WHEREAS, The New York State Electronic Signatures and Records Act (ESRA) allows NYS governmental entities to utilize electronic signatures (e-signatures) in place of wet signatures so long as these e-signatures comply with Section 540.4 of the ESRA Regulations, which defines e-signatures, its proper usage, and requires that governmental entities "complete and document a business analysis and risk assessment when selecting an electronic signature to be used or accepted by that government entity in an electronic transaction"; and

WHEREAS, Staff across all of CUNY's academic and administrative functions process a significant volume of electronic transactions that require a handwritten ("wet") signature for authorization and over time can be expected to move many more paper transactions to electronic records; and

WHEREAS, CUNY has yet to adopt a policy that allows the University to implement and use e-signatures across its transactions under the guidelines of ESRA to eliminate significant time spent on processing documentation using wet signatures, especially for high volume transactions where multiple signatures are required (such as employee timesheets, employee personnel action forms, new hire onboarding documents, prospective and transfer student applications, and student records); and

WHEREAS, Wet signatures, which create a non-automated workflow, are inefficient, decrease productivity, and require costly purchasing of paper, ink, document storage, and other devices as required; and

WHEREAS, Following the adoption of an e-signature policy, as part of the Administrative and Academic Excellence Initiative, CUNY will begin identifying and implementing e-signatures for high volume, high priority transactions across administrative and academic areas of the University to generate cost savings on materials and increase the efficiency of University employees by reducing the time required to process wet signatures; now therefore be it

RESOLVED, That The City University of New York adopts an Electronic Signature Policy to govern the establishment and implementation of e-signatures at CUNY in accordance with the ESRA Regulations to reduce costs and increase the efficiency of processing transactions. To satisfy requirements laid out in ESRA Regulations, CUNY will conduct a business analysis and risk assessment as required by section 504.4 of the ESRA Regulations before implementing e-signatures on any transaction types.

EXPLANATION: The business analysis and risk assessment of all transactions will require approval by the Department business owner, the Central Office business owner, and a representative from Central Computing and Information Services (CUNY CIS). For transactions that are deemed high risk, CUNY Procurement will facilitate the acquisition

of an enterprise-wide third party vendor who provides high level data security for these transactions. CUNY CIS will maintain an online repository for the University that lists all transactions that have been approved for electronic signature with an attached business analysis and risk assessment that can be leveraged or referenced for similar transactions.

CUNY Electronic Signature Policy <DRAFT>

I. Purpose and Scope of the Policy

Purpose
The City University of New York (CUNY) recognizes the general standard and increased operational efficiency gained from conducting business transactions electronically. This policy establishes guidelines for units within CUNY to authorize the use of electronic signatures (e-signatures) to the fullest extent permitted by law using methods that are secure and practical.

Supporting Law
The following laws were enacted to support the use of electronic signatures:

- **Federal Law**
  The federal government authorized the use and acceptance of electronic signatures in The Electronic Signatures in Global and National Commerce Act (E-Sign) in 2000.
- **New York State Law**
  The Electronic Signatures and Records Act (ESRA), the New York state law that authorizes the acceptance of electronic signatures in most documents, went into effect in August of 1999. The Act was updated in 2002 to make New York State law consistent with the federal E-Sign law. The act provides that "signatures" made via electronic means will be as legally binding as handwritten signatures. It does not mandate the use of, or require a specific form of, electronic signature.

Scope
This policy applies to all members of the University community, including students and prospective students, employees and prospective employees, faculty, staff, volunteers in connection with University activities, business partners, affiliates, associates, and auxiliary services. It applies to all uses or potential uses of e-signatures to conduct the official business of the University, including transactions with third-party vendors and contractors.

This policy does not mandate the use of an e-signature or otherwise limit the right of a party to conduct a transaction on paper, nor does it apply to any situation where a written signature is required by law. Facsimile signatures used on checks issued by the University do not fall within the scope of this policy.

This policy does not require a specific method for acceptance of an e-signature. It authorizes the University and Computing & Information Services (University CIS) to approve the implementation method proposed by the CUNY unit, department, or administrative office if it provides the appropriate level of authentication assurance to address the identified degree of risk in each transaction as described within this policy.

Exceptions
E-Sign and ESRA contain exceptions to the general standard that e-signatures are afforded full

legal effect. These exceptions indicate when an electronically signed document is not afforded the same legal standing as a handwritten signature. A handwritten signature is required for documents or notices pertaining to:

- the transfer of real property
- eviction and foreclosure
- cancellation of health insurance or life insurance (excluding annuities)
- cancellation or termination of utility services
- the Uniform Commercial Code.
- recall of a product, or material failure of a product, that risks endangering health or safety
- any document required to accompany any transportation or handling of hazardous materials, pesticides, or other toxic or dangerous materials

Section 103 of E-Sign and section 307 of ESRA should be referenced for additional information about exceptions to the legal use of e-signatures on NYS transactions.

