AN AGREEMENT
BY AND BETWEEN
THE TEXAS A&M UNIVERSITY SYSTEM OFFICES
AND ASYSCO, INC.

This Services Agreement ("Agreement") is entered into and effective April 22, 2019 (the "Effective Date"), by and between The Texas A&M University System (hereafter referred to as "A&M System"), an agency of the state of Texas, and Asysco, Inc (hereafter referred to as "ASYSCO"). A&M System and ASYSCO are sometimes hereafter referred to as "Party" individually or "Parties" collectively).

A&M System and ASYSCO hereby agree as follows:

1. SCOPE OF WORK

A. ASYSCO will use reasonable efforts and work with A&M System to perform the scope of work set forth in Exhibit A, Scope of Work ("SOW"), attached hereto and incorporated for all purposes, in accordance with the schedule set forth in Exhibit A. Any revision to the SOW must be set forth in a written modification (a "Change Order") signed by both Parties.

B. The general objective of this Agreement is to provide services relating to re-platforming the A&M System's current Financial Accounting Management Information System ("FAMIS"). The work to be performed by ASYSCO is divided into two phases.

C. Phase 1, Proof of Concept. The objective of the first phase of the work ("Phase 1") is to validate the proof of concept ("POC") for the re-platforming of the FAMIS system.

D. Phase 2: Re-Platforming. If Phase 1 is successful and A&M System believes a full re-platform project can be successfully executed, A&M System may enter into discussions with ASYSCO to develop a statement of work for Phase 2 to complete the full re-platforming. Factors influencing the A&M System decision to proceed with a full re-platforming will be:

(1) The ability of the re-platform technology, as demonstrated in Phase I, to create an application in the desired technical state that is functionally equivalent to the current FAMIS application;
(2) The estimated cost of a full re-platform;
(3) ASYSCO's demonstrated ability to execute the full re-platform project;
(4) The anticipated quality and supportability of the application after the re-platform activity is completed;
(5) Stakeholders feedback on the Project; and
(6) Other factors unrelated to the re-platform Project, not limited to, but including, options for financial solutions available in the marketplace.

E. Authorization to perform Phase 2 can only be accomplished through a written amendment to Exhibit A, signed by both Parties.

2. TERM OF THE AGREEMENT

The initial term of this Agreement shall begin on the Effective Date and will expire upon completion of the Exhibit A deliverables as described herein. Any extensions shall be upon the same terms and conditions plus any approved changes to be determined by A&M System and negotiated in writing with ASYSCO.

3. PAYMENT TERMS

A. For the services rendered under this Agreement, A&M System shall pay ASYSCO in accordance with the provisions of Exhibit A. Any Change Order agreed to by the Parties that affects the payment amount must clearly state the revised payment amount and any changes to Exhibit A that are necessary.

B. ASYSCO shall invoice A&M System according to the payment schedule outlined in Exhibit A. Payment will be made to ASYSCO upon approval of such invoice by A&M System. A&M System will make payment on a properly prepared and submitted invoice within thirty (30) days of the latter of the final acceptance of performance or the receipt of a properly submitted invoice, in conformance with the Texas Prompt Payment law. Generally, payment will be made on the 30th day unless a discount has been arranged for more immediate payment.

C. All payments shall be made by electronic direct deposit. ASYSCO is required to complete and submit to A&M System a Vendor Direct Deposit Authorization form prior to the first payment request. The form can be accessed at;

https://www.tamus.edu/business/budgets-and-accounting/accounting/general/.

All invoices must reference the A&M System purchase order number (which will be provided to ASYSCO within 15 days of the execution of this Agreement) and description of services provided to include but not limited to time, deliverables, and activities.

4. DEFAULT AND TERMINATION

A. In the event of substantial failure by ASYSCO to perform in accordance with the terms hereof, and where ASYSCO has been unable to reasonably remedy such failure, A&M System may terminate this Agreement upon fifteen (15) days written notice of termination setting forth the nature of the failure (the termination shall not be effective if the failure is fully cured prior to the end of the fifteen-day period), provided that said failure is through no fault of A&M System.

B. A&M System may terminate this Agreement for convenience at any time upon thirty (30) days prior notice to ASYSCO. Should A&M System exercise its right to terminate this Agreement for convenience, A&M System agrees to pay ASYSCO a price equal to the full amount of the deliverable (as described in Exhibit A) then in progress at the time of the termination.

5. DATA PRIVACY AND SECURITY

The requirements for data privacy and security are set forth in Exhibit B, which is attached hereto and incorporated by reference.

