



NMLS

Summary of Technical and Data Security Protocols

State Regulatory Registry LLC provides NMLS on behalf of, and under contract with, state regulatory agencies and the Consumer Financial Protection Bureau (Agencies) and has been approved for use by these Agencies. NMLS undergoes rigorous testing and reviews to ensure that sensitive and non-public data is protected. What follows is a summary of the technical and data security protocols.

- **Technical Details**

- NMLS is a web-based system that uses HTTPS (HTTP over Secure Transport Layer). Protocols older than TLS 1.2 are not supported.
- RSA 2048 bit certificates are used to encrypt and decrypt data as it transfers from the user page requests to the NMLS web server. The system performs a certificate revocation list (CRL) check during the communication process to ensure that the certificate presented by the server being communicated with has not been revoked.
- NMLS supports IE 11.0, Chrome 30, and Firefox 32 or greater. The browser must be java script enabled and it is recommended that cookies are enabled. If you would like to download the latest version of these browsers, the [Technical Requirements](#) page on the NMLS Resource Center has links available to each of them.
- Email notifications sent from NMLS come from NMLS_Notifications@NmlsNotifications.com. They do not contain sensitive information.

- **User Accounts**

- System passwords must be complex with a minimum length as defined when the account is established.
- Passwords expire at set intervals. Users are prompted to change their passwords upon expiration.
- An account is considered dormant if it contains no data such as testing and education results, regulatory actions or submitted licensure applications on the record. NMLS will delete a dormant account after 180 days for company and individual users. Pending filings do not prevent an account from dormancy and will be deleted after 180 days along with any related dormant accounts.
 - The System will prevent a company record from being marked dormant if an ESB exists for the company in a “Pending Principal Signature,” “Returned to Surety,” or “Executed” status. The System will delete any ESB in a “Requires Rep Signature” status and remove licensee authority after the surety deletes/voids the last bond preventing company dormancy.
- For accounts with education and testing results or submitted or approved filings, NMLS will disable the account if it has not been accessed in 120 days by a company account user or 15 months by an individual user. If a user account is disabled, the System prompts the user to provide identifying information before they can log into their account.
- Users are locked out after a set level of invalid login attempts.

- Users' sessions expire after 30 minutes of general inactivity and after 15 minutes of inactivity on payment processing pages.
 - Accounts are provided access through Role Based Access Controls (RBAC) wherein each user identifier is given a specific role within the application.
- **Data Protection**
 - Infrastructure, applications, and data are protected by multiple layers of security to guard against both external and insider threats.
 - NMLS has implemented a logging and auditing protocol that helps to identify suspicious behaviors.
 - Sensitive information is encrypted in transit and at rest.
 - All NMLS staff, contractors and agents with access to data undergo annual Privacy and Security Awareness training.
 - All uploaded files are inspected for malicious code prior to being written to the database.
- **Fingerprint Record Security**
 - Fingerprint records are securely received, stored, and transmitted by the NMLS Fingerprint (NFP) system. Technologies utilized include session encryption including secure web access and secure transport. The background check results are purged from NFP after a set number of days, though the Fingerprints themselves are archived according to archival requirements.
 - In addition to the secure transmission of fingerprint records, there are layers of physical and network security applied. The NFP system is segregated from that of NMLS and additional physical controls have been established.
- **Testing, Reviews and Compliance**
 - NMLS undergoes a rigorous Application Certification process to ensure it meets the specified standards.
 - Data centers hosting NMLS have been audited according to SSAE-16 SOC 1 Type II¹ and SOC 2 Type II standards. CSBS also conducts a biennial independent third-party SSAE-16 SOC 1 Type II audit of financial controls within NMLS.
 - NMLS is fully accredited (FISMA Certification & Accreditation) by the Consumer Financial Protection Bureau (CFPB). FISMA security controls within NMLS are reviewed by an independent third-party security assessor annually.
 - There is an independent third-party security penetration test performed on NMLS annually.
 - NMLS complies with the requirements of U.S. Department of Justice-Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy² for the storage of fingerprint and background check results records and is periodically audited by the FBI for compliance to the CJIS.
 - NMLS receives annual Attestation of Compliance from appropriate Service Providers to the Payment Card Industry (PCI) Data Security Standards (DSS).
 - Third parties receiving, storing or processing sensitive data are required to adhere to all applicable regulations and laws, providing supporting documentation to NMLS on at least an annual basis.

¹ Previously this used to be a SAS70 report

² Version 4.5, December 2008 (CJISD-ITS-DOC-08140-4.5)

- **Federal Registry Specifics**

- All NMLS Federal Registry users are required a "two-factor" authentication mechanism at assurance level 3³. This includes users at Federal Agencies, Agency-regulated institution and NMLS Call Center staff with federal record access.
- The MLO Batch Upload feature is only available to users that have been authenticated into NMLS and have been granted the role necessary to perform batch upload. The uploaded file is encrypted and stored in the database.

³ Consistent with OMB Memo M-04-04, E-Authentication Guidance for Federal Agencies, 16 December 2003, and NIST SP 800-63-1, Electronic Authentication Guidance, 8 December 2008 (DRAFT)