequently it is audited.

5. **Ensure separation of duties.** Creating a separation of duties between the corporate security office and the database administrator will ensure that no single individual or group controls access to information in the database without oversight of the LC Web Security Team, mitigating the chance of a data breach.

## Revision History

| Date | Change Made | Author |
|---|---|---|
| 6/10/2015 | Added Form and Data Security Standards. | J. Rhines |
| 8/12/2015 | Added Qualys vulnerability assessments and .NET web.config file(s) connection string encryption. | J. Rhines |