6. INTELLECTUAL PROPERTY RIGHTS

A. "Intellectual Property" means, individually and collectively: (a) inventions, discoveries, and/or improvements which are conceived or first reduced to practice, whether or not patentable, in the performance of the work under this Agreement; and (b) all works of authorship created, prepared and/or developed (including compilations) in the performance of the work hereunder that are the subject matter of copyright under Chapters 1 through 8 of Title 17 of the United States Code.

B. The allocation of intellectual property rights to Intellectual Property, as well as to pre-existing intellectual property owned by a Party or licensed to a Party by a third party shall be described in the SOW.

7. PUBLIC INFORMATION

A. ASYSCO acknowledges that A&M System is obligated to strictly comply with the Public Information Act, Chapter 552, *Texas Government Code*, in responding to any request for public information pertaining to this Agreement, as well as any other disclosure of information required by applicable Texas law.

B. Upon A&M System's written request, ASYSCO will provide specified public information exchanged or created under this Agreement that is not otherwise excepted from disclosure under chapter 552, Texas Government Code, to A&M System in a non-proprietary format acceptable to A&M System. As used in this provision, "public information" has the meaning assigned Section 552.002, *Texas Government Code*, but only includes information to which A&M System has a right of access.

C. ASYSCO acknowledges that A&M System may be required to post a copy of the fully executed Agreement on its Internet website in compliance with Section 2261.253(a)(1), *Texas Government Code*.

8. DISPUTE RESOLUTION

The dispute resolution process provided in Chapter 2260, *Texas Government Code*, and the related rules adopted by the Texas Attorney General pursuant to Chapter 2260, shall be used by A&M System and ASYSCO to attempt to resolve any claim for breach of contract made by ASYSCO that cannot be resolved in the ordinary course of business. ASYSCO shall submit written notice of a claim of breach of contract under this Chapter to Billy Hamilton, Executive Vice Chancellor and Chief Financial Officer for A&M System, who shall examine ASYSCO's claim and any counterclaim and negotiate with ASYSCO in an effort to resolve the claim.

9. INSURANCE

The requirements for insurance are described in Exhibit C, attached hereto and incorporated by reference.

10. MISCELLANEOUS

A. **Indemnification. Each Party agrees to indemnify and hold harmless the other Party from any claim, damage, liability, expense, or loss to the extent resulting from the negligent or willful acts or omissions of the indemnifying Party, but such indemnity shall not apply to the other Party's negligent or willful errors or omissions under this Agreement. The foregoing obligation only applies to A&M System to the extent permitted by the laws of the State of Texas.**

B. **Independent Contractor.** ASYSCO is an independent contractor, and neither ASYSCO nor any employee of ASYSCO shall be deemed to be an agent or employee of A&M System. A&M System will have no responsibility to provide transportation, insurance or other fringe benefits normally associated with employee status. ASYSCO shall observe and abide by all applicable laws and regulations, policies and procedures, including but not limited to those of A&M System relative to conduct on its premises.

C. **Delinquent Child Support Obligations.** A child support obligor who is more than 30 days delinquent in paying child support and a business entity in which the obligor is a sole proprietor, partner, shareholder, or owner with an ownership interest of at least 25 percent is not eligible to receive payments from state funds under an agreement to provide property, materials, or services until all arrearages have been paid or the obligor is in compliance with a written repayment agreement or court order as to any existing delinquency. The *Texas Family Code* requires the following statement: "Under Section 231.006, *Texas Family Code*, the vendor or applicant certifies that the individual or business entity named in this contract, bid, or application is not ineligible to receive the specified grant, loan, or payment and acknowledges that this contract may be terminated and payment may be withheld if this certification is inaccurate."

D. **Payment of Debt or Delinquency to the State.** Pursuant to Section 2252.903, *Texas Government Code*, ASYSCO agrees that any payments owing to ASYSCO under this Agreement may be applied directly toward certain debts or delinquencies that ASYSCO owes the State of Texas or any agency of the State of Texas regardless of when they arise, until such debts or delinquencies are paid in full.

E. **Previous Employment.** ASYSCO acknowledges and understands that Section 2252.901, *Texas Government Code*, prohibits A&M System from using state appropriated funds to enter into any employment contract, consulting contract, or professional services contract with any individual who has been previously employed, as an employee, by the agency within the past twelve (12) months. If ASYSCO is an individual, by signing this Agreement, ASYSCO certifies that Section 2252.901, *Texas Government Code,* does not prohibit the use of state appropriated funds for satisfying the payment obligations herein.

F. **Franchise Tax Certification.** If ASYSCO is a taxable entity subject to the Texas Franchise Tax (Chapter 171, *Texas Tax Code*), then ASYSCO certifies that it is not currently delinquent in the payment of any franchise (margin) taxes or that ASYSCO is exempt from the payment of franchise (margin) taxes.

