COLLEGE of CHARLESTON

OFFICIAL POLICY

11.5.1	COLLEGE OF CHARLESTON POLICY ON UNIFORM ELECTRONIC TRANSACTIONS ACT	7/26/2016

Policy Statement

It is the Policy of the College to use and accept Electronic Records and Electronic Signatures and to do so in a manner and to an extent that is fully consistent with both the UETA and the Standards.

Policy Manager and Responsible Department or Office

Information Security/ Information Technology

Policy

1.0 PURPOSE

This Policy implements the South Carolina Uniform Electronic Transactions Act ("UETA") (S.C. Code Ann. §§26-6-10 et seq.) that was enacted in 2004 and the South Carolina Standards for Electronic Signatures promulgated on February 28, 2007 (the "Standards") by the South Carolina Budget and Control Board.1 This Policy also specifies the terms and conditions under which the College will use Electronic Records and Electronic Signatures for the conduct of its business and academic operations.2

2.1 DEFINITIONS3

The following terms shall have the definition ascribed to each:

(a) "Agreement" means the bargain of the parties in fact, as found in their language or inferred from other circumstances and from rules, regulations, and procedures giving the effect of agreements under law otherwise applicable to a particular Transaction.
(b) "Computer Program" means a set of statements or instructions used directly or indirectly in an Information Processing System to bring about a certain result.
(c) "Electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.
(d) "Electronic Agent" means a Computer Program or an Electronic or other automated means used independently to initiate an action or respond to Electronic Records or performances in whole or in part, without review or action by an Individual.
(e) "Electronic Record" means a Record created, generated, sent, communicated, received, or stored by Electronic means.

1 Section 26-6-190 of UETA states, in part:
The South Carolina State Budget and Control Board shall adopt standards to coordinate, create, implement, and facilitate the use of common approaches and technical infrastructure, as appropriate, to enhance the utilization of Electronic Records, Electronic signatures, and security procedures by and for public entities of the State.
The Standards are available at: http://cio.sc.gov/NR/rdonlyres/A825AF86-8FDA-4A63-8A02- 8907639020EC/0/scrUETASCStandardsforElectronicSignatures.pdf.

2 Statutory references in this Policy will be to the South Carolina Uniform Electronic Transactions Act, unless otherwise noted. Portions of this Policy are quoted directly from the statute and the Standards or are slightly modified to more directly relate to the operations of the College.

3 S.C. Code Ann. § 26-6-20.

(f) "Electronic Signature" means an Electronic sound, symbol, or process attached to or logically associated with a Record and executed or adopted by a Person with the intent to sign the Record.
(g) "Individual" means a single natural Person; one human being.
(h) "Information" means data, text, images, sounds, codes, Computer Programs, software, databases, or other forms for the communication or reception of knowledge.
(i) "Information Processing System" means an Electronic system for creating, generating, sending, receiving, storing, displaying, or processing Information.
(j) "Person" means an Individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, governmental agency, public corporation, or other legal or commercial entity.
(k) "Record" means Information that is inscribed on a tangible medium or that is stored in an Electronic or other medium and is retrievable in perceivable form.
(l) "Transaction" means an action or set of actions occurring between two or more Persons relating to the conduct of business, commercial, or governmental affairs.

3.0 POLICY STATEMENT

It is the Policy of the College to use and accept Electronic Records and Electronic

Signatures and to do so in a manner and to an extent that is fully consistent with both the UETA and the Standards.

4.1 APPLICABILITY TO TRANSACTIONS AND RECORDS

4.2 Generally. (a) In accordance with the Standards, while Fax transmissions, voice mails, PDA communications, and tape backups are Electronic Records, they are "out of the scope of these [S]tandards."4 Consequently, unless otherwise specifically noted below, this Policy will not apply to Fax transmissions, voice mails, or PDA communications.

(b) The decision as to whether Electronic Signatures or Records may be used with respect to a particular type of Transaction or Record shall be made by Executive Vice President or Senior Vice President having management responsibility for that type of Transaction or custody over that type of Record.

4.3 Electronic Records. Except as specifically excluded by the UETA5, all Records that the

4 Standards, Section 1.2.

5 See S.C. Code Ann. §26-6-30. Neither this Policy nor the UETA is applicable, for example, to wills, codicils or testamentary trusts; an order for prescription drugs; certain sections of the Uniform Commercial Code; and several consumer notices required by law. In addition, neither this Policy nor UETA is intended to override any provision of the federal Electronic Signatures and National Commerce Act (15 USC §7001 et seq.)(the "E-Act"). Accordingly, any conflict between UETA/this Policy and the E-Act will be resolved in favor of the E-Act.

College is required to maintain under the South Carolina Public Records Act (S.C. Code Ann.
§30-1-10 et seq.) or any other provision of State law may be stored and maintained in an Electronic format, provided that all State laws, rules, regulations and guidance of particular application to each type or class of Records are observed by the custodian of the Records.

