BOARD OF TRUSTEES

Tentative Agenda Summary for the
Regular Meeting of July 21, 2020
Subject to such additional items as members of the
Board of Trustees wish to bring before the meeting.
Teleconference # 1-646-558-8656, Meeting ID 999 6793 8059#

Teleconference # 1-646-558-8656, Meeting ID 999 6793 8059#
BOARD OF TRUSTEES
TENTATIVE AGENDA
FOR THE REGULAR MEETING OF
JULY 21, 2020
Subject to such additional items as members of the Board of Trustees wish to bring before the meeting.

1. Meeting called to order. Reading of public announcement:

   In compliance with the Open Public Meetings Act of the State of New Jersey, adequate notice of the revised format of this Regular Meeting of the Board of Trustees was provided on July 15, 2020. Advance written notice of this meeting was posted on the County College of Morris webpage, was sent to the Star Ledger and Daily Record, and was filed with the Clerk of the County of Morris.

   The meeting agenda and referenced attachments are made available to the public and can be accessed on the CCM website at the following link: https://www.ccm.edu/trustees/public-meeting-schedule-agenda/ .

   I direct that this public announcement be entered in the minutes of this meeting.

2. Roll Call

3. Administration of Oath of Office to the Freeholder Appointed Trustee, Lauren Inganamort, for a term through October 31, 2023, and Alumni Trustee Emma Mendoza for a term through June 30, 2021.

   I, *Lauren Inganamort / Emma Mendoza*, do solemnly swear that I will support the Constitution of the United States and the Constitution of the State of New Jersey, and that I will bear true faith and allegiance to the same, and to the Governments established in the United States and in this State, under the authority of the people, and that I will faithfully, impartially and justly perform all of the duties of the Office of Trustee according to the best of my ability, so help me God.

4. Adoption of resolution to discuss matters in closed session.

   RESOLVED, At the Regular Meeting of the Board of Trustees on July 21, 2020, that pursuant to Sections 7 and 8 of the Open Public Meetings Act, the following subjects be discussed in a session closed to the public at approximately 6:00 p.m., via teleconference.
   1. Compensation for Professional Services
   2. Acceptance of Employee Resignations, Retirements, and Terminations
   3. New Employee Appointments

4. Adjunct Faculty Appointments and Salaries, Summer Semesters
5. Recall of Furloughed Employee
6. Reorganization of Departments in the Business and Finance Division
7. Matters involving the attorney-client privilege.

It is anticipated that all of the above items will be disclosed to the public at the reconvened session of the Board at 6:30 p.m. with the exception of Item #7.

5. Pledge of Allegiance

   A. Moment of Silence

6. Consideration of the minutes of the regular meeting of June 16, 2020

7. Report of the President – Dr. Iacono

   A. Advanced Manufacturing and Engineering Center Update– Vice President Karen VanDerhoof

8. Report of the Treasurer – Trustee Licitra

   A. RESOLVED, That the check numbered 27935 in the amount of $1,316,970.00 be approved and payment authorized for capital improvements.

   B. RESOLVED, That in accordance with the County College Contracts Law, a purchase order be issued to the following vendor through the Joint Purchase Agreements - Consortium:

Co-Op #	Description	Vendor	Amount
ESCNJ 1819-67	Computers	Apple Computer Freemont, CA	$63,920.00

   13-inch MacBook Pro: 3.6GHz Retina Display Intel Core i5 - 40 @ $1,399.00 each = $55,960.00 funded by CARES Act; Three Year AppleCare Protection Plan 40 @ $199.00 each = $7,960.00 funded by the Technology Plan. For Information Systems.

9. Committee on Personnel – Trustee Weisberg

   A. BE IT RESOLVED, That the Board of Trustees approve compensation for those persons listed on Attachment #1 for professional services to the College for the purposes stated on Attachment #1.

Attachment #1 is on pages 6 through 7.

B. BE IT RESOLVED, That the Board of Trustees approve the acceptance of the following employee resignations, retirements, and termination:

David Ackerman; retirement effective 06/26/20
Bonnie Ayres; resignation effective 06/30/20
Stuart Bidgood, termination effective 07/17/20
Barry Bilinkas; retirement effective 07/15/20
Cheryl Borer; retirement effective 09/18/20
Sara Dolan; resignation effective 06/24/20
Elizabeth Fitzgerald; resignation effective 06/24/20
Joseph Moore; resignation effective 07/01/20
Miriam Pottinger; retirement effective 07/31/20
Jennifer Ryan; resignation effective 06/24/20
John Young; resignation effective 07/17/20
Jean Wallace; termination effective 07/17/20

C. BE IT RESOLVED, That the new employee appointments listed on Attachment #2 be approved.

Attachment #2 is on page 8.

D. BE IT RESOLVED, That the adjunct faculty appointments and salaries for the Summer 20SU5E and Summer 20SU10W semesters be approved as stated on Attachment #3.

Attachment #3 is on pages 9 through 10.

E. WHEREAS, Governor Murphy has lifted the restrictions for indoor swimming pool facilities put in place as a result of the COVID-19 global pandemic; and

WHEREAS, the County College of Morris has received requests to rent the aquatic facility;

NOW THEREFORE BE IT RESOLVED, That Krystal Hoffman, Aquatics Supervisor, AAPF, be recalled from furlough effective July 13, 2020.

F. WHEREAS, The Personnel Committee has reviewed the rationale for the following reclassifications in the Business and Finance Division;

NOW THEREFORE BE IT RESOLVED, That upon the recommendation of the Personnel Committee and the President, the Board authorizes the following reclassifications:

- Reclassify the position of College Architect and Director of Facilities Planning, to Assistant Vice President for Business and Finance, Management Grade 37, at an annual salary of $135,000 effective July 22, 2020;
- Reclassify the vacant position of Director of Budget and Compliance, to Budget and Compliance Manager, Management Grade 33;
- Reclassify the position of Manager of Purchasing, AAPF Grade 19, to Director of Purchasing, Management Grade 34, at an annual salary of $91,000 effective July 22, 2020;
- Reclassify the vacant position of Purchasing Specialist, CCMSA Grade G-35, to Technical Purchasing Agent, AAPF Grade 14;
- Reclassify the position of Buyer, CCMSA Grade F-35, to Technical Purchasing Agent, AAPF Grade 14, at an annual salary of $54,673 effective July 22, 2020.

