ICAC Remote Proctoring Policy

(Adopted 26 March 2020)

ICAC considers that the remote proctoring of examinations falls within the guidelines of the ISO/IEC 17024 standard. Remote proctoring is becoming more popular daily and as a result, many companies are entering the field as Remote Proctor providers. Accordingly your organization should assure that processes adhere to the following guidelines:

Interface Requirements:

Development: Application programming interfaces (APIs) shall be designed, developed, deployed and tested in accordance with leading industry standards (e.g., OWASP for web applications, SEI CMM standards) and adhere to applicable legal, statutory, or regulatory compliance obligations.

Access: Access authorization needs to include role, level of access, purpose of access, role level, length of access needed, and written consent from customer representative assigned as the dedicated contact.

Data Security: Data Security Architecture must be implemented in compliance with industry standards. This includes, but is not limited to:

- All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes
- All staff understand their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.
- All staff complete appropriate annual data security training.
- Confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to confidential data on IT systems can be attributed to individuals.

- Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.
- Cyber-attacks against services are identified and resisted and responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.
- A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.
- No unsupported operating systems, software or internet browsers are used.
- A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.
- IT suppliers are held accountable via contracts for protecting the personal confidential data they process.

Software Management: Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components. Admin level restrictions are setup on workstations and laptops.

E-Commerce Transactions: Data related to electronic commerce (e-commerce) that traverses public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure, or modification in such a manner to prevent contract dispute and compromise of data.

Key Generation, Encryption: Keys must have identifiable owners (binding keys to identities) and there shall be key management policies. Policies and procedures shall be established for the management of cryptographic keys in the service's cryptosystem (e.g., life cycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions).

Provider shall inform the customer (certifying body) of changes within the cryptosystem, especially if the customer data is used as part of the service, and/or the customer has some shared responsibility over implementation of the control.

Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations) and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.

Platform and data appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud consumer or trusted key management provider. Key management and key usage shall be separated duties.

Virus & Malware: Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.

Remote Proctoring: The system must incorporate a human (remote) proctor who has the capability to monitor the candidate's behavior (visually and audibly) during the entire examination process. The proctor must have the ability to pause, stop, or even suspend tests. The proctor must also be able to communicate with the candidate.

Management Processes:

Ongoing Assessment: Assessments shall be performed at least annually by the remote proctoring provider to ensure that the organization addresses non-conformity to established policies, standards, procedures and compliance obligations. This annual assessment also ensures changing standards, regulatory, legal, and statutory requirements relevant for their business needs are incorporated into the delivery process.

Documentation & Support: Information system documentation (e.g., administrator and user guides, and architecture diagrams) are made available to authorized personnel to ensure the following:

- Configuring, installing, and operating the information system,
- Effectively using the system's security features, access to contact and support personnel.

Environmental Risks: The remote proctoring process should provide physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disasters. The system shall anticipate, and be designed with countermeasures to protect the exam data and security as well as administration against such disruptions.

Data Retention Policies: Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness.

No part of the examination process shall be subcontracted to a third party without the specific authorization of the certification body.

No data generated through the examination process (question database, application data, psychometrics, etc.) will be shared with any third party without the specific authorization of the certification body.

User Access

User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal and external users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures must incorporate the following:

- Procedures and supporting roles and responsibilities for provisioning and deprovisioning user account entitlements.
- Business case considerations for higher levels of assurance and multi-factor authentication secrets (e.g., management interfaces, key generation, remote access, segregation of duties, emergency access, large-scale provisioning or geographically distributed deployments, and personnel redundancy for critical systems)
- Access segmentation to sessions and data in multi-tenant architectures by any third party (e.g., provider and/or other customer (tenant))
- Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and federation)
- Account credential life cycle management from installation through revocation
- Account credential and/or identity store minimization or re-use when feasible
- Authentication, authorization, and accounting (AAA) rules for access to data and sessions (e.g., encryption and strong/multi-factor, expireable,

non-shared authentication secrets)

- Permissions and supporting capabilities for customer (tenant) controls over authentication, authorization, and accounting (AAA) rules for access to data and sessions
- Adherence to applicable legal, statutory, or regulatory compliance requirements
- Controls in place ensuring timely removal of systems access that is no longer required for business purposes.
- User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict of interest.
- Access to the organization's own developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted.