G. **State Auditor's Office.** ASYSCO understands that acceptance of funds under this Agreement constitutes acceptance of the authority of the Texas State Auditor's Office, or any successor agency (collectively, "Auditor"), to conduct an audit or investigation in connection with those funds pursuant to Section 51.9335(c), *Texas Education Code*. ASYSCO agrees to cooperate with the Auditor in the conduct of the audit or investigation, including without limitation, providing all records requested. ASYSCO will include this provision in all contracts with permitted subcontractors.

H. **Entire Agreement.** This Agreement constitutes the sole agreement of the parties and supersedes any other oral or written understanding or agreement pertaining to the subject matter of this Agreement. This Agreement may not be amended or otherwise altered except upon the written agreement of both parties.

I. **Severability.** If any provisions of this Agreement are rendered or declared illegal for any reason, or shall be invalid or unenforceable, such provision shall be modified or deleted in such manner so as to afford the Party for whose benefit it was intended the fullest benefit commensurate with making this Agreement, as modified, enforceable, and the remainder of this Agreement and the application of such provision to other persons or circumstances shall not be affected thereby, but shall be enforced to the greatest extent permitted by applicable law.

J. **Headings.** Headings appear solely for convenience of reference. Such headings are not part of this Agreement and shall not be used to construe it.

K. **Non-Assignment.** ASYSCO shall neither assign its rights nor delegate its duties under this Agreement without the prior written consent of A&M System.

L. **HUB Subcontracting Plan.** If a subcontractor will be used to provide any commodity or service as part of the scope on a specific assignment, the ASYSCO will be required to make a good faith effort and complete the state of Texas HSP found at https://www.tamus.edu/business/hub-procurement/hub-programs-3/system-offices-hub-program/. If there are pre-existing agreements in place with companies who will be hired as subcontractors, the ASYSCO will show those companies as subcontractors on the HSP and provide an explanation as to why solicitations were not done, e.g. contractual requirements. If no pre-existing agreements with companies who will be hired as subcontractors exist, then the ASYSCO will be expected to make a good faith effort according to the HSP instructions.

In the event that you determine you will be using a subcontractor, please contact Mr. Jeff Zimmermann from the A&M System's HUB Program at (979) 458-6410 or jzimmermann@tamus.edu for assistance in determining available HUB subcontractors and proper completion of the HSP.

M. **Force Majeure.** Neither party is required to perform any term, condition, or covenant of this Agreement, if performance is prevented or delayed by a natural occurrence, a fire, an act of God, an act of terrorism, or other similar occurrence, the cause of which is not reasonably within the control of such party and which by due diligence it is unable to prevent or overcome.

N. **Loss of Funding.** Performance by A&M System under this Agreement may be dependent upon the appropriation and allotment of funds by the Texas State Legislature (the "Legislature"). If the Legislature fails to appropriate or allot the necessary funds, A&M System will issue written notice to ASYSCO and A&M System may terminate this Agreement without further duty or obligation hereunder. ASYSCO acknowledges that appropriation of funds is beyond the control of A&M System.

O. **Governing Law.** The validity of this Agreement and all matters pertaining to this Agreement, including but not limited to, matters of performance, non-performance**,** breach, remedies, procedures, rights, duties, and interpretation or construction, shall be governed and determined by the Constitution and the laws of the State of Texas.

P. **Venue.** Pursuant to Section 85.18, *Texas Education Code*, venue for any suit filed against A&M System shall be in the county in which the primary office of the chief executive officer of A&M System is located, which is Brazos County, Texas.

Q. **Non-Waiver.** ASYSCO expressly acknowledges that A&M System is an agency of the State of Texas and nothing in this Agreement will be construed as a waiver or relinquishment by A&M System of its right to claim such exemptions, privileges, and immunities as may be provided by law.

R. **Conflict of Interest.** By executing this Agreement, ASYSCO and each person signing on behalf of ASYSCO certifies, and in the case of a sole proprietorship, partnership or corporation, each party thereto certifies as to its own organization, that to the best of their knowledge and belief, no member of The A&M System or The A&M System Board of Regents, nor any employee, or person, whose salary is payable in whole or in part by The A&M System, has direct or indirect financial interest in the award of this Agreement, or in the services to which this Agreement relates, or in any of the profits, real or potential, thereof.

S. **Prohibition on Contracts with Companies Boycotting Israel.** If ASYSCO is a for-profit sole proprietorship, organization, association, corporation, partnership, joint venture, limited partnership, limited liability partnership, or limited liability company, including a wholly owned subsidiary, majority-owned subsidiary, parent company, or affiliate of those entities or business associations that exists to make a profit, by executing this Agreement, the ASYSCO certifies it does not and will not, during the performance of this contract, boycott Israel. ASYSCO acknowledges this Agreement may be terminated if this certification is or becomes inaccurate.