BE IT FURTHER RESOLVED, That the vacant Purchasing Coordinator. CCMSA Grade E-35 position be permanently eliminated.

G. BE IT RESOLVED, That the Board of Trustees of the County College of Morris approve and adopt the revisions to Infectious Disease Control Policy for Employees as indicated on Attachment #4.

Attachment #4 is on pages 11 through 14.

10. Committee on Finance and Budget – Trustee Aprile

A. RESOLVED, That the contracts for sign language interpreter services and CART services be awarded to Sign4U Interpreting Services and CART services be awarded to SignGlasses LLC as indicated on Attachment #5.

Attachment #5 is on page 15.

B. BE IT RESOLVED, that the following contracts not solicited by public advertisement, be awarded based upon preclusion from consideration for the contract award of any contractor who is ineligible under N.J.S.A. 19:44A-20.4 by reason of a reportable political contribution.

Contractor	**Nature of Contract**	**Term of Contract**	**Estimated Contract Value**
Ad Astra Information Systems, LLC	Data consultant services	07/22/20 – 07/21/22	$145,000.00
Philadelphia Press	Books for resale	07/01/20 – 06/30/22	Will exceed $17,500.00

The forms of resolution hereby adopted awarding the contract is set forth in Attachment #6.

Attachment #6 is on pages 16 through 17.

11. Committee on Audit – Trustee Aprile

    A. BE IT RESOLVED, That the Board of Trustees of the County College of Morris approve and adopt an Information Security Program Policy as indicated on Attachment #7.

    Attachment #7 is on pages 18 through 22.

    B. BE IT RESOLVED, That the Board of Trustees of the County College of Morris approve and adopt the revisions to the Data Security Policy as indicated on Attachment #8.

    Attachment #8 is on pages 23 through 28.

12. Committee on Organization, Bylaws, Planning, and Nomination – Trustee Advokat

13. Any matters to be brought to the attention of the Board by officers of the Board

14. Unfinished business

15. New business

16. Comments from the public

17. Adjournment

REMUNERATION FOR PROFESSIONAL SERVICES

Name	Date(s) of Service	Payment	Reason
Bahner, Hilda	05/19/20-07/02/20	$1,512.00	ESL Early Beginner, Pt. 2/3 for WFD
Bamford, Colleen	02/01/19-07/15/20	$1,500.00	Course Design for Virtual Campus (CMP128 Computer Science I)
Binowski, Nancy	01/01/19-06/15/20	$1,500.00	Course Design for Virtual Campus (CMP239 Internet & Web Page Design)
Bowman, Isabel Maria	05/19/20-07/02/20	$1,316.00	ESL Beginner, Pt. 2/3 for WFD
Breiten, James	03/01/19-08/15/19	$1,500.00	Course Design for Virtual Campus (PBH101 Principles of Public Health)
Crespo-DiStefan Leonor	04/25/20-06/13/20	$882.00	QuickBooks Essentials for WFD
Cutrone, Marco	01/01/19-05/30/20	$500.00	Gallery Assistant
Faines, Ronald	05/26/20-05/28/20	$408.00	C109 - Compulsive Gambling for WFD
Faines, Ronald	06/09/20-06/11/20	$408.00	C201 - Introduction to Counseling for WFD
Faines, Ronald	06/16/20-06/18/20	$408.00	C202 - Introduction to Techniques & Approaches for WFD
Ferreira, Sharon	05/18/20-06/10/20 & 06/15/20-07/06/20	$1,428.00	ESL Advanced for WFD
Fitzpatrick, Kelly	04/05/20-06/09/20	$500.00	Program Development - Tableau II, III, IV for WFD
Fitzpatrick, Kelly	06/02/20-06/11/20	$600.00	Tableau Part IV - 13 Students for WFD
Fulton, Diane	06/08/20-06/17/20	$658.00	Physician's Practice Management and Regulatory Issues (Accelerated) for WFD
Gigliotti, Samantha	01/01/19-06/15/20	$1,500.00	Course Design for Virtual Campus (BIO127 Env. Bio Concerns)
Gordon, Ramon	05/19/20-06/11/20 & 06/16/20-07/02/20	$1,428.00	ESL Early Beginner, Pt. 2/3 for WFD
Grundfest, Robert	06/08/20-06/29/20	$705.00	NPTNJ Introduction to Teaching - 50 Hour Preservice Component for WFD
Lemme, Bryan	03/01/20-05/31/20	$5,912.00	Co-Director Center for Teaching and Learning - Remote Assistance
Lemme, Bryan	03/01/20-05/31/20	$2,015.00	Co-Director Center for Teaching and Learning - Remote Training
Lilley, R. Jeff	06/05/2020	$350.00	Six Sigma: an Introduction for WFD
Martino, Nicole	05/18/20-06/10/20 & 06/15/20-07/06/20	$1,316.00	ESL Beginner, Part 1 for WFD
McNeil, Kathleen	09/19-05/20	$2,000.00	Advisor to the Promethean for Campus Life
Petti, Ciro	04/29/20-05/01/20	$810.00	Microsoft Project 2016 for WFD
Petti, Ciro	05/02/20-06/17/20	$2,079.00	Project Management PMP, CAPM Prep for WFD
Pietropollo, Frank	Spring Semester 2020	$150.00	Facilitate Shindig and TechSmith Relay Learning Session - Training
Poetsch, Deborah	03/01/20-05/31/20	$1,950.00	Co-Director Center for Teaching and Learning - Remote Assistance
Poetsch, Deborah	03/01/20-05/31/20	$1,650.00	Co-Director Center for Teaching and Learning - Remote Training
Pravec, Norma	05/18/20-06/10/20 & 06/15/20-07/06/20	$1,428.00	ESL Intermediate Pt. 2/3 for WFD

