LEADERSHIP COUNCIL MEETING
Friday, April 13, 2018
Clayton Glass Library
Room CG 129
AGENDA

1. Approval of Minutes:
· March 2, 2018

2. Updates:
· Faculty Council- Dr. Lucy Craig
· Administrative Council- Elizabeth Fitch
· Support Staff Council- Bertha Smith
· Student Government Association- Danny McFarland

3. Review of Policies
· Bring Your Own Device Policy 1:08:00:05
· Use of Social Media Policy 1:08:00:03
· Website Publishing Policy 1:03:00:04
· Curriculum Chair Policy 5:10:00:01
· Grant Sub Awards Policy 4:02:01:01

4. Commencement Update - Hilda Tunstill

5. Budget Update- Jay Turney

6. Future Meetings: TBD

MOTLOW STATE COMMUNITY COLLEGE

POLICY

Category
BRING YOUR OWN DEVICE (BYOD) – 1:08:00:05
Approval
Corresponding Policies: TBR Guidelines G-051; G-052
Leadership Council Approved:
Effective Date/Approved:
Revised:
Responsible Party: Chief Information Officer

I. PURPOSE

A. The purpose of this policy is to define standards, procedures, and restrictions for end users who have legitimate requirements to access the college's data from a mobile device connected to an unmanaged network outside of Motlow State Community College's direct control.

B. The overriding goal of this policy is to protect the integrity of the private and confidential institutional data that resides within Motlow's technology infrastructure. This policy intends to prevent this data from being deliberately or inadvertently stored insecurely on a mobile device or carried over an unsecure network where it can potentially be accessed by unsanctioned resources.

C. A breach of this type could result in loss of student or employee information, damage to critical applications, and damage to the institution's public image. Therefore, all users employing a mobile device connected to an unmanaged network outside of Motlow's direct control to backup, store, and otherwise access corporate data of any type must adhere to college-defined processes for doing so.

II. APPLICABILITY

A. This mobile device policy applies to any hardware and related software that could be used to access institutional resources including, but not limited to, all devices and accompanying media that fit the following device classifications, even if said equipment is not college sanctioned, owned, or supplied:

1. Laptop/notebook/tablet computers
2. Ultra-mobile PCs (UMPC)
3. Mobile/cellular phones
4. Smartphones
5. Personal Digital Assistants (PDAs)
6. Home or personal computers used to access institutional resources
7. Any mobile device capable of storing corporate data and connecting to an unmanaged network

B. This policy applies to all Motlow State Community College employees, including full and part-time staff, contractors, freelancers, and other agents who utilize either company-owned or personally-owned mobile devices to access, store, back up, relocate or access any department or student-specific data. Such access to this confidential data is a privilege, not a right, and forms the basis of the trust Motlow has built with its students, employees and community. Consequently, employment at Motlow does not automatically guarantee the initial and ongoing ability to use these devices to gain access to institutional networks and information. IT addresses a range of threats to – or related to the use of – institutional data:

Threat	Description
Loss	Devices used to transfer or transport work files could be lost or stolen.
Theft	Sensitive institutional data is deliberately stolen and sold.
Copyright	Software copied onto a mobile device could violate licensing.
Malware	Viruses, Trojans, Worms, Spyware and other threats could be introduced via a mobile device.
Compliance	Loss or theft of financial and/or personal and confidential data could expose the college to the risk of non-compliance with various identity theft and privacy laws.

C. Addition of new hardware, software, and/or related components to provide additional mobile device connectivity will be managed and issued at the sole discretion of the Information Technology (IT) Department.

III. AFFECTED TECHNOLOGY

A. Connectivity of all mobile devices will be centrally managed by Motlow's IT Department and will utilize authentication and strong encryption measures.
B. Although Motlow is not able to directly manage external and mobile devices which may require connectivity to an external network, end users are expected to adhere to the same security protocols when connected to non-institutional networks.
C. Failure to do so will result in immediate suspension of all network access privileges so as to protect the college's infrastructure.