4.4 Electronic Signatures. There are four elements to a valid Electronic Signature: (1) use of a signature unique to the signer; (2) Agreement by the parties to use an Electronic Signature; (3) a clear intent to sign; and (4) association of the signature with the signed Record. When determining if the conditions are present, the College will examine the authentication of the signer, non-repudiation by the signer, and integrity of Record. 6

4.5 Originality. In the absence of any reasonable suspicion, when an Electronic Signature meeting the four elements listed in Section 4.3 is presented the College will presume the originality of the Record that has been signed. Only one version may be treated as the authoritative version and as the original Record, whether or not there are

multiple copies of that Record. If Information is added or changed to that Record it will be deemed to comprise a new version of the Record, to which the original signature no longer applies. This new Record may be stored as a separate, duplicate or ancillary Record. The version to be treated as an original signed version may not change. The new Record may in turn be signed, creating a new,
separately verifiable Electronic Signature.7

5.1 STANDARDS FOR ELECTRONIC SIGNATURES

5.2 General Rule. Electronic Signatures accepted by the College must meet the standards contained in this Section 5.0 in addition to any other standards that may be imposed by a law of specific application to the particular Record that is being signed.

5.3 Use of Signature Unique to the Signer. (a) The Electronic Signature must uniquely identify the signer, be under the reasonable control of the signer, and be unlikely of use by any unauthorized entity.

The Standards advise, in part, as follows:

The Electronic sign, symbol, or process serving as the Electronic Signature must uniquely identify the Person, business, agency, or system which is the signer of the Electronic Record, and be under the reasonable control of that party. The most commonly used form of identification in Electronic Transactions is the Personal Identification Number (PIN) or password, either assigned arbitrarily to the party by a service provider or self-selected by the party, and used in conjunction with a unique user identification. This PIN or password serves as an Electronic Signature either by being entered in response to a request to sign a Transaction, or by the party's executing an action with intent to sign, while

6 Standards, Section 1.2

7 Standards, 1.2

authenticated by the PIN or password.8

(b) The party using the Electronic Signature bears the responsibility for maintaining control and security of the relevant "sign, symbol, or process" signifying the signature. Security, however, over the means for assigning the means of creating the Electronic Signature, and for maintaining the confidentiality of the Electronic Signature received reside with the College office that has custody of the Records and administrative control over the Electronic Signature process.

5.4 Agreement by The Parties. (a) In the case of an Electronic Signature, both the signer of the signed document and the authorized College representative for that Transaction must agree, either explicitly or implicitly, that the Electronic sound, symbol, or process will serve as a signature for the Electronic document or Record.

(b) The College may negotiate separate Agreements with business concerns dealing with the use and acceptance of Electronic Signatures. Such Agreements, however, are not necessary. Participation in a Transaction by a business or Individual party containing clear and unambiguous provisions dealing with the required or permitted use of Electronic Signatures constitutes acceptance of those provisions and all other terms and conditions of the underlying Transaction.
(c) An Electronic Signature may be created by the signing party or on behalf of a party by an authorized agent, including an Electronic Agent.
(d) A party that agrees to conduct a Transaction by Electronic means may refuse to conduct other Transactions by Electronic means. This right of refusal shall not be waived by Agreement.9
5.5 Intent to Sign. The act of applying the Electronic Signature to a Record must be intentional. Intent will be inferred by the contents of the document or Record and the facts and circumstances surrounding the Transaction. The College requires a prior Agreement with the signer or clear and unambiguous notification in or accompanying the Transactional document or subject Record stating that the execution of the Transaction or authentication of the Record can or must be effected by an Electronic Signature.

5.6 Association of the Signature With the Signed Record. The Electronic Signature must be physically or logically associated with the Electronic Record that is signed, and that association must persist for as long as the Record is maintained in accord with the Records retention schedule of the College or, if the Record is maintained for a longer period for good cause, then for the life of the Record.

5.7 Notarized Signatures. A law requiring a signature or record to be notarized, acknowledged, verified, or made under oath is satisfied if the Electronic Signature of the person

8 Standards, 1.4

9 S.C. Code Ann. §26-6-50

authorized to perform those acts, together with all other information required to be included by other applicable law, is attached to or logically associated with the signature or record.10
6.1 SECURITY

6.2 Risk Assessment. (a) The Chief Information Officer of the College ("CIO") shall perform, or cause to be performed with outside consultants, as appropriate, periodic risk assessments to determine the best means of implementing Electronic Signatures and maintaining the appropriate level of security for each type of activity for which Electronic Signatures may be used. The first such assessment shall be conducted and completed by July 23, 2010. Thereafter, such assessments must be conducted no less frequently that once during each three year period.