Name	Date(s) of Service	Payment	Reason
Rothman, Nancy	03/23/20-06/02/20	$850.00	CNA Program coordination, candidate screening, scheduling and CAN makeup for WFD
Swern, Lauren	05/27/2020	$94.00	Ethics in Grant Writing for WFD
Taylor, Anna	05/18/20-06/10/20 & 06/15/20 to 07/06/20	$1,316.00	ESL Intermediate - Part 3 for WFD
Viola, Thomas	05/27/20-06/01/20	$282.00	C509 - Community Involvement for WFD
Viola, Thomas	06/08/20-06/10/20	$282.00	C101 - Initial Interviewing Process for WFD
Viola, Thomas	06/15/20-06/24/20	$564.00	C102 - Biopsychosocial Assessment for WFD
Williams-Bogar, Rita	05/18/20-05/21/20	$636.00	Outlook for WFD Business Solutions
Williams-Bogar, Rita	06/02/20-06/08/20	$848.00	MS Teams for WFD Business Solutions for WFD
Williams-Bogar, Rita	06/09/20-06/11/20	$318.00	Microsoft Teams - Collaborative Communication in the Workplace for WFD
Williams-Bogar, Rita	06/11/20-06/12/20	$212.00	Leading and Managing Remotely for WFD
Zejnullahi, Rreze	03/28/20-06/06/20	$1,200.00	Excel Essentials - end date extended from 5/30/20

RATIONALE:	NAME:	EFFECTIVE DATE:	ACTION/ POSITION:	SALARY/ WAGE:
CCMSA:				
NEW	Wills, Emily	27-Jul-20	***Appointed to:*** ***GRANT FUNDED*** HealthWorks Success Coach Workforce Development	$42,057
REPLACEMENT	Hamilton, Craig	23-Jul-20	***Appointed to:*** Custodian II (Evenings) Plant & Maintenance	$35,523
PART-TIME:				
REPLACEMENT	Dixon, Patricia	22-Jun-20	***Appointed to:*** PT Administrative Assistant Communication	$14.00ph
TEMPORARY:				
TEMPORARY	Segan, David	29-Jun-20	***Appointed to:*** ***GRANT FUNDED*** Fellowship Climate Corps Fellowship Grant	$12,500

ADJUNCT FACULTY APPOINTMENTS AND SALARIES
Summer 5E 2020

DEPT NAME	LAST	FIRST	SALARY
LGESL	Miers	Brenda	$ 5,285.00
LGESL	Moch Arias	Rita	$ 3,380.00
LGESL	Morales	Vita	$ 6,760.00
LGESL	Schwenk-Alcala	Yajana	$ 3,020.00
AAD	Cutrone	Marco	$ 4,225.00
ENGPH	Furlong	Thomas	$ 1,436.50
ENGPH	Giffoniello	Michael	$ 6,760.00
ENGPH	McKinney	Kellie	$ 2,112.50
COM	Lenar Cummins	Danielle	$ 5,915.00
AAD	Schwartz	Nicole	$ 3,775.00
SAHS	Gattie	Kenneth	$ 3,020.00
SAHS	Kloby	Gerald	$ 5,070.00
SAHS	Reinschmidt	Richard	$ 3,380.00
PSY	Brodhead	Sheila	$ 3,380.00
PSY	Finn	Kim	$ 3,380.00
PSY	Maret	Stephen	$ 4,077.00
HIS	Lorenzo	William	$ 6,760.00
CJS	Hurd	John	$ 5,070.00
BUS	Caplin	Glen	$ 3,380.00
BUS	Katz	Joel	$ 755.00
BUS	Rodriguez	Sugeily	$ 755.00
AAD	Santangelo-Mosley	Linda	$ 1,612.43
MATH	Elmuccio	John	$ 2,535.00
MATH	McCracken	Jennifer	$ 3,380.00
MATH	McLoughlin	Robert	$ 3,380.00
MATH	Shah	Grishma	$ 3,775.00
MATH	Shoenfelt	Nanette	$ 2,535.00
MATH	Theis	John	$ 3,775.00
ESET	Messano	Al	$ 4,026.67
IT	Adamczyk	Barbara	$ 5,633.33
IT	Agar	John	$ 3,523.33
HES	DeNure	Brenda	$ 1,971.67
HES	Huber	William	$ 1,971.67
HES	Run-Kowzun	Trayer	$ 3,943.33
RAD	Badini	Alannah	$ 6,071.71
RAD	Niemczyk	Faye	$ 6,071.71
BIOCHM	Firooznia	Fariborz	$ 7,361.00

ADJUNCT FACULTY APPOINTMENTS AND SALARIES
Summer 10W 2020

DEPT NAME	LAST	FIRST	SALARY
MATH	Demirel	Emel	$4,225.00
MATH	Garlick	Dale	$4,225.00
MATH	Mathus	Lisa	$2,112.50
IT	Agar	John	$3,271.67
IT	Pisciotta	Barbara	$3,661.67

INFECTIOUS DISEASE CONTROL POLICY FOR COLLEGE EMPLOYEES

It is the goal of County College of Morris (CCM) in the event of an infectious disease outbreak to strive to operate effectively and ensure that all essential services are continuously provided and that employees are safe within the workplace. CCM will take proactive steps to protect the workplace during any such time period.

CCM is committed to providing authoritative information about the nature and spread of infectious diseases, including symptoms and signs to watch for, as well as required steps to be taken in the event of an illness or outbreak.

In the event of an infectious disease outbreak, this *policy* and related procedures replaces and *supersedes* any other college *policies* and procedures on the following topics. It is understood that the policies herein are subject to change upon directives from Local, State and Federal agencies.

Preventing the Spread of Infection in the Workplace

CCM will foster a clean workplace, including the regular cleaning of objects and areas that are frequently used, such as bathrooms, breakrooms, conference rooms, door handles and railings. An emergency management team will be designated to monitor and coordinate events around an infectious disease outbreak, as well as to create work rules that could be implemented to promote safety through infection control.

