## 1.1 CREDENTIAL ANALYSIS

The credential analysis method provided by a remote notarization system provider must, at a minimum, satisfy the following requirements:

1.1.1 Use automated software processes to assist the remote notary public in verifying the identity of the remotely located individual and any credible witness.

1.1.2 Ensure that the credential passes an authenticity test, consistent with sound commercial practices that:

1.1.2.1 Use appropriate technologies to confirm the integrity of visual, physical, or cryptographic security features;

1.1.2.2 Use appropriate technologies to confirm that the credential is not fraudulent or inappropriately modified;

1.1.2.3 Use information held or published by the issuing source or authoritative sources, as available, to confirm the validity of personal details and credential details; and

1.1.2.4 Provide the result of the authenticity test to the remote notary public.

1.1.3 Enable the remote notary public to visually compare for consistency both:

1.1.3.1 The information and photo presented on the credential itself; and

1.1.3.2 The remotely located individual viewed by the remote notary public in real time through audio-visual transmission.

1.1.4 Use a government-issued identification credential that satisfies the requirements of Revised Uniform Law on Notarial Acts (Title 24, Article 21, Part 5, C.R.S.), including the requirements for both the signature and the photograph of the remotely located individual per section 24-21-514.5 (6)(b)(II), C.R.S.

1.1.5 Employ a credential image capture procedure that verifies that:

1.1.5.1 The remotely located individual is in possession of the credential at the time of the notarization;

1.1.5.2 The submitted credential image or images have not been manipulated; and

1.1.5.3 The credential images match the credential in the remotely located individual's possession.

1.1.6 Ensure captured image resolution that:

1.1.6.1 Is sufficient enough for the provider to perform credential analysis per the requirements above;

1.1.6.2 Enables visual inspection by the remote notary public of photographs, text, and other credential features; and

1.1.6.3 Captures all images necessary to perform visual inspection and credential analysis.

## 1.2 DYNAMIC KNOWLEDGE-BASED AUTHENTICATION ASSESSMENT

The dynamic knowledge-based authentication assessment provided by a remote notarization system provider must, at a minimum, satisfy the following requirements:

1.2.1 The remotely located individual must complete a quiz consisting of a minimum of five questions related to that individual's personal history or identity, formulated from public or private (proprietary) data sources.

1.2.2 Each question must have a minimum of five possible answer choices.

1.2.3 At least 80% of the questions are to be answered correctly within two minutes.

1.2.4 All questions are to be answered within two minutes.

1.2.5 If the remotely located individual fails the first attempt, the individual may retake the quiz one time within 24 hours:

1.2.5.1 During the retake, a minimum of 40% of the previous questions are to be replaced; and

1.2.5.2 If the remotely located individual fails the second attempt, the individual is not permitted to retry with the same remote notary public for 24 hours.

## 1.3 PUBLIC KEY CERTIFICATE

Use of a public key certificate by a remote notarization system provider must, at a minimum, satisfy the following requirements:

1.3.1 Provider must ensure that digital signatures are accompanied by a digital certificate for document integrity.

1.3.2 Provider must use a Public Key Infrastructure (PKI) to create certificates based on X.509 standards.

## 1.4 IDENTITY VERIFICATION BY A TRUSTED THIRD PARTY

Use of an identity verification by a trusted third party provided by a remote notarization system provider must, at a minimum, meet or exceed the accuracy of identity verifications conducted through using either a dynamic knowledge-based authentication assessment or a public key certificate under the standards above in Sections 1.2 and 1.3.

## 1.5 DATA SECURITY AND STORAGE REQUIREMENTS

Remote notarization system providers and remote notarization storage providers must satisfy the following data requirements:

1.5.1 Network Architecture

1.5.1.1 A provider must have a network firewall system in place that isolates each internet connection from any enclaves/demilitarized zones and internal networks.

1.5.1.2 A provider must have an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) in place and configured on firewalls and/or the network.

1.5.2 System Security

1.5.2.1 A provider must scan and audit its system for compliance with hardening standards at least once quarterly.

1.5.2.2 A provider must use and review file-integrity monitoring tools to prevent unauthorized system changes internally.

1.5.3 Data Security

1.5.3.1 A provider must ensure that all data, including data backups, is stored in secure locations.

1.5.3.2 A provider must encrypt data using at least 256-bit encryption.

1.5.3.3 A provider must use full disk or database encryption for data.

1.5.3.4 A provider must have a process in place for changing cryptographic keys and key management.

1.5.3.5 A provider must have forms of data leak protection in place to prevent data from leaving through an unauthorized channel.

1.5.3.6 A provider must properly destroy media when no longer needed for business purposes.

1.5.3.7 A provider must store media backups offsite in a secure climate-controlled facility.

1.5.4 Vulnerability and Patch Management

1.5.4.1 A provider must protect components and software protected from known vulnerabilities by having the latest vendor-supplied security patches installed.

1.5.4.2 A provider must have a process in place to identify newly discovered security vulnerabilities and the system must rate the vulnerabilities according to an industry standard.

1.5.4.3 A provider must perform vulnerability scanning at least once a month on all internal systems and perform vulnerability remediation.

1.5.5 Access Control

1.5.5.1 A provider must limit access to system components and data to only those individuals whose jobs require such access.

1.5.5.2 A provider must implement two-factor authentication for all internal and remote (i.e., network level access originating from outside the network) system access.

1.5.5.3 A provider must audit user access on a quarterly basis.

1.5.5.4 A provider must immediately deactivate or remove access for any terminated users.

1.5.5.5 A provider must remove or disable inactive user accounts over 90 days old.

1.5.6 Logging, Monitoring, and Auditing

1.5.6.1 A provider must have automated audit trails for all system components utilized to track the following items:

1.5.6.1.1 User access to systems

1.5.6.1.2 Administrator access to systems and administrator/root actions taken on systems

1.5.6.1.3 Invalid login attempts, date/time of events and success/failure of events

1.5.6.2 A provider must run internal and external network vulnerability scans at least once quarterly.

1.5.6.3 A provider must review and act on results to prevent vulnerabilities.

1.5.6.4 A provider must retain all logs for at least one year.

1.5.7 Security Policy Enforcement

1.5.7.1 A provider must establish and distribute a security policy to all personnel that manage or interact with systems holding data.

1.5.7.2 A provider must review the security policy at least once per year.

1.5.7.3 A provider must perform proper background checks and review qualifications for all personnel.

1.5.7.4 A provider must adhere to all applicable State of Colorado cybersecurity laws and regulations.

1.5.8 Incident Response

1.5.8.1 In the event of a data breach, a provider must have a designated specific person to be responsible for notifying customers and Colorado Secretary of State who have had their information compromised.

1.5.8.2 A provider must have an Incident Response Plan in place that includes digital forensics and log analysis by computer forensics experts.

1.5.9 Maintenance plan

1.5.9.1 A provider must have a plan for maintaining the authenticity and integrity of notarized electronic records and audio and video recordings if the provider's storage solution becomes obsolete or if the provider ceases operating as a business. The plan must detail where or with whom these items will be stored and how they will be maintained.