IV. APPROPRIATE USE

A. It is the responsibility of any employee of Motlow who uses a mobile device to access institutional resources to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here.
B. It is imperative that any mobile device that is used to conduct college business be utilized appropriately, responsibly, and ethically.
C. Failure to do so will result in immediate suspension of that user's account. Based on this, the following rules must be observed:
    1. ACCESS CONTROL
        a. Motlow reserves the right to refuse, by physical and non-physical means, the ability to connect mobile devices to institutional and institutional-connected systems.
        b. Motlow will engage in such action if it feels such equipment is being used in such a way that puts the college's systems, data, employees, and students at risk.
        c. Prior to initial use on Motlow's network or related infrastructure, **all college owned mobile devices must registered with the IT Department.**
        d. All mobile devices attempting to connect to the corporate network through an unmanaged network (i.e. the Internet) will be inspected using technology centrally managed by Motlow's IT Department.
        e. Devices that have not been previously approved by IT, are not in compliance with IT's security policies, or represent any threat to the college network or data will not be allowed to connect.
        f. Laptop computers or personal computers may only access the college network and data using a Secure Socket Layer (SSL) Virtual Private Network (VPN) connection. The SSL VPN portal Web address will be provided to users as required.
        g. Smart mobile devices such as smartphones, PDAs, and UMPCs will access the corporate network and data using Mobile VPN software installed on the device by IT.

2. SECURITY
   a. Employees using mobile devices and related software for network and data access **will**, without exception, **use secure data management procedures.**
   b. All mobile devices must be protected by a **strong password (See TBR guideline G-051)**.
   c. **Employees agree to never disclose their passwords to anyone**, particularly to family members if institutional work is conducted from home.
   d. All users of mobile devices must employ reasonable physical security measures. End users are expected to secure all such devices used for this activity whether or not they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain college data.
   e. Any non-college computers used to synchronize with these devices will have installed up to date anti-virus and anti-malware software deemed necessary by Motlow's IT Department.
   f. Any mobile device that is being used to store Motlow State Community College data must adhere to the authentication requirements of Motlow's IT Department.
   g. IT will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable.
   h. Any attempt to contravene or bypass said security implementation will be deemed an intrusion attempt and will be dealt with in accordance with Motlow's Information Technology policy.
   i. Employees, contractors, and temporary staff must erase all college related data permanently from **personally owned devices** once their use is no longer required.
   j. Divisions and departments must notify the IT Department when a **college owned device** needs a transfer in users, be replaced or is no longer needed.
   k. In the event of a lost or stolen mobile college device it is incumbent on the employee to report this to IT immediately. IT will attempt to remotely wipe all data and lock the device to prevent access by anyone other than IT. If the device is recovered, it can be submitted to IT for re-provisioning.
   l. Usage of location-based services and mobile check-in services, which leverage device GPS capabilities to share real-time user location with external parties, is prohibited within the workplace. This applies to corporate-owned mobile devices being used within the college premises.

V. HELP & SUPPORT

A. Motlow's IT Department will support its sanctioned hardware and software, but is not accountable and will support such devices on a very limited basis and at the discretion of the CIO for conflicts or problems caused by the use of unsanctioned media, hardware, or software. This applies even to devices already known to the IT Department.

B. Employees, contractors, and temporary staff will make no modifications of any kind to company-owned and installed hardware or software without the express approval of Motlow's IT Department. This includes, but is not limited to, any reconfiguration of the mobile device.

C. IT reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on the enterprise network.

VI. ORGANIZATIONAL PROTOCOL

A. IT can and will establish audit trails and these will be accessed, published and used without notice. Such trails will be able to track the attachment of an external device to a device, and the resulting reports may be used for investigation of possible breaches and/or misuse.

B. The end user accepts that his or her access and/or connection to Motlow's networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. This is done in order to identify accounts/devices that may have been compromised by external parties. In all cases, data protection remains Motlow's highest priority.