We ask all employees to cooperate in taking steps to reduce the transmission of infectious disease in the workplace. The best strategy remains the most obvious—frequent hand washing with warm, soapy water; covering your mouth whenever you sneeze or cough; and discarding used tissues in wastebaskets. We will also maintain alcohol-based hand sanitizers throughout the workplace and in common areas. **We require employees to practice social distancing as much as possible and may change work schedules and/or locations if social distancing cannot be accomplished within the regular work environment.**

Unless otherwise notified, our normal attendance and leave policies will remain in place. Individuals who believe they may face particular challenges reporting to work due to an infectious disease outbreak not related to CCM, should take steps to develop any necessary contingency plans. For example, employees might want to arrange for alternative sources of child care should schools close and/or speak with supervisors about the potential to work from home temporarily or on an alternative work schedule.

Travel

During periods of an infectious disease outbreak, travel will be restricted. Employees are not permitted to travel out of state for college purposes without approval from their respective vice president. Business-related travel out of the continental United States must receive the approval

Code:
New text
~~Deleted text~~

of the college president and the chair of the Board of Trustees. Employees traveling to or employees returning from travel to locations designated by the CDC **or New Jersey State Government** as a threat are required to notify their Vice President and the Office of Human Resources before returning to campus. The employee will be required to follow the CDC recommendations for self and/or public health official imposed quarantine. These employees will not be permitted on campus without medical certification. The college reserves the right to require a second medical opinion. Current leave policies will be applied to these types of absences. Employees should check the College website regularly for updates to restrictions which may change rapidly.

Staying Home When Ill

Many times, with the best of intentions, employees report to work even though they feel ill. During the pendency of an infectious disease outbreak, we encourage employees with symptoms of communicable diseases to stay home. We provide paid sick time and other benefits to compensate employees who are unable to work due to illness. Review your union contract or contact Human Resources for additional information.

During an infectious disease outbreak, it is critical that employees do not report to work while they are ill and/or experiencing the following symptoms which may include **but are not limited to** fever, cough, sore throat, runny or stuffy nose, body aches, headache, chills ~~and~~ **or** fatigue. Currently, the Centers for Disease Control and Prevention recommends that people with an infectious illness such as the flu remain at home until at least ~~24~~ **72** hours after they are symptom free without the use **of** medications. Employees who report to work while ill will be sent home on sick leave in accordance with these health guidelines. The appropriate Vice President and Human Resources should be contacted; however, before sending the employee home.

Requests for Medical Information and/or Documentation

If you are out sick or show symptoms of being ill, it may become necessary to request information from you and/or your health care provider. In general, the Office of Human Resources will request medical information to confirm your need to be absent, to show whether and how an absence relates to the infection, and to know that it is appropriate for you to return to work. As always, we expect and appreciate your cooperation if and when medical information is sought.

Confidentiality of Medical Information

Our policy is to treat any medical information as a confidential medical record. In furtherance of this policy, any disclosure of medical information is in limited circumstances with supervisors, managers, first aid and safety personnel, and government officials as required by law.

Request for Temporary Alternative Work Arrangement and/or Accommodation

Employees considered vulnerable due to underlying health concerns during an outbreak and/or with concerns about their personal safety and/or the safety of relatives with compromised immune systems may request an alternative work arrangement and/or a leave of absence within the guidelines of federal and state sick leave laws, collective bargaining agreements and Board of Trustees policy. The employee should discuss their circumstances with their direct supervisor first. The Division Vice President; in consultation with the Office of Human Resources, will review the employee's request for an accommodation for final approval. In the case of a medical leave, documentation from a health provider will be required, as permissible by HIPAA, and should be sent to the Office of Human Resources only. HIPAA guidelines will continue to be followed to ensure the confidentiality of the employee's medical information.

Social Distancing Guidelines for Workplace Infectious Disease Outbreaks

In the event of an infectious disease outbreak impacting the CCM community, CCM may issue directives implementing social distancing guidelines to minimize the spread of the disease among the staff and students.

During the workday, employees will be required to:

1. Participate in daily temperature checks before being permitted entry to buildings on campus.

2. Wear Personal Protection Equipment (i.e., masks, cloth face coverings, rubber gloves, etc.) when two or more persons are present. Employees who have a medical reason for not wearing PPE should notify their supervisor and Human Resources. Employees not wearing PPE may be required to leave the worksite.

3. Avoid meeting people face-to-face. Employees are encouraged to use the telephone, online conferencing, e-mail or instant messaging to conduct business as much as possible, even when participants are in the same building.

4. ~~If~~ **When** a face-to-face meeting is unavoidable, minimize the meeting time, choose a large meeting room and sit at least ~~one yard~~ **six feet** from each other if possible; avoid person-to-person contact such as shaking hands.

5. Avoid any unnecessary travel and cancel or postpone nonessential meetings, gatherings, workshops and training sessions.

6. Avoid congregating in work rooms, pantries, copier rooms or other areas where people socialize.

7. Bring lunch and eat at your desk or away from others (avoid lunchrooms and crowded restaurants). **If you leave the campus, you must have a temperature check upon return.**

8. Encourage others to request information and orders via phone and e-mail in order to minimize person-to-person contact. Have the orders, materials and information ready for fast pick-up or delivery.

9. Work staggered schedules or work remotely (if the position may be performed remotely) if social distancing is difficult to maintain.

Code:
New text
~~Deleted text~~

10. Notify their supervisor and Human Resources if they exhibit symptoms of an infectious disease while at work. The employee must leave campus or isolate themselves in the Health Office until transportation can be arranged.

