Remote Notarization Provider Application

Colorado Secretary of State
Notary Program
1700 Broadway, Ste. 550
Denver, CO 80290

Phone: 303-894-2200, press 4, then 1
Fax: 303-869-4864
Email: notary@sos.state.co.us

Business entity

ID number

Name

Provider's contact person

First name | Middle name | Last name | Suffix

Email address

Provider's authorized agent

☐ I certify that the undersigned provider and its system comply with the requirements of section 24-21-514.5, C.R.S., and the rules adopted under section 24-21-527, C.R.S.

First name | Middle name | Last name | Suffix

Technology system

Type of remote notarization system being provided

MISMO RON certification

Are you a MISMO RON certified provider

If no, are you in the process of obtaining a MISMO RON certification?

Network architecture

Do you have network firewall systems in place?

If yes, provide description of firewall systems.

Do configuration standards include requirements for a firewall at each Internet connection and between any enclaves/demilitarized zone (DMZ) and the internal network zone?

If no, provide more information.

Is an IDS/IPS system in place and configured on firewalls and/or the network?

Provide more information.

Security system

Are systems scanned and audited for compliance with hardening standards at least quarterly?

Describe the process, plans for implementation or alternate solution.

Are file-integrity monitoring tools utilized and reviewed to prevent un-authorized system changes internally?

Describe the process, plans for implementation or alternate solution.

Data security

Is full disk or database encryption utilized for data?

If yes, is there a process in place for changing cryptographic keys and key management?

Do you have any forms of data leak protection to prevent data from leaving through an unauthorized channel?

Data security continued on next page

Data security (continued)

Will you ensure Personally Identifiable Information (PII), Private Health Information (PHI), or other sensitive information is kept secure?

If yes, how?

Will any of the data you collect be sold to third parties?

If yes, explain.

Are data backups encrypted and stored in secure locations?

Data security continued on next page

Data security (continued)

Is media properly destroyed when no longer needed for business purposes?

Provide specific levels of encryption and destruction procedures.

Are copies of media backups stored off site in a secure climate-controlled facility?

If no, provide details about what you're doing with media backups.

Vulnerability and patch management

Are all system components and software protected from known vulnerabilities by having the latest vendor-supplied security patches installed?

Is there a process in place to identify newly discovered security vulnerabilities?

Does this system rate the vulnerabilities according to an industry standard?

Provide specific details about the tools used and frequency of scans.

Access control

Is access to system components and data limited to only those individuals whose jobs require such access?

Is two-factor authentication incorporated for administrator access, especially for systems containing sensitive data?

If no, describe plans for implementation or alternate solution.

Access control continued on next page

Access control (continued)

Is two-factor authentication incorporated for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties?

If no, describe plans for implementation or alternate solution.

Is access for any terminated users immediately deactivated or removed?

If no, describe plans for implementation or alternate solution.

Are inactive user accounts over 90 days old either removed or disabled?

If no, describe plans for implementation or alternate solution.

Logging, monitoring, and auditing

Are automated audit trails for all system components utilized to track the following items?

- User access to systems
- Administrator access to systems and administrator/root actions taken on systems
- Invalid login attempts, date/time of events and success/failure of events

If no, explain.

Are internal and external network vulnerability scans run at least quarterly?

Are the results reviewed and acted upon to prevent vulnerabilities?

Will all logs be retained for at least one year?

Security policy enforcement

Is a security policy established and distributed to all personnel that manage or interact with systems?

If no, describe plans for implementation or alternate solution.

Is this policy reviewed at least once per year?

Are proper background checks and qualifications reviewed for all personnel?

If no, describe plans for implementation or alternate solution.

Is the provider willing to adhere to the State of Colorado Cyber Security laws and rules?

If no, describe plans for implementation or alternate solution.

Incident response

In the event of a data breach, have you designated a specific person to be responsible for notifying customers who have had their information compromised?

If yes, provide the designated person's name, title, phone number and email.

Name

Title

Phone

Email

Does your incident response plan include digital forensics, log analysis, and analysis by computer security experts?

If no, describe your forensic analysis solution or plan.

Remote notarization

If requested by the Secretary of State, will you provide a remote notarization demonstration?

Will the authenticity and integrity of notarized documents and audio-video recordings be maintained if your solution becomes obsolete or you go out of business?

If yes, how will they be maintained?

Where, or with whom, will those items be stored if you go out of business?

Remote notarization continued on next page

Remote notarization (continued)

Will any other business entities and/or any of your affiliates have access to either Personally Identifying Information or any Non-Personally Identifying Data gathered during your remote notarization process or procedures?

If yes, explain.

Proof of identity - if not MISMO certified

Do you provide a credential analysis process or service?

If yes, please describe the credential analysis process or service to be used, specifically addressing the criteria and standards in RULONA and 8 CCR 1505-11.

Proof of identity continued on next page

Proof of identity - if not MISMO certified (continued)

You must mark yes to at least one of the three following questions:

Do you provide a dynamic knowledge-based authentication assessment?

If yes, please describe the process or service to be used, specifically addressing the criteria and standards in RULONA and 8 CCR 1505-11.

Do you use a public key certificate?

Describe the process or service to be used, specifically addressing the criteria and standards in RULONA and 8 CCR 1505-11.

Do you use an identity verification by a trusted third party?

If yes, please describe the process or service to be used, specifically addressing the criteria and standards in RULONA and 8 CCR 1505-11.