T. **Certification Regarding Business with Certain Countries and Organizations.** Pursuant to Subchapter F, Chapter 2252, Texas Government Code, ASYSCO certifies it is not engaged in business with Iran, Sudan, or a foreign terrorist organization. ASYSCO acknowledges this Agreement may be terminated if this certification is or becomes inaccurate.

U. **Accessibility.** ASYSCO represents and warrants that the electronic and information resources and all associated information, documentation, and support that it provides to the A&M System under this Agreement (collectively, the "EIRs") comply with the applicable requirements set forth in Title 1, Chapter 213 of the Texas Administrative Code and Title 1, Chapter 206, §206.70 of the Texas Administrative Code (as authorized by Chapter 2054, Subchapter M of the Texas Government Code). To the extent ASYSCO becomes aware that the EIRs, or any portion thereof, do not comply, then ASYSCO shall, at no cost to the A&M System, either (1) perform all necessary remediation or (2) replace the EIRs with new EIRs.

V. **Notices.** Any notice required or permitted under this Agreement must be in writing, and shall be deemed to be delivered (whether actually received or not) when deposited with the United States Postal Service, postage prepaid, certified mail, return receipt requested, and addressed to the intended recipient at the address set out below. Notice may also be given by regular mail, personal delivery, courier delivery, facsimile transmission, email or other commercially reasonably means and will be effective when actually received. A&M System and ASYSCO can change their respective notice address by sending to the other party a notice of the new address. Notices should be addressed as follows:

A&M System:

The Texas A&M University System
301 Tarrow St., Suite 361
College Station, Texas 77840
Attention: Jeff Zimmermann
Phone: (979) 458-6410
Fax: (979) 458-6250
E-mail: jzimmermann@tamus.edu

ASYSCO:

Asysco, Inc.
403 Westpark CT, Suite 140
Peachtree City, GA 30269
Attention: Jayson B. Goldman
Phone: 866-241-3301
Email: j.goldman@asysco.com

IN WITNESS WHEREOF, intending to be bound, the Parties have entered into this Agreement as of the Effective Date.

The Texas A&M University System

By Billy Hamilton

Billy Hamilton
Exec. Vice Chancellor & Chief Financial Officer

5/16/19
Date

Asysco, Inc.

By

Jayson B. Goldman, President

05/14/2019
Date

TEXAS A&M UNIVERSITY

EXHIBIT A – SCOPE OF WORK

Asysco Statement of Work for FAMIS Technology Re-Platform Proof of Concept Document version 1.0

Table of Contents

1. Purpose and Confidentiality

This preface contains a statement of purpose, and a confidentiality notice.

1.1 Purpose of the document

This document describes the Statement of Work (“SOW”) for services to be provided under Phase 1, Proof of Concept (the “Services”) of the Agreement, including discovery work, for re-platforming the current Financial Accounting Management Information System (“FAMIS”).

1.2 Confidentiality notice

ASYSCO uses certain proprietary and confidential information, technology, and methodologies, collectively ("ASYSCO Confidential Information”). ASYSCO requires access to the A&M System’s Confidential Information such as FAMIS application data and application code. (“A&M Confidential Information”) for purposes of furnishing to the A&M System the services to be provided under this SOW. Each of the Parties considers its respective Confidential Information to have significant value and agrees to disclose such information to the other Party (the “Receiving Party”) only for the purpose set forth above and the Receiving Party agrees to receive and use such Confidential Information only for such purpose.

The Receiving Party shall not disclose Confidential Information of the other Party to any person or entity except to (i) the employees of the Receiving Party and its Affiliates, and (ii) the consultants, contractors and professional advisors of the Receiving Party and its Affiliates who have a need to know such information provided they have agreed to maintain the confidentiality of such information pursuant to confidentiality agreements containing confidentiality obligations that are not materially less restrictive than those contained herein or they are bound by law or codes of professional conduct to keep such matters confidential (the requirement for a written confidentiality agreement shall not apply to the employees of a Party so long as such employees are informed of and agree to the confidentiality restrictions described herein). The Receiving Party shall use not less than the same degree of care (but not less than a reasonable degree of care) to avoid disclosure of such Confidential Information as it uses for its own confidential information of like importance.

The restrictions on disclosure of Confidential Information shall not apply to any Confidential Information which: (a) is lawfully received free of restriction from another source the Receiving Party reasonably believes is under any obligation to keep the information confidential; (b) is or becomes generally available to the public without breach of these confidentiality provisions by the Receiving Party or its affiliate companies; (c) at the time of disclosure was known to the Receiving Party or its affiliates free of restriction; (d) the Receiving Party’s records demonstrate it was developed independently by the Receiving Party; (e) is approved by the other Party for disclosure; or (f) the Receiving Party is required to disclose pursuant to subpoena, applicable law, or other governmental mandatory process, provided that before making such disclosure the Receiving Party shall furnish the other Party with timely written notice prior to such impending disclosure to permit the other Party to seek a protective order.

