Cayen Systems' Data Stewardship Commitment

Reviewed December 2016

Cayen Systems takes seriously the security of the data entrusted to us. Our current strategy contains many elements that show our commitment to keeping information secure. Cayen Systems stores over 2 million people records from thousands of organizations across the nation on its production servers, which are housed in a secure data center located in the upper Midwestern United States. In our 18+ years of working with student data, we have never had a security breach or a data loss.

All system data is encrypted using an SSL protocol (256-bit RSA encryption) while it is transmitted between our servers and the user; this includes any data that to be uploaded into our system.

Client data resides on a redundant storage system and the applications are run on a cluster of high quality servers to provide maximum security and performance. A limited number Cayen Systems' Managers and Engineers have access to these servers and the data that resides on the storage system.

Website Data

Web-based traffic is secured using a 256-bit RSA encryption (SSL) protocol, so all data passing between a client's web browser and the Cayen website are encrypted. Once data is on our servers, it is protected by firewalls and industry standard security practices.

Website log files are kept for seven days then removed from production servers and archived off site. These log files contain the originating IP addresses used to access our websites, but they otherwise contain anonymous usage statistics which are not directly linked to student or user data.

Secure logins are built into our application creating a tiered access structure, thereby preventing unauthorized access to data. We strongly recommend to our customers that they require password changes on a regular basis.

Access to "directory" and "personally identifiable information" is dependent upon security level as defined by the customer. Access to data is granted on a per organization basis. Disclosure documents (i.e. applications, registration/enrollment forms) may be customized to include locally required consent language. Documents can be uploaded and stored in the system and attached to the people record for viewing by concerned parties.

Stringent firewall and application security schemes are used to keep data secure. Cookies are not linked to any personally identifiable information.

Non-Website Data

Non-web based transfers that occur between the customer and Cayen Systems utilize SFTP with keyed encryption. SFTP data transfers are moved nightly from an externally accessible server to a secure internal server before processing occurs.

Data contained on our SQL servers is not publicly accessible outside of our website interface. Database servers are secured on an isolated VLAN, behind strict firewall rules, to help prevent unauthorized access to our customer's data. Cayen Systems preserves all data for the length of our client relationship.

Employee Procedures for Safeguarding Personal Information

A limited number Cayen Systems' Managers and Engineers have access to these servers and the data that resides on the storage system. Employee workstations are monitored and access logs pertaining to VPN access, email, intranet communication and server and website access are archived for review as needed. Employees are required to sign both a Confidentiality Agreement and a Data Security Policy and are trained to be good stewards of the data entrusted to us. These policies are available upon request.

Cayen Systems does not manage user accounts/access to the application. As Cayen Systems supports our clients remotely, we have no ability to verify the identity or employment status of the person requesting login/password information via our phone or email communications with them. Therefore, all requests for login/password information will be directed to the organization administrator for review/resolution.

Interoffice security measures are enforced to protect confidential information. Unattended workstations are required to be locked (password protected) to prevent customer information from being seen by those that do not have access. Network and file-access security is enforced. Cayen staff login credentials are reset frequently.

Our primary data center is physically restricted to access by Cayen Systems' IT staff and our hosting facility's engineers. The data center has multiple redundancies for internet, power and cooling and is secured by a combination of biometric and keyed security. Our backup data center is physically secured with a combination of biometric and keyed security.

Access to Cayen Systems' networks and data by staff that are no longer employed by Cayen Systems is terminated immediately upon their separation from the company including: any access to data centers, servers, domain, email, VPN, application, interoffice communication and SFTP access.

Questions about this Data Stewardship Commitment can be directed to Ben Hinkle-Wszalek 414.257.9400, extension 114 or benw@cayen.net. Please note that while the details of this document are subject to change, Cayen Systems' commitment to the highest level of care for our customers data will always remain the same.