(b) The assessment referred to in subsection (a) of this Section 6.1 shall include consideration of the following:
(i) nature and value of the data and Records in the Transactions;
(ii) susceptibility of the Transaction's data to fraud;
(iii) type of communication for the Transactions;
(iv) security of the systems which host the Transaction processes and data;
(v) reliability of the systems which host the Transaction processes and data;
(vi) consequences of successful fraud for participants, the College, and the system(s);
(vii) role and authority of the user base, especially on those systems where there are multiple levels of authorization on the data;
(viii) existing technology base and the cost of technology;
(ix) required level of confidence in establishing the users' identity;
(x) required level of communication integrity;
(xi) required level of Record integrity; and
(xii) required level of non-repudiation for Records.11

6.3 Risk Mitigation Plan. Within 30 days after the first risk assessment required under Section 6.1(a), the CIO shall prepare, and keep current, a risk mitigation plan that will detail how action will or can be taken to resolve all known risks, mitigate the risk, or have a contingency operating plan in response to a particular risk. The risk mitigation process will be fully documented. No system for the collection or use of Electronic Signatures or sensitive Records will continue to be operated if there is an unacceptable risk of unauthorized access, improper Recordation of the Transaction, or other critical failure dealing with the integrity or security of the Record. The determination of an "unacceptable risk" shall be made by the appropriate Executive or Senior Vice President having management responsibility for that type of Transaction or custody over that type of Record.

10 S.C. Code Ann. § 26-6-110

11 Standards, 3.1.

6.4 Freedom of Information Act. Because of the risk to Individual privacy and identity theft, and the need to protect critical operations and Records of the College, risk assessments and the Risk Mitigation Plan will not be provided to the general public under the provisions of the South Carolina Freedom of Information Act (S.C. Code Ann. §30-4-10 et seq.). Within the College, such assessments and Plan may only be provided to the following: the President, each member of the President's Executive Team, and upon request, to the Chair of the Board of Trustees or such other members of the Board as may be designated by the Chair. Others within the employee of the College may have access to such documents only on a need-to-know basis, as determined by the Executive Vice President for Business Affairs.

7.1 TECHNICAL OPERATING PROCEDURES

The CIO shall establish, develop, implement and maintain operating procedures to carry out this Policy and to ensure its continued effectiveness, security and ease of operation and continuing compliance with the provisions of S.C. Code Ann. §26-6-180 (B).12 In addition thereto, the CIO shall also investigate and develop capabilities for systems that would address each of the following:

12 S.C. Code Ann. §26-6-180 (B) provides:

(B) To the extent that a governmental agency uses electronic records and electronic signatures pursuant to subsection (A), the governmental agency, in consultation with the South Carolina State Budget and Control Board, giving due consideration to security, may specify:

(1) the manner and format in which the electronic records must be created, generated, sent, communicated, received, and stored and the systems established for those purposes;

(2) if electronic records must be signed by electronic means, the type of electronic signature required, the manner and format in which the electronic signature must be affixed to the electronic record, and the identity of, or criteria that must be met by, a third party used by a person filing a document to facilitate the process;

(3) control processes and procedures appropriate to ensure adequate preservation, disposition, integrity, security, confidentiality, and auditability of electronic records; and

(4) other attributes required for electronic records which are specified for corresponding nonelectric records or reasonably necessary under the circumstances.

(a) Use of Countersignatures - The capability to prove the order of application of signatures.
(b) Independent Verifiability - The capability to verify a party's Electronic signature without the cooperation of the signer.
(c) Interoperability of Electronic Signature Technology - The assurance that applications, systems or other Electronic components used during phases of communication between trading partners and/or between internal components of an entity, are able to read and correctly interpret the Transaction Information communicated from one to the other.
(d) Multiple Signatures - The capability of multiple parties to sign an Electronic Record, document or Transaction.
(e) Data Transportability - The ability of a signed document to be transported over an insecure network to another system, while maintaining the integrity of the document, including content, signatures, signature attributes, and (if present) document attributes.13

8.0 AMENDMENTS

This Policy may be amended at anytime in accordance with the Colleges Campus Wide Policy Making Procedures.

9.0 RESPONSIBILITY

The Chief Information Officer of the College shall be responsible for the maintenance of this Policy.

Sections 6.1 and 6.2 of this Policy shall become effective immediately. All other sections of the Policy shall be effective 30 days after completion of the first Risk Mitigation Plan, as further described in Section 6.2.

****

Departments/Offices Affected by the Policy

All Departments

Procedures Related to the Policy

Related Policies, Documents or Forms

Issue Date: 7/26/2016 Date of Policy Revision:7/26/2016	Next Review Date:10/26/2020

POLICY APPROVAL
(For use by the Office of the Board of Trustees or the Office of the President)

Policy Number: 11.5.1

President or
Chairman, Board of Trustees Glenn F. McNally, Pres. Date: 7/26/16