2. Objectives

This SOW provides details pertaining to the Services which will be supplied by ASYSCO to the A&M System for Phase 1. This SOW may be updated from time to time by written agreement signed by both Parties. If there are conflicts between this SOW and the terms and conditions in the main body of the Agreement, this SOW shall take precedence.

The A&M System is considering retiring its mainframe computing environment. For this mainframe retirement to occur, FAMIS would need to be migrated to an alternate platform on a X86 architecture. The objective of Phase 1, is to further explore the migration and re-platforming of FAMIS, including programs, databases, JCL and utilities.

2.1. Scope of the Services

The Services outlined in this SOW consist of:

A. Transforming a well-defined number of FAMIS programs ("FAMIS Sub-set")
B. Discovery of the current FAMIS application landscape (AS IS) and description of the target landscape (TO BE)
C. Providing a design, planning, and cost for the re-platforming of FAMIS.
D. In collaboration with the A&M System staff provide communication and awareness to stakeholders across the A&M System. This is to include executive stakeholders, Finance Discovery Working Group, town halls in College Station as well as in north Texas and south Texas, and other stakeholder groups as necessary.

2.2. Timing of the Services

The execution of the Services will be conducted over a period of 4-5 months, currently scheduled to start in the week of April 22, 2019 and ending no later than October 31, 2019. The actual duration may vary, depending on the availability of the A&M System staff during these months.

The October end date may not include all of the Communication and Awareness to stakeholders as this will be dependent on how things are progressing.

2.3. Deliverables of the Services

At the completion of the Services, ASYSCO will present a Discovery Report and the migrated FAMIS Sub-set to all concerned stakeholders of the A&M System.

2.3.1. Discovery Report

The Discovery Report will provide the A&M System with:

- A description of the current mainframe system landscape
- A description of the migration processes required to re-platform FAMIS:
  - Natural to C#
  - ADABAS to Oracle or SQL Server
  - JCL to PowerShell
  - Replacement of all other artifacts, such as Shadow Server software, WYLBUR, etc.
- A budget broken out into deliverables and associated go/no-go decisions, including a fixed

price proposal, required to successfully execute the full FAMIS re-platforming. Not included in such budget are items that are outside the control of ASYSCO, e.g. Hardware acquisition costs, costs of third-party software etc.

- A plan including the efforts and activities of all involved parties, required to perform the full FAMIS re-platforming. Such plan will also include and describe the choices associated with the full FAMIS re-platforming.

2.3.2. FAMIS Sub-set

ASYSCO will prepare an infrastructure to demonstrate and explain the migrated FAMIS Sub-set to the A&M System.

2.4. Phase-2 GO/NO-GO decision

At the end of the Services, the A&M System will be able to decide whether to start Phase-2, i.e. the full FAMIS re-platforming project.

3. Scope of Services

This section describes the work required for the Services to be accomplished.

3.1. POC/FAMIS Sub-set migration

The following processes, code, and activities for the proof of concept are agreed upon and described in the sections below.

Mainframe 3270 Screens

- FAMIS FRS screen 028 - Bank maintenance. This screen, based on user security, will allow a user to add, update, or view FAMIS bank account records.
- FAMIS FRS Screen 112 – Pending voucher create/modify/post. This is a complex data entry screen with pop-up windows that allow the user to create and edit payment vouchers and post them to accounting.
  - Posting of these vouchers to the FAMIS GL will be considered in scope.
- FAMIS Screen 162 – Voucher Search/browse by Vendor. This screen allows a user to view all vouchers for a given vendor. During the POC, vouchers entered on screen 112 should be viewable on screen 162 provided the correct vendor is used.
- FAMIS Screen 168 – voucher total inquiry. This is a standard FAMIS inquiry screen. On this screen users can view full details and line items of a single payment voucher. Vouchers entered in the POC on screen 112 should be viewable on screen 169.
- The above screens should be fully functioning screens with the implementation of:
  - Appropriate help routines
  - Application security and access

Supporting Logon processes

In order to support the above 3270 screens, the FAMIS user logon and initialization process must be executed. These supporting processes are in scope for the POC.

- Identification of initial user is currently done via Natural system variable *INIT-USER which Natural obtains from CICS. ASYSCO or the A&M System may implement a selection screen to simulate various user logons
- User's security profile must be loaded from the FAMIS application security ADABAS files.
- System Globals must be populated with data from the FAMIS application security files and the logon process
- The initial FAMIS FRS menu (screen 001) must be presented
- Navigation to the POC screens (028, 112, 162, etc.) must be supported

Batch Processes and Reports

- FAMIS update program/process FCAU150 – the Concur inbound integration. This process reads a sequential file provided by Concur and takes necessary action on it in the database and produces reports as it executes.
- FAMIS batch program FBMR295. This program produces an end of month account statement and is widely distributed to many stakeholders. The program involves multiple sorts and reporting options.

Data Conversion

- Data conversions of all necessary ADABAS files to support the POC functionality. This is expected to be approximately 20 – 25 ADABAS files.

Shadow Server, Scheduler, and Dynamic "&" Programs

ASYSCO will:

- Analyze the functionality provided by the Shadow Server software and, if possible, demonstrate the equivalent functionality via the implementation of FAMIS program FNNPACDT.
- If possible, demonstrate an equivalent tool for CA-Scheduler to be used in the new environment or at a minimum propose or recommend a replacement.
- Analyze and discuss the approach to the conversion of Dynamic (programs with variables prefixed by "&") programs. These programs are not compiled by the Natural compiler.

Changes to POC FAMIS Sub-set scope

The A&M System understands that the scope of this FAMIS subset must be kept manageable in order to achieve the overall objectives of the POC. At times, reasonable assumptions may need to be made in order to implement the proposed FAMIS sub-set.

The A&M System and ASYSCO will work together and negotiate in good faith to manage the scope of the FAMIS sub-set. Changes to the sub-set must be agreed upon in writing by both Parties.

ASYSCO accepts that the extended scope of the POC compared to the RFP requirements is done with good reasons and has indicated that this will not invoke additional costs over the bid reply on the RFP (RFP01 CIO-19-035).

A&M System Preparation of snapshot

A&M System will create the subset (the POC snapshot) of FAMIS that is consistent, complete and independent enough to be runnable as the POC on a reference mainframe environment, A&M System will install and prove this snapshot before or in parallel with the delivery of the snapshot to ASYSCO including the TestMatch recordings.

ASYSCO Requirements

ASYSCO will transform these components to equivalents of the target environment, i.e.:

- Natural programs, including any reports, to C#
- ADABAS files to RDBMS tables (SQL Server or Oracle)
- JCL to PowerShell scripts
- IBM & ADABAS Utilities to equivalent functionality

For the transformation of these components ASYSCO will use its tools and standard method in a factory setting, i.e. the selected components will be transformed at ASYSCO's premises.

ASYSCO will install the transformed components on an infrastructure representing the target platform and it will share that infrastructure with the A&M System during the Services.

When the migration of the FAMIS Sub-set is complete, ASYSCO will conduct educational sessions for the A&M System staff that would be involved in the full re-platform project. These sessions involve:

- Demonstrate that the FAMIS Sub-set migration process provides identical results
- Review of the database conversions and walk-through of resulting database schema's

- Code walk-through of converted Natural code in the new Java or .NET language
- Walk-through of the new technical IDE and related tools
- Demonstrate how the code in the new development environment can be maintained and updated
- Demonstrate the build and deploy process for the new environment
- Demonstrate the automated testing framework that can be used for the full re-platform project and for on-going maintenance post migration
- Explain and, if possible, demonstrate how batch scheduled output will be processed and delivered
- Demonstrate the operation and execution of transformed JCL scripts for regular scheduled processes
- Explain and demonstrate the approach to character set conversion
- Explain and demonstrate the equivalent/identical commit/rollback functionality with the new code base
- Explain and, if possible, demonstrate the equivalent functionality for the Shadow Server software

3.2. FAMIS discovery

For the FAMIS discovery part of the Services, ASYSCO uses its standard methodology to collect the information about the current FAMIS application landscape required to determine the target landscape. This will be approached through several workshops, during which the A&M System and ASYSCO consultants review the AS IS information. Subsequently, the ASYSCO consultants will continue their synthesis work offsite in ASYSCO's offices.

All FAMIS application landscape components – software, hardware, interfaces, etc. - will be analyzed and inventoried, considering current and future FAMIS requirements and needs.

3.2.1. Questionnaires and Workshops

ASYSCO consultants will meet with the A&M System staff to better understand the current FAMIS application landscape and business requirements. Through questionnaires, workshops, and studying of existing materials, the ASYSCO consultants will collect information to help assess existing and potential future technology infrastructure as well as formulate options for moving to the target platform.

Topics to explore are:

- Existing deployment procedures
- Existing testing abilities and strategies
- VPS mainframe software from Levi, Ray & Shoup, Inc. (LRS) and software from Software AG to direct output to printers and imaging systems
- CA-Scheduler usage
- Used code pages
- Analysis of Shadow Server software
- Refactoring options and opportunities during the re-platform project
- Discuss moving some 3270 screens to Canopy – general strategic direction
- Code control and versioning system

- Approach to be used in the new environment for web services / micros services
- Authentication options to be used with the re-platform project
- Long term reporting strategy for financial data, and the A&M System data warehouse
- AFR reporting
- Integration between Maestro and FAMIS
- Replacement of the WYLBUR software
- Current technology standards
- Resource capabilities and availability
- Surrounding systems impact
- Natural SQL Gateway

Other topics to explore are potentially:

- Change management
- Rollout strategies
- Security concerns; current and future
- Business needs and constraints

The workshops will require the involvement of various A&M System staff (e.g. IT manager or director, project managers, team leaders, developers etc.).

3.2.2. System inventory and analysis of FAMIS artifacts

ASYSCO will provide delivery guidelines to allow the A&M System to extract all FAMIS application artifacts, except data, in a format that can be used by the ASYSCO tools for further analysis and to create the FAMIS system inventory.

Artifacts in use will be inventoried as follows:

- Natural programs
- ADABAS file structures
- File types, e.g. GDG files
- JCL and procedures
- IBM and ADABAS utilities
- CA schedules

Statistics for each technology will be gathered.

Metrics to be gathered or confirmed by technology (Natural, ADABAS, etc.) will be as follows:

- Lines of code
- Number of programs
- Number of sub- and help-programs
- Number of databases and size
- Number of data files and size
- Number and type of interfaces

- Number of test cases

All provided artifacts (Programming language(s), JCL's) will be analyzed by Anubex tools to detect:

- Program dependencies
- Type of intrinsic calls
- Missing components
- Special constructs

3.3. FAMIS solution architecting and project planning

For all FAMIS artifacts, ASYSCO will identify and determine migration strategies that are efficient and that respect the A&M System's business needs.

The principal activities are:

- Identification of target technologies to support FAMIS re-platforming
- Identification of best-of-breed migration and modernization tools and utilities to support project timelines
- Identification of issues that would render the migration of certain artifacts difficult and suggestions for alternative approaches
- Scoping and estimation of total effort required for FAMIS re-platforming
- Defining resource requirements for FAMIS re-platforming, including cost and staffing requirements for all involved parties
- Communication and awareness to stakeholders in the form of onsite presentations.
    - One session in College Station
    - One session in North Texas (Tarleton State University)
    - One session in South Texas (Texas A&M University – San Antonio)

4. Services Deliverables

Upon the end of the Services, the A&M System will be able to take a GO/NO-GO decision in a well-founded way, based on the following deliverables of ASYSCO.

Discovery

POC/FAMIS Sub-set

4.1. Migrated FAMIS Sub-set

ASYSCO will:

- Provide infrastructure containing the migrated FAMIS Sub-set including copy of source code and data in form of SQL database
- Demonstrate to the A&M System stakeholders the migrated FAMIS Sub-set
- Explain to the A&M System development and maintenance staff how to develop and maintain re-platformed FAMIS
- Keep the infrastructure containing the migrated FAMIS Sub-set with the A&M System

during a few weeks for further internal validation by the A&M System staff

4.2. Discovery Report

The FAMIS discovery will provide the following information:

- A solution matrix
  - Description of the current FAMIS application landscape, AS IS
  - Description of the re-platformed FAMIS application landscape, TO BE
- A description of the processes and tools used for the replacement of all FAMIS application components
- A description of the future development and deployment procedures
- A list of challenges for a FAMIS re-platform project
- A list of potential risks and possible mitigation actions for a FAMIS re-platform project