II. Definitions

- **Authentication** means to establish as genuine and verify the identity of a person providing an
- electronic signature.
- **Business analysis and risk assessment** refers to the process of identifying and evaluating various factors relevant to the selection of an electronic signature for use or acceptance in an electronic transaction. Such factors include, but are not limited to, relationships between parties to an electronic transaction, value of the transaction, risk of intrusion, risk of repudiation of an electronic signature, risk of fraud, functionality and convenience, business necessity and the cost of employing a particular electronic signature process.
- **Electronic signature, or "e-signature,"** is an electronic sound, symbol, or process, attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the record. E-signature does not refer to facsimile signatures used on checks issued by the University.
- **Electronic record** is any record created, used, or stored in a medium other than paper, including information processing systems, computer equipment and programs, electronic data interchanger, electronic mail, voice mail, text messages, and similar technologies. To the extent that facsimile, telex and/or telecopying, and/or former hard copy documents are retained in electronic form through a scanning process, they are also considered electronic records. An electronic record used by a person shall have the same force and effect as those records not produced by electronic means.
- **Electronic transaction, or "e-transaction,"** is a transaction conducted or performed, in whole or in part, by electronic means or electronic records. The information provided, sent, or delivered, in an electronic record must be capable of retention by the recipient at the time of receipt to qualify as an electronic transaction.
- **Governmental entity** means any State department, board, bureau, division, commission, committee, public authority, public benefit corporation, council, office, or other

governmental entity or officer of the State having statewide authority, except the state legislature, and any political subdivision of the State.

- **Approval Authority** means a business process owner designated by the college President, such as the Vice President of Administration, Provost or their designees responsible for overseeing the unit, department or administrative office proposing the use of an electronic signature.
- **Central Office Business Owner:** is the Vice Chancellor, or their designee, of the relevant functional department for which the e-signature transaction has been requested.
- **CIS Security Reviewer:** is the designated reviewer in University Computing & Information Services of proposed e-signature transactions
- **Approved electronic signature method** is one that has been approved by the Approval Authority, the Central Office Business Owner and CIS Security Reviewer in accordance with this policy and applicable state and federal laws, and which specifies the form of the electronic signature, the systems and procedures used with the electronic signature, and the significance of the use of the electronic signature.
- **Level of Assurance** is the degree of confidence in the identity of the individual providing an e-signature.

III. Policy

When a signature, approval or authorization is required for a University transaction, by law or by University policy or practice, an e-signature, approval or authorization will meet the requirement, and will be accepted as legally binding and equivalent to a handwritten signature when:

- The particular unit, office or department has designated the transaction as an appropriate e-transaction, after completing the analysis of the benefits and risk laid out below and in the CUNY E-signature Form; and
- The Approval Authority for the particular Unit, office, or department has authorized the use of e-signature for that transaction; and
- The Central Office Business Owner or their designee has approved the business and risk analysis; and
- The CIS Security Reviewer has approved the proposed electronic signature method and user authentication protocol as appropriate to establish the level of assurance needed for the degree of risk identified in the analysis.

Once the form has been approved by all three parties mentioned above, the transaction that is approved cannot materially change from what was approved.

IV. Minimum Standards

Use of an e-signature must be in accordance with the following minimum standards, consistent with NYS issued guidelines. Compliance with these standards helps to ensure the validity of an e-signature.

- Preparation:
  - Determine that the e-signature methodology will be made in accordance with specific standards outlined in this policy.

- Verify that electronically signed documents going to external agencies abide by guidelines set forth by the external agency and meet the requirements of the receiving organization.

- Processing:
  - Provide opportunity for the signer to review the entire document or content to be signed prior to applying an e-signature.
  - Make it impossible for an e-signature to be applied to a document without the signer having been informed that a signature is being applied.
  - Allow the signer's intent to be expressed as part of the record or in a certification statement submitted with and linked to the signed record.
  - Require the signer to act affirmatively to indicate assent to the document being signed. For example, require the signer to click an "Accept" button. A button allowing the signer to "Reject" could also be presented to demonstrate that a choice was made. Alternately, the signer could be required to type specific words of acceptance (e.g., "I ACCEPT" or "I AGREE").
  - Format an electronically signed record to contain the same accepted signature elements captured in a paper record allowing a reader to readily identify the significance of the signature appearing on the bottom line.

- Signature Retention:
  - Record the date, time, and fact that the signer indicated his or her intent and retain this information for evidentiary purposes. This may be different from the time the signer accessed the application or was authenticated.
  - Retain all electronically signed documents in accordance with the CUNY's Records Retention and Disposition Policy.