Essential Personnel

Each division Vice President will designate essential personnel needed to staff emergency operations in the event of a partial or total closure of the college. Essential personnel may be required to report to the campus or may be designated to work remotely. The college will issue computer equipment as necessary. Essential personnel who fail to report for duty may be subject to disciplinary action unless documentation is provided to certify the illness of the employee and/or a member of the employee's family. **Comp time or overtime must be approved in advance of the employee working additional hours.**

Code:
New text
~~Deleted text~~

RESOLUTION AUTHORIZING CONTRACT OVER $17,500
FOLLOWING PUBLICLY ADVERTISED SOLICITATION
CONTRACT FOR SIGN LANGUAGE INTERPRETER AGENCIES
AND CART SERVICES

WHEREAS, the County College of Morris ("College") has a need to acquire sign language interpreter agency services and CART services; and

WHEREAS, the purchasing agent has determined and certified in writing that the estimated value of the full term of the contracts for the above services exceeds $17,500.00; and

WHEREAS, the anticipated term of these contracts is one year commencing July 1, 2020 through June 30, 2021 with an option to renew for one additional year; and

WHEREAS, notice of request for proposals for the above contracts was publicly advertised on May 12, 2020 on the CCM website; and

WHEREAS, the solicitation of proposals is based upon a request for proposals for sign language interpreter agencies and CART services dated May 12, 2020 (the "RFP"), which sets forth the contract terms and specifications of the proposals solicited, including the criteria to be used as the basis of the contract award; and

WHEREAS, two proposals were received and opened on May 27, 2020; and

WHEREAS, sufficient funds are available to pay for the aforesaid services or goods;

NOW THEREFORE, BE IT RESOLVED by the Board of Trustees of the County College of Morris that a contract be awarded to: Sign4U Interpreting Services (1st placement for sign language interpreters and on-site CART Services, and 2nd placement for remote CART services) ("Contractor") and to SignGlasses LLC (1st placement remote CART services) ("Contractor") for a one-year contract term from July 1, 2020 through June 30, 2021 to provide sign language interpreting services and CART services. These contract awards are based upon determination that the named Contractors have submitted the lowest responsible proposal and have submitted the most advantageous proposal, price and other factors considered.

These Contracts are awarded pursuant to a fair and open contract solicitation process.

The form of contract shall be approved by the attorney for the College.

RESOLUTION AUTHORIZING CONTRACT OVER $17,500 WITHOUT PUBLICLY ADVERTISED SOLICITATION CONTRACT FOR DATA CONSULTANT SERVICES

WHEREAS, the County College of Morris ("College") had a need to acquire Data Consultant Services for Student-Centered Academic Planning and Scheduling; and

WHEREAS, the purchasing agent has determined and certified in writing that the value of the full term of the contract for the above services is $145,000.00; and

WHEREAS, the anticipated term of this contract is two year(s) commencing July 22, 2020 through July 21, 2022; and

WHEREAS, in lieu of a publicly advertised solicitation of proposals, the College has precluded from consideration for the agreement award, any contractor who is ineligible under N.J.S.A. 19:44A-20.4 by reason of a reportable political contribution; and

WHEREAS, Ad Astra Information Systems, LLC ("Contractor") has submitted a proposal dated May 29, 2020 indicating that Contractor will provide the Data Consultant Services for Student-Centered Academic Planning and Scheduling for a value of $145,00.00; and

WHEREAS, Contractor has completed and submitted a Business Entity Disclosure Certification which certifies that Contractor has not made any reportable contributions to a political or candidate committee representing an elected official of the County of Morris in the previous one year, and Contractor has agreed to contract language prohibiting Contractor from making such reportable contributions during the term of the contract; and

WHEREAS, Contractor has completed and submitted ten days in advance of adoption of this resolution, a Chapter 271 Political Contribution Disclosure form which will be placed on file with this resolution; and

WHEREAS, sufficient funds are available to pay for the aforesaid services or goods;

NOW THEREFORE, BE IT RESOLVED that the Board of Trustees of the County College of Morris authorizes the College to enter into a contract with the above identified Contractor on an as needed basis; and

BE IT FURTHER RESOLVED that the Business Disclosure Entity Certification and the Determination of Estimated Value be placed on file with this resolution.

RESOLUTION AUTHORIZING CONTRACT OVER $17,500
WITHOUT PUBLICLY ADVERTISED SOLICITATION
CONTRACT FOR BOOKS FOR RESALE

WHEREAS, the County College of Morris ("College") had a need to acquire books for resale; and

WHEREAS, the purchasing agent has determined and certified in writing that the value of the full term of the contract for the above goods will exceed $17,500.00 and is not available from more than one source; and

WHEREAS, for the foregoing reasons the purchase is exempt from requirements for public advertising under N.J.S.A. 18A:64A-25.5(6); and

WHEREAS, the anticipated term of this contract is two years commencing July 1, 2020 through June 30, 2022; and

WHEREAS, in lieu of a publicly advertised solicitation of proposals, the College has precluded from consideration for the agreement award, any contractor who is ineligible under N.J.S.A. 19:44A-20.4 by reason of a reportable political contribution; and

WHEREAS, Philadelphia Press ("Contractor") is a Sole Source Contractor and will provide books for resale exceeding $17,500.00 based upon the published wholesale price on the date of the order; and

WHEREAS, Contractor has completed and submitted a Business Entity Disclosure Certification which certifies that Contractor has not made any reportable contributions to a political or candidate committee representing an elected official of the County of Morris in the previous one year, and Contractor has agreed to contract language prohibiting Contractor from making such reportable contributions during the term of the contract; and

WHEREAS, Contractor has completed and submitted ten days in advance of adoption of this resolution, a Chapter 271 Political Contribution Disclosure form which will be placed on file with this resolution; and

WHEREAS, sufficient funds are available to pay for the aforesaid services or goods;

NOW THEREFORE, BE IT RESOLVED that the Board of Trustees of the County College of Morris authorizes the College to enter into a contract with the above identified Contractor on an as needed basis; and

BE IT FURTHER RESOLVED that the Business Disclosure Entity Certification and the Determination of Estimated Value be placed on file with this resolution.