C. Motlow employees must **immediately report** to his/her manager and Motlow's IT Department **any incident or suspected incidents of unauthorized data access**, data loss, and/or disclosure of company resources, databases, networks, etc.

D. Motlow State Community College will not reimburse employees if they choose to purchase their own mobile devices. Employees will not be allowed to expense mobile network usage costs.

MOTLOW STATE COMMUNITY COLLEGE

POLICY

Category
USE OF SOCIAL MEDIA – 1:08:00:03
Approval
Corresponding Policies: TBR Guideline G-054; MSCC Policy 1:08:00:00
Leadership Council Approved: April 13, 2018
Effective Date/Approved: April 13, 2018
Revised: N/A
Responsible Party: Vice President for Marketing & Campus Activities

I. PURPOSE

The purpose of the Use of Social Media policy is to provide guidance to ensure that social media tools are used properly, to address potential risks, and to ensure consistency for all social media sites associated with Motlow State Community College.

II. DEFINITIONS

Social media – includes, but is not limited to: Facebook, Twitter, YouTube, Flickr, LinkedIn, Instagram and related systems.

III. POLICY

A. Professional Social Media Accounts
   1. All official social media accounts representing Motlow State Community College, its units/departments/functions must be established and maintained by the Motlow State Community College Webmaster or approved designees.
      a. Access to and passwords for the accounts are limited to designated Marketing & Campus Activities staff members and others only as authorized by the President and/or Vice President for Marketing & Campus Activities and the respective Vice President for the unit.
      b. Any accounts created to imply representation of Motlow State Community College must be approved and authorized by the Vice President for Marketing & Campus Activities and the respective Vice President for the unit.
         i. Password access to management of the social media account must be provided to the Vice President for Marketing & Campus Activities, even if responsibility for the account resides elsewhere.
      c. Content created for and distributed through Motlow State Community College social media accounts is the sole property of the college and not the employee managing the account. All followers, friends and connections associated with the account belong to the college.
         i. Motlow social media account managers must relinquish all rights and access to the accounts upon termination of their employment for any reason.

B. Personal Social Media Accounts
   1. While this policy is not intended to dissuade employees from using personal social media accounts or any other forms of communication protected by local, state or federal law, Motlow employees must abide by the following guidelines when using any form of external electronic social networking, communications systems, web logs (blogs), etc. This applies to both Motlow resources and all other electronic resources, as well as any personal social media/networking/communications accounts.
      a. Do not imply to represent the Motlow in any unauthorized way or identify yourself as a Motlow employee or representative when conducting any of the following activities (the following list is intended to be illustrative and not exhaustive).
         i. Posting, sending or displaying any inappropriate materials or messages including, but not limited to, those identified in TBR Guideline G-054 IT Acceptable Uses .
         ii. Communicating in a way that could negatively impact the reputation of Motlow State Community College or interfere with its mission or performance of its employees.
         iii. Sharing, accessing or discussing any proprietary or confidential information, especially and including, but not limited to those identified in Motlow policies and those governed by copyright law.
         iv. Engaging in political activities, private commercial transactions or private business activities.
         v. Violating any federal, state or local law or policy.
      b. Motlow employees may be honest about their identities and employment; however, they should make very clear when sharing their personal views that they do not represent the views of Motlow State Community College. A disclaimer should be included on employees' personal profiles if Motlow is listed as the employer. (Example: "The views/posts/comments/opinions expressed on this site are my own and do not necessarily reflect the views of Motlow State Community College or the Tennessee Board of Regents.")
      c. Employees may not use the Motlow seal/logo on any unauthorized or personal postings.
      d. Employees' social media accounts may be subject to monitoring without notice or consent if these sites are accessed using Motlow property or resources.
      e. Violation of these policies/guidelines may result in disciplinary action.

