SEARCH REAL FAST SECURITY AND ACCESS USAGE POLICIES

Published by

Search Real Fast))))™

www.searchrealfast.com

SEARCH REAL FAST SECURITY AND ACCESS USAGE POLICIES

THE SECURITY OF YOUR INFORMATION AND DATA IS EXTREMELY IMPORTANT TO SRF Query. If you wish to also view our privacy policy, please click here.

1 **ALL OUR CONNECTIONS TO OUR WEB SERVICES USE SECURE HTTPS PROTOCOLS.**

2 ALL OUR WEB SERVICES ARE HOSTED ON OUR SECURE SERVER PROVIDED BY ARMOR.COM using Armor Complete Virtual Private Cloud (VPC). Inside our VPC, all access to our website and database processing code, files, and data is FURTHER protected by our own Virtual Private Network – VPN.

3 When each of our Search Site Library's database URL is created, that URL is filtered through the BrightCloud® Web Classification Service to eliminate websites that do not meet our database site policy to guard against categories that often host malicious content or illegal or objectionable content and activities.

4 Search Real Fast is willing to sign a Confidential Data Agreement – CDA - with the administrator of each Subscription Group to protect each of their user's confidential information at least to a reasonable degree of care.

5 When each user buys an individual subscription or registers under a group subscription for Search Real Fast access, each user selects as a username their individual or their group's email address (if under a group subscription e.g., user@group-domain-name.) Each user also selects their own private password for their account. To complete their initial registration, each user must then click a registration link in an email sent to their registration email address. If their email domain's server does not forward that registration email to that user's registered email address, their registration cannot be completed. Therefore, only a valid group email address may register under that group subscription. For groups that do not provide their users a group email address, users may only register when located in, connected to, and communicating to the Search Real Fast web server from the group's particular IP address for the facility. After registering in the group's facility, the user may log onto the Search Real Fast service from any location and IP address allowed to connect to web servers in the US.

6 After the user logs into Search Real Fast with their username and password, transmission of user data over the internet in HTTPS packets is not identified by their username, but only by our identifier for that user. Each Search Real Fast service request packet for text processing, event logging, or another service must submit this identifier to receive service. Our web browser and server code automatically provides this user identifier as part of each request packet sent to our Search Real Fast web server. Before any user processing begins, each packet is checked by our web server for this identifier.

7 After a user logs into Search Real Fast, each user is allocated a maximum time period of inactivity. If the user is logged in and yet inactive for a significant amount of time, the user is sent a message to re-authenticate.

8 Search Real Fast keeps records and logs information and associates each user with their user text, keywords, and key sentences submitted in each access HTTPS request packet. When a user clicks on the "Extract Keywords", the "Submit Query", and other buttons on a Search Real Fast screen, we log the items and query string displayed on the main screen along with the user text, keywords and key sentences. The user text, keywords and key sentences are encrypted before these data fields are stored in our database server.

9 THE ONLY EXCEPTION TO THIS DATA RECORDING POLICY (see #8) IS WHEN THE SUBMITTED HTTPS request packet has "text" which CAUSES A SERVER TEXT PROCESSING ERROR! When the web server text processing code experiences an error, we save the text and other information from this packet which caused the error along with its associated user's identity. We use this information to determine the cause of the error, correct the error, prevent future errors and test future server code for this same condition. When we have corrected the error in the current server code, the user's identity will be removed from this error record information and it will be encrypted using our Search Real Fast key and stored in our internal database records documenting that error condition.

10 If over a short period of time Search Real Fast receives multiple packets from a particular user causing server processing errors, then that user will be blocked. A message stating "User must re-authenticate with the Search Real Fast website to continue service" will be sent to the submitting browser. In addition, an email will be sent to that user's registered email address informing them of this action, the reason for it, and what the user should do to continue service. Further request packets from this user and source address will be dropped until the user re-authenticates. This action is to prevent misbehaving browsers, unauthorized automated access, hackers, or impostors from overloading our server resources and denying our authorized users access to our service.