Caliber Public Safety Accurint Embedded Query Audit/Security Program

OVERVIEW

Colossus, Incorporated (herein referred to as "Caliber Public Safety", "Caliber", or "CPS") has partnered with LexisNexis (herein referred to as "LN") to offer for resale access to Accurint Public Data Queries embedded within Caliber Public Safety products. The LN Accurint reseller agreement requires Caliber to maintain an audit program that will monitor Customers' usage, prevent unauthorized usage, and detect unauthorized or inappropriate use of Accurint data.

AUDITING PROGRAM DETAILS

Caliber will perform the below activities in compliance with the Auditing program:

1. Log individual query transactions initiated by Customers. The following information will be logged for tracking and audit purposes.
    a. Customer – name of Agency that performed the search;
    b. User – the User ID used to access the system including the name of the individual who is authorized to use the User ID;
    c. Date/Time – Actual date and time of the search;
    d. IP address – the IP address from which the search originated; and
    e. Permissible Use – Defined as Law Enforcement Access for all queries.
2. Conduct audits of Customer usage as defined below.
    a. New Customer Audits – When access is enabled to Accurint Public Data Queries for a Customer, Caliber will perform 2 separate audits per new Customer with the first 90 days. Each audit will include selecting at least two queries within the last 30 days to validate with the Customer that the searches were performed for a permissible business reason, and in accordance with all laws, regulations and contractual obligations underlying access.
    b. Customer Random Audits – Caliber will randomly select ten percent (10%) of Customers having access to the Accurint Public Data Query service each year to audit five (5) random queries from each Customer to validate with the Customer that the searches were performed for a permissible business reason, and in accordance with all laws, regulations and contractual obligations underlying access.
    c. Event Driven Audits – Perform audits on accounts, or users, that have been referred by LN due to potentially unauthorized activity, or concern for which developed as a result of a report received from by a third party, such as another company or a consumer, may have conducted unauthorized searches. Caliber will respond to all such requests within an acceptable, pre-determined timeframe, which should be no longer than 120 days from the time the audit letter is received, and validate that the searches were performed for a permissible business reason, and in accordance with all laws, regulations and contractual obligations underlying access.
    d. Maintain a process whereby Customers can perform self-audits of Accurint Public Data Queries as desired.
        i. A search utility will be available for Customers to search by User Name, Agency, and Date Parameters to view queries that were initiated by end users.
3. Caliber will work to educate Customers that are found to have inappropriately misused Accurint data. Failure by the Customer to correct such action or unresponsiveness to respond to requests for audit information will result in termination of the embedded Accurint Public Data Query service.

SECURITY PROGRAM DETAILS

Caliber Public Safety has reviewed Appendix V of the LN Non-FCRA Government Reseller Agreement and will abide by the business practices that are stated. Caliber maintains security policies and procedures in alignment with the AICPA trust services criteria. Controls are in place to meet governance across Organization and Management, Communications, Risk Management, Logical and Physical Access, System Operations, Change Management and Monitoring of Controls categories. Third party SOC 2 audits are performed on an annual basis to assess effectiveness of these controls and verify conformance across the Security and Availability principals. Controls encompass key threat categories, established and implemented for reducing or eliminating risk in conjunction with a structured mitigation process which involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls. These controls are used to mitigate risk for better protection of mission-critical information and the systems that store and process this information. Recurring reviews ensure risk exposure changes are being continually evaluated. Technological, regulatory and internal changes which affect controls are identified, monitored and assessed and control additions/adjustments are incorporated to the overall risk mitigation strategy as necessary.