MOTLOW STATE COMMUNITY COLLEGE

POLICY

Category
WEBSITE PUBLISHING – 1:08:00:04
Approval
Corresponding Policies: MSCC Policy 1:08:00:00
Leadership Council Approved: April 13, 2018
Effective Date/Approved: April 13, 2018
Revised: N/A
Responsible Party: Vice President for Marketing & Campus Activities

I. PURPOSE

Motlow State Community College websites exist as the institution's most important communication tool. Therefore, websites should maintain and build upon the projected image of Motlow through the highest level of excellence in education, policy, research, and workforce development by concerning the administration with the digital image projected. This policy should facilitate usability and consistency and promote a cohesive online brand throughout all Motlow websites that correlates directly with other Motlow methods of communication and visual representation.

II. GOALS

A. Identify a consistent brand for the Motlow system and all of its programs and services.
B. Effectively serve students, faculty, staff, legislators, and other people of interest with useful and easily accessible information.
C. Provide easy to use information and services on as many devices as possible.
D. Promote a positive impression of Motlow, its staff, and its institutions with a unified and compelling image.
E. Promote ease of use with intuitive web standards.
F. Present Motlow and its activities as a seamless entity.

III. SCOPE

Any Web document that represents Motlow, its units and their activities, its initiatives, its programs and collaborations, and its contractors and partners, while having its own purpose and agenda, is also part of the whole and, therefore, needs to be clearly identified with the Motlow brand and is expected to follow this policy.

IV. Management of Websites

The Webmaster, under direction of the Vice President for Marketing & Campus Activities, maintains and enforces this policy, including any granted exceptions, and has primary responsibility for the content, format and appearance of all web pages and systems.

Updated by TBB using input from PC mtg 4.3.18. Ready to move forward to Leadership Council on 4.13.18 /Users/dseal/Downloads/agenda april 13/1080004 Website Publishing updated 4.5.18 by TBB.DOCX

V. CONTENT MANAGERS

A. Content managers must be classified as regular full-time or regular part-time Motlow staff or an approved third-party vendor who works under the direct supervision of the Webmaster.
B. Request for access must be submitted for each unit/content manager to the Marketing Department who will maintain an accurate list of content managers and the purpose of their access. The Vice President of Marketing & Campus Activities and the unit's leader must approve each access request.
C. Management of web content, including web pages, media and data, and ensuring that pages within their unit are up to date, meaningful and appropriate, and follow the official Motlow Electronic Publishing and Web Style Guide, is the sole responsibility of the corresponding department and their designated content manager(s).
D. Web content ownership and responsibility will be directed to the unit leaders who are ultimately responsible for each unit's access and their web-publishing activities.

VI. GUIDELINES

A. Use
1. Motlow websites may only be used for official college, administrative and educational activities.
2. Websites must comply with all Information Technologies policies regarding the use of Motlow resources.

B. Organization
1. All websites should strive to be a part of the overall web structure of Motlow. No unit may go outside the Motlow web structure and represent itself or activities unless an exception is granted by the Vice President of Marketing & Campus Activities and the respective Vice President for the unit.

C. Web Projects
1. All website projects must comply with Motlow policies and media guidelines, and request for web projects must be submitted in writing via the Marketing Request form and be assessed for feasibility and authorized action.
2. All websites, when feasible, should be developed in-house and within the available systems.
3. If the Marketing determines a project cannot be completed in-house, Marketing will work with the requesting division to develop a project plan and will make a recommendation on how to achieve the desired goal. Marketing, IT, and the collaborating division must achieve approving consensus for any outside contract web project to move forward.

D. Layout and Design Elements
1. All Motlow websites should follow the official Motlow Electronic Publishing and Web Style Guide.
2. When possible, all sites should be developed device agnostic.
3. Visible credits such as "Site powered by..." or "Site created by..." are prohibited.
4. Federal law and guidance letters regarding nondiscrimination policies require that the nondiscrimination statement be available. The official statement will be provided in the Electronic Publishing and Web Style Guide.
5. All websites associated with Motlow and its affiliate groups must follow the current approved Motlow web template(s) and style guides to maintain institutional consistency of image and brand.