User ID Credentials:
Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures:

- Identity trust verification and service-to-service application (API) and information processing inter-operability (e.g., SSO and Federation)
- Account credential life cycle management from installation through revocation
- Account credential and/or identity store minimization or re-use when feasible
- Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expireable, nonshared authentication secrets)
- Support for identity federation standards (SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users
- Strong (multifactor) authentication options (digital certs, tokens, biometrics, etc.) for user access

- Password (minimum length, age, history, complexity) and account lockout (lockout threshold, lockout duration) policy enforcement
- Mechanisms in place for unlocking accounts that have been locked out (e.g., self service via email, defined challenge questions, manual unlock)
- Utilities that can significantly manage virtualized partitions (e.g., shutdown, clone, etc.) are appropriately restricted and monitored

Examination Process:

The credentialing body shall establish remote proctoring guidelines and provide them to applicants. These shall include, but are not limited to:

- Exam scheduling process and restrictions
- **Testing Environment Restrictions.** For example:
    - You must take the exam in the same room that you scanned during the proctoring setup for the current exam. The room must have floor to ceiling walls and a door that closes.
    - The exam may not be taken in a public area.
    - No other person is allowed to enter the room while you are taking the proctored exam.
    - The lighting in the room must be bright enough to be considered “daylight” quality. Overhead lighting is preferred. If overhead lighting is not available, the source of light must not be behind you.
    - You must sit at a clean desk or table. The following items must not be on your desk or used during your proctored exam, unless posted rules for the exam specifically permit these materials: books, paper, pens, calculators, phones, etc.
    - The desk or walls around you must not have any writing.
    - You may not communicate with anyone else during the exam.
    - You may not leave the room during the exam.
    - There may be no other computers running in the exam room.
    - You may not wear headphones or ear buds.

  - The room must be as quiet as possible. Sounds such as music or television are not permitted.
- **Computer Requirements.** Such as:
  - Minimum software and hardware requirements.
  - The computer used to take the exam must not have more than one display or monitor.
  - All other programs or windows (other than the examination software) on the testing computer must be closed before the exam begins.
  - Broadband internet access requirements.
  - A webcam + microphone.

Examination Process Policies:

Policies should be in place that address issues that may occur during the examination process. These include, but are not limited to:

- Addressing examination interruption or technical problems
- Time limits
- Dealing with ADA compliance issues
- Consequences should irregularities be observed during the examination process

During the Examination:

Online proctoring provides for the effective observation of and communication with the test taker and the test environment throughout the testing session.

- The online proctoring system enables at least the observation of the workstation, desk surface and keyboard.
- The online proctoring system enables the observation of the test taker's head, torso, arms and hands.
- The online proctoring system enables the relatively unobstructed and

clear observation of the environment in which the test is being administered. The proctor may ask the examinee to use the camera to show any other area of the testing room.

- The online proctoring system enables the monitoring of sound in the testing environment.
- The online proctor can communicate to and collect information from the test taker prior to and during the testing session.
- The online proctoring system provides a way for examinees to provide feedback regarding the online proctor or the proctoring process.
- The online proctoring system provides a means for examinees to seek help prior to the start of testing and during the testing session. This could include accessing FAQs, requesting an online chat, instant messaging, phone call, etc.
- The online proctor can control the testing session, including pausing, un-pausing, suspending or canceling the test, based on established rules.
- The online proctor is capable of guiding a test taker through a restart of the test delivery system in the event that the testing session is interrupted due to technical difficulties.

Irregularities:

Online proctoring should provide for the video and audio recording of the testing session and interactions between the test taker and online proctor.

- The video and audio relevant to a security incident should be recorded and stored, including interactions between the test taker and online proctor, system logs, decisions made, etc.
- Incidents recorded and stored should be time-stamped to allow easy retrieval.
- There should be a secured online access system to the stored testing session.
- The recording should be saved for test security purposes for a specified period of time.