Castle IRB
16759 Main St, Suite #208
Wildwood, MO 63040
(888) 442-2472
www.castleirb.com

Doc Name: **Castle Policy 002 – Electronic Signature Policy**		
Corporate Owner:	**Document Type:**	**Document Date:**
Castle IRB	**Policy**	**12 FEB 2021**

1. Purpose:

To the fullest extent permitted by law, Castle IRB uses and accepts electronic signatures as the legally binding equivalent to handwritten signatures. This policy provides guidelines for the adoption of electronic signatures, including defining the circumstances under which electronic signatures will be used and accepted by Castle IRB in its business operations.

2. Definitions:

"Electronic Signature" is a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be a legally binding equivalent of the individual's handwritten signature (21 CFR 11.3(b)(7)).

"Digital Signature" is an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified (21 CFR 11.3(b)(5)).

"Handwritten Signature" is the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark (21 CFR 11.3(b)(8)).

3. General Requirements:

To ensure that Castle IRB operates in compliance with electronic signature requirements of the U.S. Food and Drug Administration's (FDA) 21 CFR Part 11: Electronic Records; Electronic Signatures, Castle IRB has adopted the following requirements:

3.1. Each electronic signature shall be unique to one individual and shall not be reused or reassigned to anyone else.

3.2. Prior to establishing, assigning, certifying or otherwise sanctioning an individual's electronic signature, Castle IRB shall verify the identity of the individual.

3.3. Castle IRB shall certify to the FDA that electronic signatures in its system are intended to be the legally binding equivalent of traditional handwritten signatures.

3.4. Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:

a. The printed name of the signer;

b. The date and time when the signature was executed; and
c. The meaning (such as review, approval, responsibility, or authorship) associated with the signature.

3.5. Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.

4. Quality Controls:

4.1. To ensure quality control of the use and acceptance of electronic signatures, Castle IRB will maintain the following electronic signature components and controls:

a. Employ at least two distinct identification components, such as an identification code and password.

b. Permit use of an electronic signature by its genuine owner.

c. Ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.

4.2. Individuals who will use electronic signatures based upon use of identification codes (ID Code) and passwords shall employ controls to ensure their security and integrity. Such controls shall be in compliance with password requirements in Sabai Policy 012 – Information Privacy and Security, and shall include:

a. Maintaining the uniqueness of each combined ID Code and password, such that no two individuals have the same ID code and password.

b. Ensuring that ID Code and password issuances are periodically checked, recalled, or revised (reset).

c. In cases where the ID code and password is lost, stolen, missing or forgotten, temporary or permanent replacements are issued using equivalent controls.

d. Use of safeguards to prevent unauthorized use of ID codes and passwords.

e. When unauthorized uses are detected, timely reports are given to the CEO of Castle IRB/Chairman of Sabai Global, IT/Operational Systems Architect, Sabai Global, and Chief Operations Officer, Sabai Global.

f. Initial and periodic testing of systems or devices that bear or generate ID codes and password information to ensure that they function properly and have not been altered in an unauthorized manner.

4.3. When business risks are not high, and laws allow it, Castle IRB may use or accept electronic signatures using a secure signing process by which an email request is sent to a signer's unique email. The signer clicks the unique link embedded in the email to access the document and apply their electronic signature. In such cases, authentication will be maintained, logged and stored in an audit trail and a certification seal will confirm the document's integrity.

a. Such instances might include the signing of consultant agreements, confidentiality agreements, or other agreements or forms outside of the scope of FDA 21 CFR Part 11.

5. Training:

5.1. In order to assure that individuals using electronic signatures subject to FDA 21 CFR Part 11 comply with this policy, training will be provided.

a. Employees are required to review this Electronic Signature Policy and Sabai Policy 012 – Information Privacy and Security and shall be trained on any systems adopted by Castle IRB to facilitate electronic signatures (e.g., Adobe Sign, IRB software systems).

b. IRB Committee Members shall be trained on main components of this Electronic Signature Policy and systems adopted by Castle IRB to facilitate electronic signatures (e.g., Adobe Sign, IRB software systems).

c. Clients who submit forms for IRB review via Castle IRB software systems will be informed that their electronic signature is the equivalent of their handwritten signature and provided guidance on appropriate use of their system user ID and password when registering for an account in the system.

6. Noncompliance:

6.1. In accordance with Sabai Policy 012 – Information Privacy and Security, violation of the standards presented in this policy may result in disciplinary action, from warnings or reprimands up to and including termination of employment or service on the Castle IRB Committee. Claims of ignorance, good intentions or using poor judgment will not be used as excuses for non-compliance.

6.2. The CEO of Castle IRB/Chairman of Sabai Global, IT/Operational Systems Architect, Sabai Global, and Chief Operations Officer, Sabai Global reserve the right to monitor, investigate, restrict, report, and take other actions necessary to protect and secure Company data. Account abuse or signs of account sharing/compromise will be dealt with swiftly and reported.

7. Procedures:

7.1. Castle IRB will adopt Electronic Signature Procedures that help to ensure compliance with 21 CFR Part 11 and this policy [see Castle Procedure 035 – Electronic Signature Procedures].

8. Revision History:

8.1. Initially approved 12-17-2019.

8.2. Revisions to include Client training information for use of Castle IRB software systems, and to update the title of the Manager of Business Communications to IT/Operational Systems Architect, Sabai Global approved 2-12-2021.