E. Accessibility
1. All Motlow websites are subject to the same accessible web standards as state and federal agencies. Section 508 of the Federal Register establishes requirements for federal electronic and information technology, and the federal Access Board has issued the standards to meet those requirements.
2. Websites should be accessible for those using assistive methods and/or alternative methods to access the Web.
3. All Motlow websites should have a link to the Motlow's top-level "Web Accessibility" page.

F. Domains and Sub-domains
1. All domains and related product purchases (secure certificates, etc.) must be made through the Office of Information Technology.
2. The Marketing Vice President and/or Webmaster may make an exception for promotional URLs or collaboratives with other systems/partners, (e.g. tntransferpathways.org). Unless noted in the exception, all promotional domains must forward to an mscc.edu page or sub-domain.

G. Content Validity
1. Content must be kept up-to-date and relevant.
2. Any website or page deemed as outdated or incorrect may be changed or removed by the Webmaster upon notification to the respective unit.

H. Disclaimer of Endorsements
1. While Motlow may allow advertising on select pages, the college does not endorse or recommend any commercial products, processes, or services. It may however, share stories related to the relationships those sponsorships, advertisements, or partnerships reflect. Therefore, mention of commercial products, processes, or services on Motlow websites must be written in a way as they may not be construed as an endorsement or recommendation of products for commercial purchase. Any advertising, logo placement, or third-party reference on the Motlow website much be approved by the Vice President for Marketing & Campus Activities.
2. When users select a link to an external website, users must be made aware they are subject to the privacy and security policies of the owners/sponsors of the external site.

I. Redundancy
1. Redundant information, especially different published versions of content, can be confusing and may result in severe consequences if incorrect or outdated information is posted. Only publish the latest version of content.
2. Repeating static information maintained elsewhere should not be copied but rather linked or be displayed by the use of a data feed such as RSS, XML, or database API.

J. Copyright
All material used on Motlow websites must comply with federal and state copyright laws, including respecting proper licensing rights for purchased reports, data, images, video, and text.

K. Exceptions and Exemptions
1. The Webmaster may exempt certain web applications that are technically limited in their ability to meet the necessary guidelines.
2. Exemptions noted in this document should be requested in writing to the Webmaster and Vice President for Marketing & Campus Activities and the respective Vice President for the unit.

POLICY

Category
CURRICULUM CHAIR SELECTION AND GUIDELINES - 5:10:00:01
Approval
Leadership Council Approved: December 9, 2016
Effective Date/Approved: January 1, 2017
Revised: N/A
Responsible Party: Vice President for Academic Affairs

I. BACKGROUND

Curriculum Chairs are selected for a term of two years by the Vice President for Academic Affairs (VPAA) with input from departmental faculty after careful review of their academic and leadership abilities both in and out of the classroom. Curriculum Chairs may have successive terms. They are evaluated annually by the VPAA with input from the departmental faculty. Curriculum Chairs have the responsibility for reviewing the programs of study, curricular changes, substitutions and waivers and advising the Deans of departmental matters.

II. SELECTION

A. When a curriculum chair position is vacated, the VPAA will send an email announcement to the full-time faculty in the department asking for resumes from interested candidates.
B. Interviews will be scheduled with departmental faculty participating in the interviews.
C. The VPAA will make the final decision with input from the departmental faculty.

III. GUIDELINES

A. To attract and retain the best possible faculty to this position, Motlow State Community College provides the following options:
   1. Curriculum Chairs have a choice of 2 courses per semester release time or a premium stipend.
   2. Premium stipends would be $700 per semester credit hour. This would total $4,200 per semester or $8,400 per academic year.
   3. Additionally, the college will pay a $1,000 per month stipend for June and July for Curriculum Chairs. Summer work is essential for credentialing, textbook, and fall semester adjunct preparation. Summer pay is capped at 25% as per TBR policy.

NOTE: Terms are retroactive for chairs currently in the position upon the revision date of the policy.