INFORMATION SECURITY PROGRAM
(and the Gramm Leach Bliley Act (GLBA)
General Policy

INTRODUCTION

The County College of Morris recognizes and respects the importance of personal privacy for our customers. We are aware of the sensitive nature of the personal information we use in providing educational services and take reasonable precautions to protect our customer's privacy. Employees, vendors and agents of the County College of Morris (the college) have a responsibility to protect the confidentiality of all customer information.

The College is bound by state and federal laws to protect the information the customer entrusts to us. The Gramm-Leach-Bliley Act (GLBA), Family Education Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), Fair and Accurate Credit Transaction Act (FACTA), and various other laws, regulations and industry standards provide the basis for the framework upon which we build our policies and procedures pertaining to safeguarding the privacy of customer information.

PURPOSE AND SCOPE

This information security program policy implements sections 501 and 505 (b)(2) of the Gramm-Leach-Bliley Act (GLBA), as promulgated under 16 CFR Part 314, to establish standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.
In addition to the information required to be protected under GLBA, the College shall protect all other sensitive personal identifiable information. Collectively this information will be referred to as "Customer Information".

DEFINITIONS

Customer Information: Any record containing nonpublic personally identifiable information (PII) that is not publicly available whether in paper, electronic, or other form, that is handled or maintained by or on the behalf of the College.

Information Security Program: The administrative, technical, and physical safeguards used to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.

Service Provider: Any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services with the College.

Relevant Area: Any office or department that has access to customer information.

STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

The safeguards included in the College's information security program policy are reasonably designed to:
(a) Ensure the security and confidentiality of customer information;
(b) Protect against anticipated threats to the security or integrity of such information; and
(c) Protect against unauthorized access to or use of such information that could result in harm or inconvenience to any customer.

POLICY ELEMENTS

(a) Designated Customer Information Security Program Coordinator

County College of Morris has designated the Director of Network and User Services as the Information Security Program Coordinator. The Coordinator is responsible for implementing and maintaining the College's Information Security Program.

The Coordinator will identify and maintain a listing of relevant areas of the College with access to customer information.

The Coordinator will ensure that risk assessments and monitoring are carried out for each relevant area, as well as system-wide risks and that appropriate controls are in place for the identified risks.

The Coordinator will ensure adequate and routine training and education is available and is provided to all employees with access to customer information.

The Coordinator will, in consultation with other College offices, verify that existing policies, procedures and guidelines that provide for the security of customer information are adequate and routinely reviewed. The Coordinator shall make recommendation for revisions to and development of policies, procedures and guidelines, as appropriate.

The Coordinator will prepare an annual report on the effectiveness of the information security program. The report shall include current risk assessments performed for each relevant area, actions taken or to be taken to correct any security concerns identified, and any other information as required to provide assurance that this Information Security Program is implemented and maintained.

The Coordinator will maintain a consolidated "Information Policy and Procedure Manual" which includes this policy, each relevant area's documented procedures, and other regulatory information pertaining to the safeguarding of customer information.

(b) Identify and Assess Risks

The Information Security Program is intended to identify reasonable foreseeable external and internal risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or otherwise compromise such information, and assess the sufficiency of any safeguards in place to control these risks.

Risk assessments will include a review of system-wide controls, testing, triggering events and monitoring activities, as well as risks unique to each relevant area with access to customer information.

Risk assessments at a minimum will include consideration of activities in each relevant area's operations, including:

(1) Employee awareness, training and management oversight.
(2) Information systems including network and software design, as well as information processing, storage, transmission, and disposal.
(3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.
(4) Preventative and detection controls

(c) Design and Routinely Test/Monitor Safeguards

Design and implement information safeguards to control the risks identified through risk assessment. The Coordinator will ensure the effectiveness of the safeguards' key controls, systems, and procedures are routinely tested and monitored.

Such safeguards, and their ongoing testing and monitoring will include the following:

(1) Employee Training and Management Oversight

Safeguards for security will include training of those individuals with authorized access to customer information. The College has adopted comprehensive policies, standards and guidelines for preserving the security of private information, including customer information.

The Coordinator will, working with relevant areas, identify categories of employees or others who have access to customer information. While each relevant area's manager is ultimately responsible for ensuring compliance with information security practices, the Coordinator will work in cooperation with each relevant area and Human Resources to develop training and education programs for all employees who have access to customer information. Training will include education on relevant policies and procedures and other safeguards in place or developed to protect customer information.

All college personnel will be required to take information security awareness training at least one time in an academic year.

Other safeguards will also be used, as appropriate, including job-specific training on maintaining security and confidentiality, requiring user-specific passwords and require passwords be based upon National Institute of Standards and Technology (NIST) guidelines, limiting access to customer information to those with a business need for access to information, requiring signed certification of responsibilities prior to authorizing access to systems containing customer information, requiring signed releases for disclosure of customer information, establishing methods for prompt reporting of loss or theft of customer information or media upon which customer information may be stored, and other measures that provide reasonable safeguards based upon the risks identified.

(2) Information Systems

Information systems include network and software design, as well as information processing, storage, transmission, retrieval, and disposal.

Network and software systems will be reasonably designed to limit the risk of unauthorized access to customer information. This may include maintaining appropriate screening programs to detect attempts of unauthorized intrusions by means of hacking and viruses.

Safeguards for information processing, storage, transmission, retrieval and disposal may include, requiring electronic customer information be entered into a secure, password-protected system; using secure connections to transmit data outside the College network; using secure servers; encrypting transmitted customer information; ensuring customer information is not stored on transportable media (floppy drives, zipdrives, etc); permanently erasing customer information from computers, diskettes, magnetic tapes, hard drives, or other electronic media before re-selling, transferring, recycling, or disposal; storing physical records in a secure area and limiting access to that area; providing safeguards to protect customer information and systems from physical hazards such as fire or water damage; disposing of outdated records under a documented disposal policy; shredding confidential information before disposal; maintaining an inventory of servers or computers containing customer information; and other reasonable measures to secure customer information during its life cycle in the College's possession and control.

(3) Managing System Failures

The College will maintain effective systems to prevent, detect, and respond to attacks, intrusions and other system failures. Such systems may include maintaining and implementing current anti-virus software; checking with software venders and others to regularly obtain and installing patches to correct software vulnerabilities; maintaining appropriate filtering or firewall technologies; alerting those with access to customer information of threats to security; backing up data regularly and storing back up

information off site, as well as other reasonable measures to protect the integrity and safety of information systems.

(4) Monitoring and Testing

Monitoring will be conducted to reasonably ensure that safeguards are being followed, and to swiftly detect and correct breakdowns in security. The level of monitoring will be appropriate based upon the potential impact and probability of the risks identified, as well as the sensitivity of the information provided. Monitoring may include sampling, system checks, reports of access to systems, reviews of logs, audits, and any other reasonable measures adequate to verify that the information security program's controls, systems and procedures are working.

(d) Oversight of Service Providers

(1) The County College of Morris will take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and

(2) Require service providers by contract to implement and maintain such safeguards to protect customer information.

(e) Evaluation and Adjustment

The Coordinator will evaluate and adjust the information security program based on the results of ongoing monitoring and testing; any material changes to operations or business arrangements; or any other circumstances that are known or have reason to know that may have a material impact on protecting the privacy of customer information.

DATA SECURITY POLICY

I. POLICY

~~Institutional data is information that supports the mission of County College of Morris. It is a vital asset and is owned by the College. Institutional data is considered essential, and its quality and security must be ensured to comply with legal, regulatory, and administrative requirements. Authorization to access institutional data varies according to its sensitivity (the need for care or caution in handling). This administrative policy sets forth the college's standards with regard to the handling and safeguarding of institutional **or sensitive** data on premise, in the Cloud, or where ever the data may be stored on the network folders.~~

Institutional data is vital to support the mission of the County College of Morris and is an asset owned and maintained by the institution. The data is considered essential, and its quality and security must be ensured to comply with legal, regulatory, and administrative requirements.

This administrative policy sets forth the County College of Morris's standards with regard to the handling and safeguarding of institutional ~~or~~ and/or sensitive data regardless of storage location or device, this includes both on premise and off premise locations.

II. PURPOSE

To establish policy for the safeguarding of restricted and sensitive data ~~relating to students and CCM personnel~~ that is created, received, maintained or transmitted by the College. This policy is intended to ensure that the information is uniformly used and disclosed in accordance with all college policies, applicable state laws and **federal laws,** ~~as well as in accordance with the~~ **and the European GDPR policy. A combination of physical security, personnel security, and system security mechanisms are used to achieve this standard.**

III. DEFINITIONS

A. Archiving/Storage: The act of physically or electronically moving Institutional data ~~inactive or other records~~ to a storage location until the record retention requirements are met or until the records are needed again.

B. Institutional Data: **is information used by the County College of Morris for legitimate business purposes, this data can include sensitive and/or restricted data, student records, and all data required for legitimate business purposes.**

C. Authorized Users (Users): Individuals who have been granted access ~~to specific~~ information ~~assets~~ in the performance of their assigned duties ~~are considered Authorized Users ("Users").~~ Users include, but are not limited to faculty and staff members, trainees, students, vendors, volunteers, contractors, or other affiliates of the college.

Code:
New text
~~Deleted text~~

D. **Use of Data: Authorized users may have access to the data for the purpose to conduct their job duties but may not have the authority to extrapolate additional meanings from the data and make conclusions based on said data, or share data with others on and off campus, that do not pertain to their job functions.**

E. Electronic Media: All media and devices, ~~on~~ which electronic data can be stored, including, but not limited to: hard drives, magnetic tapes, diskettes, CDs, DVDs, ~~and~~ USB storage devices**, cell phones, cloud applications, and any/all other devices not listed.**

F. Electronic Messaging: A set of communication processes **and tools** used to relay information ~~among the users of computers. Electronic Messages take many forms.~~ **Some examples are:** Electronic Mail (Email), File Transfer Protocol (FTP), cell phones, **hand held devices,** Instant Messaging, internet chat, **and other software used for communication or data transfers**.

G. Restricted Data: Data whose access is restricted **or regulated** by federal or state statute, **e.g., HIPAA, FERPA.** For purposes of this policy, restricted data is a subset of sensitive data.

H. Sensitive Data: Data, regardless of its physical form or characteristics, the County College of Morris has determined requires ~~with~~ the highest level of protection**, e.g.,** ~~including, but not limited to,~~ data protected by law, data protected by legal contracts, or security-related data. It also includes data that is not open to public examination. Examples include: passwords, intellectual property, on-going legal investigations, ~~medical, or~~ grades ~~information protected by FERPA or HIPAA,~~ social security numbers, birth dates, professional research, student work, bank or credit card account numbers, income and credit history.

IV. DATA COLLECTION

A. Users should collect only the minimum necessary institutional/ sensitive information required to perform college business.

B. Department heads **(Data Custodian or Data Steward)** must ensure that all decisions regarding the collection and use of institutional data are in compliance with **any** ~~the~~ **federal and state laws,** ~~law~~ and with college policy and **procedures**.

V. DATA ACCESS

A. Only authorized users may access, or attempt to access, sensitive information.

B. Authorization for access to sensitive data must be authorized **by the Vice President (Data Trustees)** and ~~department head, and is~~. **This is** ~~typically~~ granted in conjunction with an acknowledgement or authorization from the requestor's department head, supervisor, or other **institutional** ~~official~~ authority.

C. ~~Where access to sensitive data has been authorized,~~ Use of such data shall

be limited to the purpose required to perform college business.

D. Users will respect the confidentiality and privacy of individuals whose records they access, observe ethical restrictions that apply to the information they access, and abide by applicable laws and policies with respect to accessing, using, or disclosing information.

