CONSTRUCTION LABOR MARKET ANALYZER

www.myCLMA.com
Website Technology & Security Overview

Overview

Construction Industry Resources, LLC (CIR) owns and manages the Construction Labor Market Analyzer® (CLMA), a state of the art, secure, web accessible environment designed to allow owners, contractors and unions in the construction industry to input skilled labor demand and supply data, analyze their data against blind, aggregated data provided by others, and access aggregated skilled labor scenarios. All Users in the CLMA are able to access aggregate labor scenarios that help them make informed project planning and human resource decisions without being able to identify unique owners, contractors, individuals and projects. From the host facility selection, to the database technology, to the web site administration and management, steps have been taken to insure security, confidentiality, reliability, and performance of this web based application. In addition to the technology-provided security, all Users agree to the established confidentiality, security and anti-trust protocols when they set up their account.

Server Environment

The CLMA marketing website (outside the login area) and database operates from our servers located at a Peak 10 facility in Louisville, KY – http://www.peak10.com/locations/louisville#facility1 – and is managed by Hensley-Elam & Associates based in Lexington, KY.

The CLMA application, source code and database are housed in an Amazon (AWS) Security Center server environment (http://aws.amazon.com/security/). Access to these servers are retained by CIR and backups are created and held by CIR as described below. The CLMA marketing site, application, source code and database are all backed up on a regular basis and held on our AWS servers. In addition, the CIR Administrator has full access to the server environment and retains the most current version of the CLMA source code and database on a separate computer and in a remote safe.

Database Architecture

Amazon RDS MySQL cluster Database for data (Details at http://aws.amazon.com/rds/mysql/). Highly secure and inside simulated private cloud. Backed up every 2 hours and retained for 7 days. Three copies are hot at all times with automated switchover.

Server

Compute units are EC2 cluster (Details at http://aws.amazon.com/ec2/). Command and control server monitors traffic and delegates to least-used server in the query generation layer. If the cluster as a whole gets over stressed, the command unit launches another unit automatically in 60 seconds, installs a copy of the app, and begins diverting traffic there. If a server gets stuck in a loop or has a failure of any kind, the control unit will find out in 5 minutes or less by checking a digital pulse, kills the unhealthy server and replaces it. The control unit itself is monitored by AWS's cloud in the Virginia data center.

System Security

- User data is secure and not accessible by anyone lacking the requisite access rights as established by the User organization. All Users must maintain a username and password for access. Users who register must be manually approved via a CIR administrative approval process.
- Administrative backend accounts require a username and password and can only be managed by an administrator with account management rights.
- Plain passwords are not stored in the database. New and changed passwords are "hashed" using industry-standard encryption techniques (SHA1 or MD5). Only hashed versions of passwords are stored and cannot be decrypted. Administrators do not have access to User passwords. An administrator can flag a User ID for reset at their next login or they can reset to a new temporary password to be generated and sent to the User.
- All customer data is considered proprietary and vigorously protected. A User must be attached to a specific company account to be able to view data belonging to that account. Companies have the additional option of limiting access to data within the account. Companies can set up groups that have specific access to specific sets of data. The level of access can be “read only” or “edit.” The default access for data can be set to a range of options from every User in the company to only a specified few. The access controls within an account are built in a hierarchical fashion providing a flexible security structure, while insuring access to proprietary data is properly controlled.
- A review process is provided that allows the account administrators, as well as the CLMA administrator, to monitor how individuals are accessing data and what activities they are performing. This helps the account administrators to make sure the right Users are performing the expected activities on their data. It also enables the CLMA administrator to monitor overall application utilization and identify areas where potential security problems may exist or where improvements in the application would be appropriate.

Technology Team

A team of industry experts has been assembled to insure the quality, security, reliability, speed, and value of the CLMA web application.

CLMA Development and Application/Database Security

Bright Channel, LLC http://www.bright-channel.com/

Bright Channel partners with the largest companies in the world, delivering software that streamlines decision making and fosters innovation. They develop business solutions that drive innovation, boost efficiency, help visualize data, create business opportunities, and set standards.

Network Management and Security

Hensley-Elam and Associates www.hea.biz

Hensley-Elam's customers range from small business ventures to corporations with multi-billion dollar revenue streams, as well as government services. Hensley-Elam is a full-range Information Technology solutions provider. Their services include help desk and Tier 3 dispatched tech support.