MOTLOW STATE COMMUNITY COLLEGE

POLICY

Category
GRANT SUBAWARDS – 4:02:01:01
Approval
Corresponding Policies: TBR Policy 5:01:05:00; TBR Guideline G-030
MSCC Policy 4:02:01:00
Leadership Council Approved: April 13, 2018
Effective Date/Approved: April 13, 2018
Revised: N/A
Responsible Party: Vice President for Finance & Administration

I. POLICY

A. This policy includes the practices and procedures for subrecipient monitoring of sponsored subagreements. Sponsored awards may contain programmatic work that is subcontracted to one or more institutions (subrecipients). The subrecipients are made responsible for a portion of a project awarded to Motlow State Community College. The activities of the subrecipient require the leadership of a Principal Investigator (PI).

B. The PI is responsible for monitoring the subrecipients to ensure that project objectives are met, and that no conflict of interest exists between the Subrecipient, the College or the PI.

II. AUTHORITY

This guidance is established in accordance with:
1. Title 2 in the Code of Federal Regulations (2 CFR) - Part 220,
2. Title 2 in the Code of Federal Regulations (2 CFR) - Part 215,
3. OMB Circular A-133.

III. PROCEDURE

Upon recognizing a potential subrecipient for a proposal, the PI notifies the Grants Office. The PI and the Grants Office will perform a risk analysis to determine the level of risk for subcontracting with the proposed organization/institution. Based on the risk assessment, a determination is made by the Grants Office and the PI whether to continue with a subaward agreement.

A. Risk Assessment
   1. The PI and the Grants Officer will perform a risk assessment of the potential subrecipient to determine the risk category as follows:
      a. Is the subrecipient organization based in the United States?
      b. Is the subrecipient an academic institution or a non-profit subject to federal audit requirements?
      c. Is the subrecipient mature (more than 10 years)?
      d. Does the project have clear and easily-met objectives and milestones, and its progress is measured by observable outcomes?
      e. The project does not involve export-controlled materials?

f. The amount of funding to the subrecipient does not exceed $500,000 nor 50% of award?
g. Is the subrecipient known to have received awards directly from the awarding agency?
h. Does the subrecipient perform annual audits?
i. Does the subrecipient have protocols in place for compliance (such as IRB)?

2. If the answer is **No** to any of the first six questions in Paragraph III. A.1. a through f, then the subrecipient is a high-risk. If all the answers for the first six questions in Paragraph III. A.1. a through f are **Yes**, but the answer is **No** for any of the last three questions in Paragraph III. A.1. g. through i., then the subrecipient is a medium risk. If the answer was **Yes** to all nine questions in Paragraph III. A.1, then the subrecipient is a low-risk.
3. All high risk subrecipients must be approved by the Vice President for Finance and Administration.

B. Vendor or Subrecipient Determination
1. Subrecipient is measured by the following:
   a. Responsible for helping the College meet the requirements of the prime award;
   b. Performs a substantive portion of the project activities which are the primary purpose of the award;
   c. Responsible for incurring project costs that are reasonable and allowable;
   d. Measures performance against the objectives of the Federal program; and
   e. Responsible for adhering to Federal program compliance requirements.
2. A vendor is determined by the following measures:
   a. Provides goods or services as part of its normal business operations to various purchasers;
   b. Provides professional services or highly technical advice;
   c. Provides goods or services which are ancillary to the Federal award; and, is not subject to the compliance requirements of the Federal award.
3. As a general guide, if there is an identified co-principal investigator at the subrecipient organization, and the organization is free to decide how to carry out the activities requested of it, and publications are anticipated from the relationship, then the relationship probably is with a subrecipient.

   If the activity to be performed is a series of repetitive activities that require little judgment from the service provider then the relationship is likely with a vendor.

C. Award Notification and Agreement
1. Upon notification of the prime award, the Grants Officer will notify the PI and request an updated project timeline and scope.
2. After the subagreement is issued, the Grants Office provides a copy to the PI.

IV. SUBRECIPIENT MONITORING

A. The PI has the primary responsibility for reviewing programmatic, timing, administrative activities and compliance of the subrecipient typically on a monthly basis.

B. The Grants Office and Business Office will assist in managing subagreements to provide reasonable assurance that funds are expended according to provisions of pertinent regulations, terms of the award notice, agency requirements, and Office of Management and Budget (OMB) circulars. The PI, Grants Office, and Business Office will annually review and evaluate subrecipient organizations.

C. Progress reports of the subrecipient may be received informally via phone and e-mail communications. Formal technical reports may be required and due on specific dates.

D. Subrecipients are required to submit an invoice to the PI. The PI will ensure the invoices are submitted in accordance with subagreement requirements.

E. The PI will determine that the work is completed and that charges are allowable, allocable to the project and reasonable. The PI's signature acknowledges that work/milestones performed by the subrecipient are acceptable, and deliverables have been received.

F. After the PI approves and signs the invoice, it is submitted to the Grants Office for review. The Grants Office submits the invoice to Business Office for payment, if the invoice meets the conditions outlined in the contract.

V. REVIEWS

A. The Grants Office and Business Office with the assistance of the PI will conduct annual reviews that may include onsite visits to gather updated information and documentation on the financial stability of subrecipient organizations.

B. Decisions will be made within six months after receipt of the subrecipient's financial information. Problems associated with a subrecipient should be reported to the Grants Officer immediately for review. If warranted, the subagreement may be terminated.

C. All high risk subrecipients will also be reviewed by the Vice President for Finance and Administration.

VI. SUBRECIPIENT CLOSEOUT

A. The final invoice must be received and approved prior to the closeout of the prime award.

B. The PI must certify that all technical reports and deliverables and any required documentation have been received, and that the subrecipient has fulfilled its obligations before the final invoice can be paid.

VII. RESPONSIBILITIES

A. Responsibilities of PI:
1. Ensure no conflict of interest exists between his/herself and the potential subrecipient;
2. Negotiate scope of work to be performed by the subrecipient;
3. Responsible for directing and managing fiscal and scientific aspects of sponsored agreement;
4. Jointly Responsible for monitoring subrecipients to ensure compliance with federal regulations, and the award terms and conditions for both the prime and subrecipient award;
5. Report any problems with subrecipient to Business Office and Grants Office upon discovery.

B. The Grants Office at Motlow State Community College is responsible for:
1. Jointly responsible for monitoring subrecipients to ensure compliance with federal regulations, and the award terms and conditions for both the prime and subrecipient award;
2. Reviewing invoices prior to payment for subrecipients.

C. The Business Office at Motlow State Community College is responsible for:
1. Evaluation of single audit (A-133) or program-specific audit results;
2. Serving as Office of Record for record retention of final programmatic and financial reports.

D. The Vice President for Finance and Administration is responsible for:
1. Approval of all high risk subrecipients;
2. Signing all high risk subrecipient agreements;
3. Annually reviewing all high risk subrecipients.

MOTLOW STATE
COMMUNITY COLLEGE

Subrecipient Monitoring Form

(PI is responsible for this plan and initiating amendments and/or renewals to subagreement.)

1. SUBRECIPIENT:		
2. SUBAWARD NUMBER:		
3. SUBAWARD TERM:		
4. DESCRIPTION OF WORK:		
5. PAYMENT FREQUENCY: Quarterly after receipt of Quarterly Progress Report		
6. AMENDMENTS:		
Number	**Date**	**Purpose of Amendment**
7. BUDGET REVISIONS:		
Date	**Amount**	**Purpose of Revision**
8. REPORTS/DELIVERABLES:		
Date Received	**Description**	**Approved?**

9. ACTION SUMMARY: Document and date any activities, accomplishments, or barriers (if applicable) to the performance of this contract.		
Date	**Activity Description**	**Comments**

I certify that, to the best of my knowledge, the above is an accurate account of the goods/ services/activities in regards to this subaward.

Signature of PI

Date