V. Security Requirements

CUNY Business Units that choose to use e-signatures must ensure a proper level of security and ability to link the signed document with the signer. This policy does not supersede any law or scenario wherein a written signature is specifically required (see above for specific exceptions).

Various technologies support different levels of security, authentication, record integrity, and record retention. Solutions for making an e- signature trustworthy must address the following security concerns:

- **Confidentiality**
  - Protects content from unauthorized access so that only the intended audience can view it
- **Authenticity**
  - Assures that the document truly comes from the signer
- **Integrity**
  - Detects unintentional or malicious alteration and prevents signer from refuting an e-signature document to avert any risk of repudiation and fraud
- **Security**
  - Maintains security of document from origination through the entire business process to minimize any threat of intrusion
- **Accessibility**

- Allows access to document across all platforms

In addition to business analysis and risk assessment, the E-Signature Application Form must include the signature method proposed and the rationale for choosing that method to address each of these concerns.

VI. Implementation Methods

According the NYS ESRA, a governmental entity shall complete and document a business analysis and risk assessment when selecting an e-signature method to be used or accepted by that governmental entity in an electronic transaction.

Documenting the Business Analysis and Risk Assessment

The guidelines outline the factors that should be considered in documenting the business analysis and the risk assessment. A governmental entity may elect to adopt an existing business analysis and risk assessment completed and documented by another governmental entity when selecting an e-signature for use or acceptance in the same type of electronic transaction to which the existing business analysis and risk assessment applies. A governmental entity may elect to collaborate with other governmental entities in the completion and documentation of a business analysis and risk assessment when selecting an e-signature for use or acceptance in an electronic transaction common to such governmental entities.

The E-Signature Form attached to this policy shall be submitted for all requests to use e-signature. If the requestor proposes use of an existing analysis of another governmental entity, the form specifies the documentation that is needed. If this is a new request, the form includes the factors to be documented for the business analysis, the risk assessment, and how the proposed e-signature method addresses identified risks. This form must be completed and approved by the Approval Authority, the Central Office Business Owner, and University CIS Information Security. Once fully approved, the e-signature method may be implemented. If an approved e-signature transaction undergoes any material or substantive changes, the new process must be resubmitted for approval.

Selecting an Electronic Signature Method

There are a number of approaches to implementing the use of e-signatures. The technology approach selected should support the minimum standards outlined in this policy. When choosing a technology, requestors and business owners must consider the significance of the business requirement as it relates to e-signatures. For instance, applying an e-signature to an e-mail might require little to no protection, but additional validation or security in other situations may necessitate password protection or encryption. A combination of technologies may be warranted to mitigate risks. The approaches below provide varying levels of security, authentication, record integrity, and protection against repudiation. They are roughly organized from the lowest to the highest level of security, authentication, record integrity, and non-repudiation. However, each approach can be implemented in various ways and can be combined with techniques from other approaches to increase the strength of the above-mentioned attributes.

- Click Through or Click Wrap
  - Signer is asked to click a button to demonstrate intent.
- Personal Identification Number (PIN) or Password
  - Signer is asked to enter identifying information.

- Digitized Signature
  - A digitized signature is a graphical image of a handwritten signature.
- S-Signatures
  - An S-signature is a signature inserted between forward slash marks, including any signature made by electronic or mechanical means, and any other mode of making or applying a signature other than a handwritten signature.
- Signature Dynamics
  - Signature is authenticated through automated analysis.
- Biometrics
  - Signature is authenticated by physical characteristics prior to applying his or her signature.
- Shared Private Key (Symmetric) Cryptography
  - Signature is authenticated by using a single cryptographic key (encrypts and decrypts message). This method should only be used if the keys are changed regularly to ensure a higher level of security.
- Public/Private or Asymmetric Cryptography (PKI) –
  - Digital Signature is authenticated by using two cryptographic keys, one private and one public (encrypts and decrypts message).
- Microchip Devices
  - Microchip Devices can be any device that may contain a microchip and can be used for identification purposes.

Third Party Provision of Electronic Signature Method (Certification Authority)

Where CUNY agrees to use or accept an electronic signature that involves the services of a certification authority, the certification authority shall meet the standards and operating practices described in the ESRA Regulations.

VIII. Disclaimer

Nothing in this policy is intended to authorize any individual to sign on behalf of CUNY if he or she has not been granted such authority, and such signature authority continues to be governed by University bylaws and applicable University policies. The presence of an e-signature does not mean that the signatory was authorized to sign or approve on behalf of the University.

Chairperson Thompson, Jr. asked for a vote. Cal. No. 4.C. was unanimously adopted.

Moved by Trustee Cortés-Vázquez and seconded by Trustee Clarke, resolutions 4.D. through 4.G. were presented and opened for discussion: