

Board of Directors Packet

Manhattan Area Technical College

June 27, 2023

Zoom/Live Stream 5:30 pm



Board of Directors:

Ballou, Brett (Riley) Chair

Urban, David (Riley)

Armbrust, John (Riley)

Flanary, Tim (Pottawatomie) Vice-Chair

Allen, Will (Geary)

Noah, Julie (Clay)

Peterson, Heather (Pottawatomie)

Matson, Mike (Riley)

Administration/Staff:

Genandt, James (President/CEO)

Biesenthal, Hannah (Board Clerk)

Phillips, Sarah

Davis, Kimberly

Gfeller, Josh

Ross, Neil

Roberts, Nathan

Boxberger, Chris

Watts, Harry

Bellamy, Kerri

Faculty Senate

Agenda

1. Call to Order

2. Consent Agenda (Routine items requiring BOD action) *

- Approval of May 2023 Meeting Minutes (Attachment 1) *
- Approval of May 2023 Check Register w/Threshold Expenditures (Attachment 2) *
- Organizational Update (Attachment 3) *
- President's Report (Attachment 4)*

3. General Agenda (Items possibly requiring BOD Action)

- Policy Update
 - i. Policy 9.1.7 GLBA Information Security Program (Attachment 5, 5a) **Josh**
- Landmark Bank Agreement Extension (Attachment 6) * **Sarah, Kerri**
- Approval of FY2024 Interim Budget (Attachment 7) *
- Academic Program Proposal (Attachment 8) * **Sarah**
- Monitoring Report
 - i. Treatment of People (Attachment 9) *

4. Discussion of Ends (Demonstration, Testimonial, or Report of Results related to Board Mission)

- Thank You Reception for Legislators **Jim**
- Facilities/Projects Updates **Josh, Sarah**

* Requires BOD Action

Meetings and Upcoming Events

Next Board Meeting: August 29, 2023

(Unless another meeting in July is needed)

Campus Closed: July 3rd and 4th (Independence Day)

Classes Start: August 21

Board of Directors Minutes

Manhattan Area Technical College

May 30, 2023 5:30pm



1. The Board of Directors of the Manhattan Area Technical College met April 25, 2023 at 5:30 p.m., with live streaming for employees.
 - Members present: Brett Ballou, Tim Flanary, John Armbrust, Julie Noah, Will Allen, Mike Matson.
 - Administration Present: Jim Genandt, President/CEO; Sarah Phillips, Vice-President, Nathan Roberts, Dean of Academic Affairs; Chris Boxberger, Dean of Academic Partnerships and Outreach; Kim Davis, Dean of Nursing and Health Programs; Hannah Biesenthal, Executive Assistant/Board Clerk.
 - Guests: Harry Watts, Brian Koch, Deirdre Greely.
 - Meeting was live streamed.
2. **Call to Order**
 - Brett Ballou called the meeting to order at 5:30p.m.
3. **Consent Agenda**
 - Mike Matson motioned to approve consent agenda. Tim Flanary seconded. Motion carried 6 yeas and 0 nays. Motion passed.
4. **General Agenda**
 - Sarah Phillips notified the board of a change to the academic calendar to have the campus be closed on Monday, July 3rd. Tim Flanary motioned to approved the changed to the academic calendar. Will Allen seconded. Motion carried 6 yeas and 0 nays. Motion passed.
 - President Genandt reviewed the monitoring report for financial condition. Mike Matson motioned to approve the monitoring report for financial condition. John Armbrust seconded. Motion carried 6 yeas and 0 nays. Motion passed.
 - President Genandt and Hannah Biesenthal informed the board that evaluations for the President will be going out soon and prepared for the next meeting. Tim Flanary formal announced his renewal of his board term.
5. **Discussion of Ends**
 - Deidre Greely recapped the past few events that the nursing students have been involved in. Nursing students, EMT students and MLT students all participated in a emergency room simulation. EMT students brought in a person needing medical care, the nursing students assisted the patient and the MLT students ran laboratory tests. Nursing students also participated in

teaching Boy Scouts basic First-Aid and CPR.

- Kim Davis informed the board that the nursing program passed the site visit and have been reaccredited. There were a few areas of improvement but overall a great visit.
- Chris Boxberger discussed the AEFLA award for the 2024 fiscal year. MATC received renewed funding which will help with increasing numbers in adult education.
- Nathan Roberts provided a recap of the recent campus events of the Student Recognition Banquet and Nursing Pinning and Commencement. Both events were a success and it was a wonderful opportunity to celebrate the students.
- Sarah Phillips went over the newest plans and dates for the Advanced Technology Center. The parking lot behind the main building will be removed and replaced, measuring and footing for the retaining wall has begun. Concrete for the parking lot will be completed by mid-July.
- Brian Koch reviewed the Student Recognition Banquet and the opportunity to award students. Brian recognized the faculty members that make the extra effort to be out in the public at local community events. He stated that showing up to those events shows the public and possible future students the amount of care the instructors have.

6. Executive Session: Student Issue

- Tim Flanary motioned to go into executive session at 6:33pm. Mike Matson seconded. Motion carried 6 yeas and 0 nays. Tim Flanary motioned to return to open session. John Armbrust seconded. Motion carried 6 yeas and 0 nays. Motion passed. No action was taken.

7. Executive Session: Finances

- Tim Flanary motioned to go into executive session at 6:40pm. Mike Matson seconded. Motioned carried 6 yeas and 0 nays. Tim Flanary motioned to return to open session. Mike Matson seconded. Motion carried 6 yeas and 0 nays. Tim Flanary motioned to go into executive session at 6:55pm. Will seconded. Motion carried 6 yeas and 0 nays. Tim Flanary motioned to return to open session. Mike Matson seconded. Motion carried 6 yeas and 0 nays. No action was taken.

8. Adjournment: Brett Ballou adjourned the meeting at 7:05pm.

To: MATC Board of Directors
 From: Administration
 Re: May 2023 Expenditures



June 27, 2023

Category	Costs	%
Payroll, Withholdings and Benefits (200, 230, 590)	\$ 391,894.88	78.44%
Facilities (510)	\$ 11,410.85	2.28%
Student Payments (110)	\$ 13,634.00	2.73%
Program Expenditures	\$ 41,170.83	8.24%
ALC Operating Costs (excludes salary/benefits) (900, 930, 931)	\$ 4,281.42	0.86%
Wamego (excluding salary/benefits)	\$ 3,324.22	0.67%
Other Operating costs	\$ 33,926.04	6.79%
Total May Expenditures	\$ 499,642.24	100%

Threshold Expenditures > \$5,000				
Vendor Name	Item(s) Purchased	Cost	Department	Funding
Altec Industries, Inc.	winch line for digger truck	\$ 9,168.99	EPD	operating
Amazon Capital Services	Student Personal Care Items - GEER Grant	\$ 5,213.28	TLC	GEER Grant
BCBS (May 2023)	Health Insurance Premium	\$ 44,865.70	All School	payroll ded/gen fund
Anixter Inc. Kansas City	order material from anixter	\$ 8,485.85	EPD	course fee
Sanity Solutions	Switching Hardware for INT Capstone netw	\$ 5,820.00	INT	operating
IRS	PR 5.15.2023 Payroll deductions	\$ 35,733.34	All School	payroll ded/gen fund
IRS	PR 5.31.2023 Payroll deductions	\$ 38,949.23	All School	payroll ded/gen fund
KS Dept of Revenue	PR 5.15.2023 Payroll deductions	\$ 7,407.11	All School	payroll deduction
KS Dept of Revenue	PR 5.31.2023 Payroll deductions	\$ 7,961.76	All School	payroll deduction
KPERS	PR 5.15.2023 Payroll deductions	\$ 8,627.01	All School	payroll deduction
KPERS	PR 5.31.2023 Payroll deductions	\$ 9,192.31	All School	payroll deduction
Total May Expenditures Exceeding Threshold		\$ 181,424.58		



MEMORADUM TO: The Board of Directors
FROM: Jim Genandt, President
 Human Resources
DATE: June 27, 2023
SUBJECT: Consent Agenda: Organizational Update

New Hire/Rehires/New Positions					
Employee Name	Position Title	DOH	Department	Funding Source	Status
Jacob Boley	Welding Tech Instructor	6/19/2023	Faculty - Welding	Operating	New Hire
Promotions/Title Changes					
Employee Name	Position Title	DOC	Department	Funding Source	Status
Separations/Retirements					
Employee Name	Position Title	DOS	Department	Funding Source	Status
Elsa Valarezo	ALC Instructional Facilitator	6/2/2023	Adult Education	Operating	Resignation
Advertised Positions					
Position Title			Department	Funding Source	Status
Adjunct Opportunities for Consideration			All Departments	Operating	Open
Associate Degree Nursing Adjunct Clinical Instructor			Faculty	Operating	Open
Part-Time Welding Technology Program Assistant			Faculty	Operating	Open
Part-Time Allied Health Instructor			Continuing Education	Operating	Open
Emergency Medical Sciences Coordinator			Faculty	Operating	Open
Part-Time INT Program Assistant			Academics/INT	Perkins Grant	Open
Part-Time Adult Ed ESL Instructor			Adult Education	AEFLA Grant	Open
Full-Time Adult Ed ESL Instructor			Adult Education	AEFLA Grant	Open

President's Report: June 2023

Owner Expectations:

- June 1, I received an update on the HLC Assessment follow-up status from Kim Withroder and folks involved with that project. We have made progress in key areas to report to HLC.
- June 1, I met with the presidents and lobbyist for the Kansas Technical Colleges. We worked on accountability measures for the Base Operating Grant funding, and sketching out efforts to make that funding permanent.
- June 12, Greg Nichols (Salina Tech) and I met with KSU Provost Taber and Chief of Staff Stewart to discuss ideas on collaboration (rather than affiliation).
- June 14, I was on KMAN's In-Focus with MATC updates.

Employer Needs & Response:

- June 5, met with Lonnie from Meadowlark working on health care worker needs, as well as needs related to facilities and IT.
- June 6, Chris and I met with Jonathan Morgenstein, staff member with the National Renewable Energy Labs (NREL), an agency connected to the US Department of Energy. He will connect us with other staff to look at some projects to get MATC involved with appropriate renewable energy efforts and resources.
- June 7, I met with KSU and federal representatives with the new NSF Engines Grant project via Zoom.
- June 8, I met with Kristin Brighton about the HirePaths project and resources and impact of that social media venue.
- June 8, I worked with Nathan Redeker of BHS.
- June 12: Chris and I met with representatives of the Chamber of Commerce and Continental Mills to discuss our role in training workers, primarily through the Industrial Engineering and Critical Environment Technology programs.

Resource Development:

- June 1, Harry and I presented to the Riley County Commissions with a request to support the Advanced Technology Center project with \$50,000 per year for 5 years.
- June 16, I worked in Topeka with representatives of Commerce and the State Budget agencies on resources for MATC and the other technical colleges.

I did take several days or parts of days off due to family health issues in June.

**Manhattan Area Technical College
Institutional Policy and Procedure Manual**

Policy No. 9.1.7

Title: GLBA Information Security Program Policy	
Originated by: Chief Information Officer/Director of Facilities	Originated Date: 4/2023
Revised by:	Revised Date:
President/Board of Directors Approval Date:	
Reviewed on: 5/2023	

Policy Statement: GLBA mandates that the Institute appoint an Information Security Program Coordinator, conduct a risk assessment of likely security and privacy risks, institute a training program for all employees who have access to covered data and information, oversee service providers and contracts, and evaluate and adjust the Information Security Program periodically.

Rationale: This Information Security Plan describes Manhattan Area Technical College safeguards to protect covered data and information in compliance with the FTC's Safeguards Rule promulgated under the Gramm Leach Billey Act (GLBA).

These safeguards are provided to:

- Ensure the security and confidentiality of covered data and information.
- Protect against anticipated threats or hazards to the security or integrity of such information.
- Protect against unauthorized access to or use of covered data and information that could result in substantial harm or inconvenience to any student or employee.

This Information Security Program also identifies mechanisms to:

- Identify and assess the risks that may threaten covered data and information maintained by MATC.
- Develop written policies and procedures to manage and control these risks.
- Implement and review the program.
- Adjust the program to reflect changes in technology, the sensitivity of covered data and information, and internal or external threats to information security.

Procedure:

Information Security Program Coordinator(s)

The Chief Information Security Officer/Director of Facilities and the Network Administrator have been appointed program coordinators at MATC. They are responsible for assessing the risks associated with unauthorized transfers of covered data and information and implementing procedures to minimize those risks to the college. They will also conduct reviews of areas that have access to protected data and information to assess the internal control structure put in place by the administration and to verify that all departments comply with the requirements of the security policies and practices delineated in this program.

Identification and Assessment of Risks to Student/Employee Information

MATC recognizes that it is exposed to both internal and external risks, including but not limited to:

- Unauthorized access of covered data and information by someone other than the owner of the covered data and information.
- Compromised system security as a result of system access by an unauthorized person.
- Interception of data during transmission.
- Loss of data integrity.
- Physical loss of data in a disaster.
- Errors introduced into the system.
- Corruption of data or systems
- Unauthorized access of covered data and information by employees.
- Unauthorized requests for covered data and information.
- Unauthorized access through hardcopy files or reports.
- Unauthorized transfer of covered data and information through third parties.
-

Recognizing that this may not represent a complete list of the risks associated with the protection of covered data and information and that new threats are created regularly, MATC will actively participate and monitor appropriate cybersecurity advisory groups to identify risks.

Current safeguards implemented, monitored, and maintained by MATC are reasonable, and considering current risk assessments are sufficient to provide security and confidentiality to the covered data and information the Institute maintains. Additionally, these safeguards reasonably protect against currently anticipated threats or hazards to the integrity of such information.

Employee Management and Training

Per MATC policies, standards, and guidelines, reference checking and background reviews are conducted for all new hires. During employee orientation, each new employee in departments that handle protected information are required to participate in several training sessions on the importance of confidentiality of protected information. Each new employee will also be trained to use computer information and passwords properly. Further, each department responsible for maintaining protected information will provide ongoing updates to respective staff. These training efforts should help minimize risk and safeguard covered data and information security.

Physical Security

Manhattan Area Technical College has addressed the physical security of protected information by limiting access to only employees with a business reason to know or access such information.. Existing policies establish a procedure for promptly reporting the loss or

**Manhattan Area Technical College
Institutional Policy and Procedure Manual**

Policy No. 9.1.7

theft of protected information. Offices and storage facilities that maintain protected information limit customer access and are appropriately secured. Paper documents that contain protected information are shredded at the time of disposal.

Information Systems

Information systems include network and software design and information processing, storage, transmission, retrieval, and disposal. MATC has policies including standards, guidelines governing electronic resource use, and firewall and wireless policies. MATC will take reasonable and appropriate steps consistent with current technological developments to make sure that all protected information is secure and to safeguard the integrity of records in storage and transmission. MATC will follow current policies, including 9.1.1 Computer Usage Policy, 9.1.4 Clean Desk Policy, and 9.1.5 Telecommuting Policy for all electronic protected information by encrypting it for transit.

Management of System Failures

MATC 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 vendors and others to regularly obtain and install patches to correct software vulnerabilities; maintaining appropriate filtering or firewall technologies; alerting those with access to covered data of security threats; imaging documents and shredding paper copies; 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.

Oversight of Service Providers

Due to the specialized expertise needed to design, implement, and service new technologies, vendors may be needed to provide resources that MATC determines not to provide on its own. In the process of choosing a service provider that will maintain or regularly access protected information, the evaluation process shall include the ability of the service provider to safeguard protected information. Contracts with service providers may include the following provisions:

- A requirement that the protected information will be held in strict confidence and accessed only for the explicit business purpose of the contract;
- A requirement that the service provider have documented appropriate safeguards and controls (e.g., SOC2) to protect the protected information it receives and that it must promptly report any security incidents that may affect MATC protected information;
- Where appropriate, a requirement that the service provider maintain certain types of insurance to cover potential liability in the event of a security incident;
- Where appropriate, a requirement that the service provider submit to audits of its information security and privacy policies, procedures and controls.

**Manhattan Area Technical College
Institutional Policy and Procedure Manual**

Policy No. 9.1.7

Continuing Evaluation and Adjustment

This Information Security Plan will be subject to periodic review and adjustment, especially due to the constantly changing technology and evolving risks. The Coordinators, in consultation with the administration, will review the standards set forth in this policy and recommend updates and revisions as necessary. It may be necessary to adjust the plan to reflect changes in technology, student/customer data sensitivity and internal or external threats to information security.

MANAHTTAN AREA TECHNICAL COLLEGE- DATA RISK ASSESSMENT

Executive Summary

Manhattan Area Technical College performed a risk assessment of the IT infrastructure between a period of September 1, 2022, and September 30 2022. The overall status of the IT infrastructure was found to secure but, there were some areas that improvements could be made. Several areas had a calculated risk of a medium level that can be addressed by administration and the IT team.

DETAILED ASSESSMENT

1. Introduction

1.1 Purpose

Identify risks as they pertain to Information Technology at Manhattan Area Technical College. Not limited to but including disaster recovery, hacking breaches, and other types of breaches.

1.2. Scope of this risk assessment

MATC uses several internal, public-facing, and cloud systems including active directory, canvas lms, JICS, office 365, authorize.net processing and others. The scope of this assessment includes all of the components described above including supporting systems like firewall and network.

2. Risk Assessment Approach

2.1 Participants

Role	Participant
System Owner	Josh Gfeller
Network Manager	Bryanna Marihugh

2.2 Techniques Used

Technique	Description
Assessment tools	Several security tools, including application scanning, port scanning, and system penetration testing.
Interviews	Interviews were conducted to validate information
Process tracking	
Review of documentation	Reviewed process documentation and configuration.

2.3 Risk Model

In determining risk we utilized the following model for calculation.

Risk = Threat likelihood x magnitude of impact

Threat Likelihood

Likelihood (Weight Factor)	Definition
High (1.0)	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective
Medium (0.5)	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low (0.1)	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

Magnitude of Impact

Impact (Score)	Definition
High (100)	<p>The loss of confidentiality, integrity, or availability could be expected to have a <i>severe or catastrophic</i> adverse effect on organizational operations, organizational assets, or individuals.</p> <p>Examples:</p> <ul style="list-style-type: none"> • A severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions • Major damage to organizational assets • Major financial loss • Severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.
Medium (50)	<p>The loss of confidentiality, integrity, or availability could be expected to have a <i>serious</i> adverse effect on organizational operations, organizational assets, or individuals.</p> <ul style="list-style-type: none"> • Significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced • Significant damage to organizational assets • Significant financial loss • Significant harm to individuals that does not involve loss of life or serious life threatening injuries.
Low (10)	<p>The loss of confidentiality, integrity, or availability could be expected to have a <i>limited</i> adverse effect on organizational operations, organizational assets, or individuals.</p> <p>Examples:</p> <ul style="list-style-type: none"> • Degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced • Minor damage to organizational assets • Minor financial loss • Minor harm to individuals.

Risk was calculated as follows:

Threat Likelihood	Impact		
	Low (10)	Medium (50)	High (100)
High (1.0)	Low Risk (10 x 1.0 = 10)	Medium Risk (50 x 1.0 = 50)	High Risk (100 x 1.0 = 100)
Medium (0.5)	Low Risk (10 x 0.5 = 5)	Medium Risk (50 x 0.5 = 25)	Medium Risk (100 x 0.5 = 50)
Low (0.1)	Low Risk (10 x 0.1 = 1)	Low Risk (50 x 0.1 = 5)	Low Risk (100 x 0.1 = 10)

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)

3. System Characterization

3.1 Technology components

Component	Description
Applications	Managed by several vendors including Jenzabar, Microsoft, Collegeboard
Databases	Microsoft SQL 2019/21
Operating Systems	Windows 10, Server 2016/19/22, Linux
Networks	Dell networking, PFSense Firewalls
Interconnections	Authorize.net
Protocols	SSL

3.2 Physical Location(s)

Location	Description
Datacenter	3136 Dickens Ave, Manhattan KS 66503
Offsite WC	524 US Highway 24 Wamego KS

3.3 Data Used By System

Data	Description
PII	Includes Name, addresses, phone, email, SSN, DOB
Vehicle Info	Vehicle info, tag #
Financial Info	No credit card info stored on-site. Banking and routing #'s stored onsite.

3.4 Users

Users	Description
Employees	Access the systems via web browser or application.
Students	Access the systems via web browser or application.
Guests	Access the systems via web browser with guest privileges.

4. Vulnerability Statement

Vulnerability	Description
Web intrusion and cross-site scripting	The web application can be used as a mechanism to transport an attack to an end user's browser. A successful attack can disclose the end user's session token, attack the local machine, or spoof content to fool the user.
SQL Injection	Information from web requests is not validated before being used by a web application. Attackers can use these flaws to attack backend components through a web application.

Password strength	Passwords used by the web application are inappropriately formulated. Attackers could guess the password of a user to gain access to the system.
Unnecessary services	The web server and application server have unnecessary services running such as telnet, snmp, and anonymous ftp
Disaster Recovery	There are no procedures to ensure the ongoing operation of the system in event of a significant business interruption or disaster
User Error	A user falls for a phishing attempt to share sensitive information to an attacker
Lack of Documentation	System specifications, design, and operating processes are not documented.
Integrity Checks	The system does not perform sufficient integrity checks on data input into the system.

5. Threat Statement

[Compile and list the potential threat-sources applicable to the system assessed].

Threat-Source	Threat Actions
Hacker	Web defacement • Social engineering • System intrusion, break-ins • Unauthorized system access
Computer Criminal	Identity theft • Spoofing • System intrusion
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Browsing of personally identifiable information • Malicious code (e.g., virus) • System bugs • Unauthorized system access
Environment	Natural Disaster

5. Risk Assessment Results

Item Number	Observation	Threat-Source/ Vulnerability	Existing controls	Likelihood	Impact	Risk Rating	Recommended controls
1	Hacker scripting	Hackers/firewall	PFsense Firewall	Low	High	Medium	Continue to increase security levels at firewall level, office 365 defender
2	User system passwords can be guessed or cracked	Hackers/ password effectiveness	Passwords must be complex and changed frequently	Medium	Medium	Medium	Use systems like password managers such as lastpass/bit warren, MFA
3	Data inappropriately extracted or modified from student databases	Hackers, criminals, sql injection	Validation checks	Medium	High	High	Keep servers patched with latest updates and port blocking using patch management automation
4	Running unnecessary services	All	None	Medium	Medium	Medium	Verify what services are running
5	Employee falls for phishing attempt	Employees	Semesterly training to keep employees up to date on how to spot these attacks	Low	Medium	Low	Continue to improve office 365 email filtering with office 365 defender. Employee Training
6	DR Plan	Environment	Daily,nightly backups. Offsite backups and offline backups	Low	High	Medium	Do more DR testing

7	Disgruntled employee	Ex-employee	Shut off all access	Low	Low	Low	Create better processes for shutting down all access quickly and effectively.
---	----------------------	-------------	---------------------	-----	-----	-----	---



TO: Manhattan Area Technical College Board of Directors

FROM: James Genandt, President/CEO
Kerri Bellamy, Director of Finance
Sarah Phillips, Vice President Student Success/CAO/CSSO/Interim CFO

SUBJECT: Extension of Landmark National Bank Agreement

Background Information and Proposal

In accordance with the Manhattan Area Technical College Board of Directors Governance Policy and as the individuals responsible in monitoring the institution's accountability and performance in meeting our mission, vision, and values for our students and for the residents, businesses, and organizations in the college's service area, the executive administration presents the following financial proposal for approval.

For the past five years from July 1, 2018, through June 30, 2023, the college has held its fiscal operational accounts with Landmark National Bank. Due to the recent extensive capital project undertaken by the college, the administration proposes a one-year extension of the current service agreement with Landmark National Bank to be effective from July 1, 2023, through June 30, 2024, for the college's operational accounts. After January 1, 2024, the college will roll out request for proposals (RFP) specifying the service requirements in regard to the college's financial operational accounts.

The following terms and conditions have been specified by Landmark National Bank as part of the extension:

- The interest rate to be paid on the average daily collected balances will be changed from the Fed Funds rate + .10% (currently 5.35%), to the Kansas Municipal Investment Pool rate (currently 3.76%), to be adjusted monthly, beginning 7/1/23.
- The activity costs for deposit services and treasury/cash management services will remain the same as they are set forth in the existing banking services agreement.

Recommendation

Administration respectfully requests that the Board of Directors approve the one-year extension with the understanding by administration that the college will take the holding of the college's financial operational accounts out for RFP after January 1, 2024, with a recommendation to the board no later than May 2024 board meeting.



TO: MATC Board of Directors

FROM: Sarah Phillips, VP of Student Success/CAO/CSSO

DATE: June 27, 2023

RE: Academic Program Proposal

Background Information

In an effort to provide the best degree options that support both the needs of our students and meet industry requirements, the institution, through its faculty governance structure in compliance with the Higher Learning Commission, consistently assess the college's programs and certificates it awards.

Through this assessment, the Curriculum Committee approved program changes to the Associate of Applied Science, Certificate A, and Certificate B in Construction Technology; the Associates of Applied Science and Certificate B in Biotechnology Laboratory Technician; and Certificate C in Information and Network Technology.

Program Proposals

Associate of Applied Science, Certificate A, and Certificate B in Construction Technology – The Construction Technology program offers training in residential and commercial construction. Through conversations with industry partners, due to the increasing need for workforce the program has been updated to create a more efficient pathway for students. The current A.A.S (63 credit hours), Certificate A (19 credit hours), and Certificate B (39 credit hours) require OSHA 30 and Workplace Skills that is taught by the Construction Technology instructor. Industry partners have indicated that entry level workers only need OSHA 10, and the majority of our technical programs, in place of Workplace Skills, utilize a course through the business department, Global Employment Standards, that prepares students in workplace behavior, resume building, development of professional career goals, and interpersonal communication in the workplace. These two course adjustments to the curriculum result in the A.A.S. now requiring 61 credit hours, the Certificate A totally at 18 credit hours, and the Certificate B being awarded at 34 credit hours.

Associate of Applied Science and Certificate B in Biotechnology Laboratory Technician – The initial intent of the Biotechnology Laboratory Technician curriculum was to provide a pathway for students who excel in the science and want to work in a laboratory setting. As the need for skilled technicians has increased, industries seek students who have a bachelor level education with science emphasis and have the capabilities to apply scientific principles and technical skills in support of a variety of laboratories in the biotechnology arena. With that determination the necessity for an A.A.S. (65 credit hours) and Certificate B (32 credit hours) in Biotech is unnecessary. With the established Certificate A in Biotechnology (17 credit hours), graduates of a bachelor's degree can obtain the necessary skills through a one semester certificate.

Certificate C in Information and Network Technology – Information and Network Technology (INT) is focused on the design, implementation, and configuration of network servers, and their integration into a modern enterprise network. Currently the Certificate C (52 credit hours) has 6 hours of technical

electives required that are courses not associated with the INT program. These have been determined as unnecessary and create a barrier for students to complete the certificate efficiently. To increase the opportunity for student completion, the additional 6 credit hours have been removed to allow a student to concentrate strictly on network required courses. This results in the Certificate C in INT to total 46 credit hours.

Recommendation

The Administration, in agreement with the Curriculum Committee, respectfully requests that the Board of Directors approve the recommended outlined program actions.

INTERNAL MONITORING REPORT: TREATMENT OF PEOPLE

JUNE 2023

I hereby present my monitoring report on your Executive Limitations policy "Treatment of People," as scheduled. In consultation with personnel assigned to the duties of Human Resources, I certify that the information contained in this report is true.

BROADEST POLICY PROVISION:

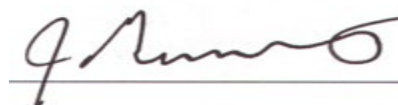
With respect to the treatment of students, staff, volunteers, and the community dealings shall not be inhumane, unfair, or undignified. Accordingly, the president shall not:

1. Operate without written procedures that clarify student and staff rules, provide for effective handling of grievances, protect against wrongful or unsafe conditions, and preferential treatment for personal reasons:
 - a. MATC has developed written policies and procedures for all operations of the College, including those listed above. All employees have access to policies, procedures, and statutes through the College's website and internal institutional portal. The College Catalog and related official materials also provides information for students guiding them on relevant policies, procedures, codes of conduct, and grievance processes. These are also accessible via the College website and internal portal. The access via the College website ensures all appropriate public access.
2. Discriminate against anyone for expressing ethical dissent;
 - a. There have been no cases of discrimination for any reason in the past year.
3. Withhold a due process procedure from students or staff;
 - a. Due process procedures are followed when dealing with any complaint and when dealing with any other matter regarding such proceedings.
4. Prevent students and staff from grieving to the board when internal grievance procedures have been exhausted;
 - a. There has been no instance of any such prevention during the past year.
5. Fail to acquaint students and staff with their rights and responsibilities;
 - a. Students and staff are made aware of their rights and responsibilities through several official College documents, including but not limited to: Personnel Handbook, College Catalog, course syllabi, Faculty Negotiated Agreement, MATC policies and procedures, and any other appropriate communication.

CEO's INTERPRETATION:

With reference to general operations and through my interpretation of the constraints listed above, I report compliance.

Signed:



President/CEO

June 20, 2023