E. Notification of a user's termination or removal of authorized access to sensitive information must be conveyed immediately to the ~~CCM Information Systems~~ **CCM Division of Information Systems and Institutional Effectiveness.**

VI. DATA HANDLING AND DATA TRANSFER

A. **Sensitive data must be protected from unintended access by unauthorized users.** ~~Sensitive information must not be transferred by any method to persons who are not authorized to access that information. Users must ensure that adequate security measures are in place at each destination when sensitive data is transferred from one location to another.~~

B. ~~Sensitive data must be protected from unintended access by unauthorized users.~~ **Users must guard against unauthorized viewing of ~~such~~ sensitive and restricted information. Users must not leave sensitive information unattended and/or accessible.**

C. Sensitive information must not be taken off campus **or electronically distributed** unless the user is authorized to do so, and only if encryption or other approved security precautions have been applied to protect that information.

D. Sensitive data should not be transmitted through electronic **messaging or by any other digital interface** even to other authorized users unless security methods, such as encryption, are employed.

E. **Users must take all appropriate measures to ensure the physical protection from theft, loss, and damage regardless of the device and ownership. Some examples are, smart phone, PDA, notepad, thumb drive or laptop.**

~~Physical protection from theft, loss, or damage must be utilized for mobile devices that can be easily moved such as a PDA, notepad, thumb drive or laptop.~~

VII. STORAGE OF SENSITIVE DATA

A. Physical protection must be employed for all devices storing sensitive data. This ~~shall~~ **includes** physical access controls that limits physical access and viewing. ~~, if open to public view. When not directly in use,~~ User's office, labs, or work locations ~~and suite doors~~ must be locked and any ~~easily~~ portable electronic media ~~transportable~~ devices should be secured in locked cabinets or drawers.

B. Users of laptop and other mobile computing devices need to ~~be particularly vigilant and take~~ ensure appropriate steps are taken **to** ~~ensure~~ protect the physical security of mobile devices at all times, this includes working

Code:
New text
~~Deleted text~~

remotely or traveling. ~~, but particularly when traveling or working away from the College~~.

C. ~~Information Systems~~ **The Division of Information Systems and Institutional Effectiveness – Chief Information Officer (CIO) or Information Security Officer is responsible for overall management of** ~~managing sd~~ the security **on** servers storing confidential information. The **servers** shall be regularly scanned for vulnerabilities, patched, and backed up.

D. Systems (hardware and software) designed to store and transfer confidential records require enhanced security protections and must be closely monitored. ~~It is strongly recommended that institutional data not be stored on PCs or other systems in offices or laboratories. Institutional data (including word documents, spreadsheets and Access databases) that is created on a PC or similar system should be stored on a network drive hosted on an Information Systems managed server.~~

E. Institutional data shall not be stored on PCs or other systems in offices or laboratories. Institutional data (including word documents, spreadsheets and Access databases) that is created on a PC or similar system must be stored on a network drive hosted on the Division of Information Systems and Institutional Effectiveness managed server.

F. Electronic media storing restricted/sensitive data must be protected by password security. To the extent possible, these devices must employ encryption methods.

VIII. DATA RETENTION AND DISPOSAL

A. Retention of Records Containing Restricted and Sensitive Data: A "schedule" describing the records and the official retention period is required by the State of New Jersey for each type of record created or maintained by a public institution. The County College of Morris uses the following guidelines and statutory procedures for records retention.

1. State of New Jersey "County Community Colleges General Records Retention Disposition Schedule".
2. New Jersey Permanent Statute Title 47 (Public Record Law).

B. Archiving: Institutional records, including sensitive information records, which are no longer being used for active college business, are to be archived until retention requirements have been met.

1. Departments determine the criteria for inactive record status in their areas, based upon need for the records, available storage space, and public law.
2. All inactive records are to be sent to the Records Management Department for storage in the College Records Archive until their legal retention requirements have been met in a controlled environment protected against unauthorized access, damage, and loss.
3. Only primary (original records) are to be archived. Duplicates (copies) of records should be destroyed.

C. Records Disposal: The proper destruction of public records is essential. All

official public records shall be destroyed once their retention period has expired. This pertains to the destruction of paper records as well as those that are microfilmed, imaged or are electronic. No records that are currently involved in, or have open investigations, audits, or litigation pending shall be destroyed or otherwise discarded.

A. The destruction of all official college records is coordinated through the Records Management Department. No individual employee of the College shall destroy, purge or discard any official college public record.

B. The authorized methods of destruction for non-electronic records are burning where authorized or shredding. The authorized methods of destruction for electronic records are wiping utilizing the US Department of Defense standard for cleaning and sanitizing electronic media, DOD 5220.22M **or newer version**, or physical destruction of the electronic media

D. RESPONSIBILITY

A. Supervisory Personnel: Every County College of Morris employee who has supervisory responsibilities and whose job responsibilities include the maintenance of or use of sensitive data is responsible for implementing and ensuring compliance with this policy and initiating corrective action if needed. In implementing this policy, each supervisor is responsible for the following:

- Communicating this policy to personnel under their supervision.
- Ensuring that appropriate security practices, consistent with the data handling requirements in this policy are used to protect institutional data.
- Providing education and training in data management principles to employees under their supervision.

B. All CCM employees, regardless of their position within the institution have a responsibility to safeguard sensitive and restricted information.

C. User Responsibilities: Users who are authorized to obtain institutional data must ensure that it is protected to the extent required by law or policy ~~after they obtain it.~~ All data users are expected to:

- Access institutional/sensitive data only in their conduct of college business.
- Request only the minimum necessary confidential/sensitive information necessary to perform college business
- Respect the confidentiality and privacy of individuals whose records they may access.
- Observe any ethical restrictions that apply to data to which they have access.
- Know and abide by applicable laws or policies with respect to access, use, or disclosure of information.

D. COMPLIANCE

Compliance with this data protection policy is the responsibility of all members of the

County College of Morris community. Violations of this policy are dealt with seriously and include sanctions up to and including termination of employment. Users suspected of violating these policies may be temporarily denied access to CCM's information technology resources during investigation of an alleged abuse. Violations may also be subject to prosecution by state and federal authorities.