TRIANGLE MLS™
MULTIPLE LISTING SERVICES

Triangle MLS, Inc.
Data Security Policy

Defined terms have the meaning given to them in licensee's data license agreement. "Firm, Consultant, or Licensee" means any party that receives TMLS data pursuant to a data license agreement, and any obligations placed on "Firm, Consultant, or Licensee" apply to any combination of those parties and other licensees.

Steps taken to protect the Confidential Information must include at least the following:

a. **Authentication**

When TMLS provides a RETS data feed, it will require username and other authentication information and may require a custom user agent, IP authentication, download quotas, time restrictions, or additional controls and TMLS will send login information with those restrictions to the Firm, Consultant, or Licensee. Firm, Consultant, or Licensee must use the custom user agent, if provided by TMLS.

b. **Transmission**

Encrypted methods of transmission, such as SSL or VPN connections, must be used if supported by TMLS servers.

c. **Data Location and Storage**

Computers where data is stored must be protected using current IT industry standard firewalling technology, which at a minimum must restrict access to mission-critical ports only, and limit administration of the server to secure encrypted protocols only.

Computers where data is stored must be secured against attack using current IT best practices and must be kept patched with all known security updates.

If permitted by agreement and data is copied to other locations, such as tapes or disk for backup, it must be stored in encrypted form and physical access controlled via key lock or stronger means. TMLS data must not be copied to and stored unencrypted on laptops, PDAs, portable hard drives, portable RAM memory drives that are not located in a secure location.

Data may not be stored outside of the United States.

d. Search, Display and Print Restrictions

If TMLS identifies a search provider (IE. Google, Yahoo, etc.) as undesirable and determine TMLS data must not appear on that providers site, the Firm, Consultant or Licensee must use a robo.txt file to prevent web crawling of that provider.

TMLS may require anti-scraping technology in its sole discretion, at least three of the following practices must be implemented:

(i) User inputs – including URL and form parameters – must not be easy to manipulate, such that TMLS non-IDX information is easily spidered and scraped. This does not mean Firm, Consultant, or Licensee is required to inhibit indexing by major search engines.
(ii) Sensitive information, such as email addresses, is obscured using JavaScript or hidden behind forms (and not present in 'hidden' form fields)
(iii) There are limits on the number of pages that can be requested in a given time period before the software validates that a user is present
(iv) Key listing information, such as price or listing address, is rendered as a graphic with no 'ALT' tag or using Flash or Java or other technology such scraping is inhibited.

Other practices can be substituted in TMLS's sole discretion for the preceding requirements if Firm, Consultant, or Licensee can show they are effective.

Scraping attempts must be logged and monitored and recurring attempts to bypass anti-scraping measures must be blocked at the firewall.

e. Additional Programming Restrictions

The following are additional secure coding practices that must be implemented as applicable:

i. User inputs and other parameters (URL, Form) must ALL be validated at both for data type, allowed character set, numeric range, enumerated legal values. Special characters, such as those used for cross site scripting attack (XSS) and SQL injection must be stripped other otherwise rendered harmless.
ii. All reasonable steps must be taken to prevent browser caching of sensitive information, such as a user password.
iii. Repeated failed logins must be logged and generate alerts.
iv. Passwords and other Confidential Information must be stored in encrypted format, and the encryption key strongly protected.
v. Logins and other parts of user sessions where Confidential Information is transmitted must utilize strong SSL encryption.
vi. If located in different data centers, back end connections between the web application and database must be strongly encrypted
vii. Every application component must be thoroughly be wrapped in error-trapping code so that Confidential Information is never displayed to the end-user.

Additional reasonable judgment must be used in developing secure web applications.

TMLS may require addition security enhancements that must be implemented by the Firm, Consultant or Licensee (at the Firm, Consultant, or Licensee's expense) and TMLS will provide notification to Firm, Consultant or Licensee that will include deadlines for compliance.

f. Data Retention

If Firm, Consultant, or Licensee is only authorized to receive active listings, then the active listings should not be retained for more than three days after a status change, with an exception granted for such listings stored on backup media which shall not be maintained for over one month.

A Firm is not bound by these data retention obligations regarding its own listings.

If you have any questions, please contact Matt Nagy at mattn@TriangleMLS.com.