Raptor Frequently Asked Questions (FAQs)

What data is collected and stored when a visitor ID is scanned into the Raptor system?

Answer: The Raptor scanner collects the ID photo, name, date of birth, and the first four digits of the license number (the other digits are replaced with ***). In the event that two or more visitors have the same first name, last name, and date of birth, Raptor uses the first four digits of the license number to differentiate between them. Only the minimum data needed to accurately identify an entrant is collected (i.e., no address information, no Social Security numbers, no physical characteristic data, etc.). No other data is collected from the ID and no photocopy of the ID is retained.

What is Raptor's data retention policy?

Answer: Raptor strongly believes that all data belongs to the client. Client data is retained until the client requests in writing that the data be deleted. This deletion can be performed at any time, but cannot be undone.

What data from other sources is stored by Raptor?

Answer: If the client uses the Student and/or Faculty modules, additional data can be imported into the Raptor system and stored similarly to visitor data. In the case of Students, student directory data including the name, student ID number, and grade level of the student can be imported. However, no student record data is imported (i.e., no test scores, no home address, etc.).

How is the data used? To what purposes am I authorizing its use?

Answer: The data is used to ensure that the district/school maintains a log of all visitor and other entry data through the front office and the district/school is able to instantly check that data against two databases: 1) a database of the registered sex offenders in all 50 U.S. states and 2) a custom database populated by school administrative personnel which can contain entry alerts such as custodial orders, known gang members, etc.

Is the data shared with any third parties? If so, which ones and which data?

Answer: No data is shared with third parties.

How is the data protected?

Answer: In addition to requiring unique usernames and passwords for each user of the Raptor system, Raptor utilizes firewalls, intrusion prevention systems, host integrity monitoring, and port filtering as well as the latest security processes and procedures to protect all of its systems. All information transmitted to Raptor's datacenter during the log in/sign in process is encrypted using 256-bit AES encryption. Raptor utilizes a Tier-1 datacenter managed by a nationally-recognized provider (Cyrus One).

How is the datacenter physically secured? Do they collocate? If so, is their cage physically secured and how?

Answer: Entry to Raptor's datacenter requires both a datacenter approved photo entry card as well as fingerprint verification of identity. The entry includes a "man-trap" and both of these listed items must be successfully supplied before admission. The datacenter is fully certified and audited under the following standards: SSAE 16 (SOC I type II), PCI DSS (sec 9 & 12), HIPAA, ISO 27001, and FISMA. Raptor's server cage is locked by key and not shared with any other tenants. Raptor owns and controls 100% of the equipment hosted in our server rack.

Is the data encrypted on disk?

Answer: The data is fully encrypted when in transit to and from the disk but is not encrypted when at rest.

How are all communications to the system and within components of the system secured?

Answer: All communications are fully encrypted when in transit using 256-bit AES encryption.

Who has access to the data? What access do Raptor employees have to the data?

Answer: Raptor employees have different access to the data based on their job requirements and associated permissions. Access and permissions are controlled by unique usernames and passwords. As mentioned earlier, the data only contains the minimum information required to screen entrants and does not include address information, Social Security numbers, physical characteristic data, etc. No other data is collected from the ID and no photocopy of the ID is retained.

What access do district/school employees have to the data?

Answer: District/school employees have different access to the data based on their job requirements and associated permissions. Permissions by user level are set by the district/school. Front desk personnel generally are restricted to the ability to sign in/sign out entrants. As mentioned earlier, the data only contains the minimum information required to screen entrants and does not include address information, Social Security numbers, physical characteristic data, etc. No other data is collected from the ID and no photocopy of the ID is retained.

Have all Raptor employees with access to private data been screened and have they signed proper non-disclosure agreements (not just protecting Raptor's intellectual property, but with regard to the data collected and stored about individuals)?

Answer: All Raptor employees have been given full criminal background screenings and are required to sign a non-disclosure agreement that covers all areas of confidentiality prior to working at Raptor.

What are the password requirements for internal and external users in regards to length, complexity, recycle, etc.?

Answer: Internal (Raptor) – we take security seriously and, as such, we have very strict internal policies (minimum of 8 characters, Uppercase, Lowercase, Symbol and number).

External (Raptor users) – We do not currently have a policy in place for ASD employees. That policy would be implemented and managed by the District.

Is there an independent audit of their security practices available?

Answer: Raptor does not conduct third-party audits, but Raptor's datacenter (where the data is stored) has attained ISO 27001 independent certification for its security compliance.

Can a user review the data collected about them to ensure it is accurate?

Answer: Whether or not an entrant would be allowed to review the data would be a policy decision on the part of the district/school and not a decision by Raptor.

Is the software open source or closed source?

Answer: Raptor's system is a proprietary application and is Microsoft based – Windows/IIS/SQL.

Does Raptor have adequate quality assurance practices to reduce the likelihood of data leaking bugs? Is there an audit available of these practices?

Answer: Raptor has a dedicated Quality Assurance team responsible for the continuous review and testing of our product. Raptor does not conduct third-party audits, but Raptor's datacenter (where the data is stored) has attained ISO 27001 independent certification for its security compliance.

What is Raptor's disclosure policy with regards to discovered vulnerabilities and possible or actual leaks of data?

Answer: In the event of a possible or actual data leak, Raptor would immediately inform the District so that the District could immediately communicate to the parents/visitors. Raptor does not store the email and/or phone numbers of the parents/visitors. As mentioned earlier, the data only contains the minimum information required to screen entrants and does not include address information, Social Security numbers, physical characteristic data, etc. No other data is collected from the ID and no photocopy of the ID is retained.