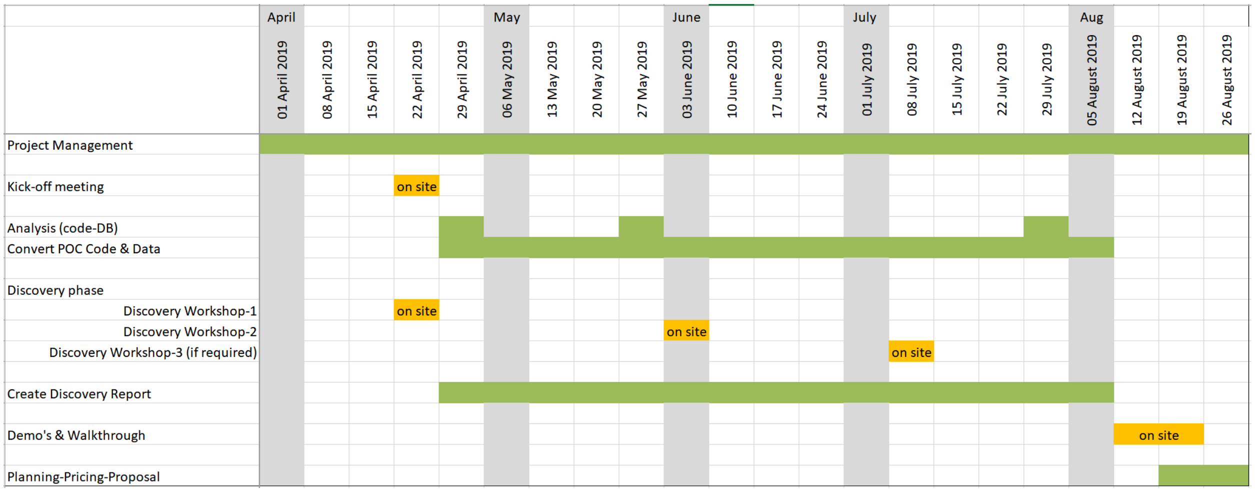
4.3. Phase-2 proposal

The final deliverable by ASYSCO is a proposal for the full re-platforming of FAMIS and includes: (successful outcomes of 4.1 and 4.2 will be GO/NO-GO deliverables and determine if 4.3 proceeds)

- Fixed price cost for the services and tools provided by ASYSCO
- A detailed plan with total duration and milestones for the execution of FAMIS re-platforming
- An overview of the A&M System staff resources required during the execution of FAMIS re-platforming

5. Services Project Plan

The planning of the Services shown here is the original scheme that reflects the course of the Services and the planning shifts depending on the date of the kick-off meeting.



	April					May				June				July					Aug			
	01 April 2019	08 April 2019	15 April 2019	22 April 2019	29 April 2019	06 May 2019	13 May 2019	20 May 2019	27 May 2019	03 June 2019	10 June 2019	17 June 2019	24 June 2019	01 July 2019	08 July 2019	15 July 2019	22 July 2019	29 July 2019	05 August 2019	12 August 2019	19 August 2019	26 August 2019
Project Management	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Kick-off meeting				on site																		
Analysis (code-DB)					🟩				🟩									🟩				
Convert POC Code & Data					🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩			
Discovery phase																						
Discovery Workshop-1				on site																		
Discovery Workshop-2										on site												
Discovery Workshop-3 (if required)															on site							
Create Discovery Report					🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩			
Demo's & Walkthrough																				on site		
Planning-Pricing-Proposal																					🟩	🟩

During the kick-off meeting the parties will discuss and probably adapt this planning according staff availability or depending other factors.

6. Services Assumptions

The following assumptions are in addition to any assumptions that have been expressed throughout the body of this document.

1. In preparation of the Services, ASYSCO has prepared a project plan. This project plan will be discussed during the kick-off meeting, and it will be possible to alter the sequence of the presented topics, in consideration of staff availability.
2. ASYSCO will have access to the A&M System staff who understand the FAMIS application landscape and who know where all components are located and how they can be extracted.
3. ASYSCO will have access to the A&M System staff who understand FAMIS' current and future business requirements.
4. A&M System creates an isolated reference environment on the mainframe with the to-be migrated FAMIS Sub-set application, that can be tested in isolation.
5. ASYSCO receives a specially prepared test data set for use during the FAMIS Sub-set testing in the factory of ASYSCO.
6. ASYSCO receives a small set of batch and online test scenarios for use during the FAMIS Sub-set testing in the factory of ASYSCO.
7. When working at the A&M System locations, ASYSCO staff will receive adequate infrastructure (office space and computer systems, internet access, remote access to ASYSCO systems) to execute their activities.
8. Parties will install a Steering Committee who meets at least once per month during the duration of the Services.
9. A resource workday is assumed to be eight (8) hours.

7. Services Project Pricing

For the proposed scope of work and deliverables during the five (5) month engagement the total fixed price amount of $297,231.

The payment schedule, based off the project deliverables, is as follows:

1. 10%- Upon execution of Agreement
2. 20%- At delivery of 1st Workshop
3. 25%- At delivery of 2nd Workshop
4. 25%- At delivery/demo of migrated FAMIS Sub-set
5. 20%- At delivery of Discovery Report and Phase-2 Proposal

Payment terms are set forth in Section 3 of the main body of the Agreement.

8. Intellectual Property

No intellectual property will be created in the course of performing this Phase I Statement of Work (Proof of Concept).

EXHIBIT B – DATA PRIVACY AND SECURITY

A. Definitions.

1. “Confidential Information” means any information that a disclosing party treats in a confidential manner and that is marked “Confidential Information” prior to disclosure to the other party. Confidential Information does not include information which: (a) is public or becomes public through no breach of the confidentiality obligations of this Agreement; (b) is disclosed by the Party that has received Confidential Information (the “Receiving Party”) with the prior written approval of the other Party; (c) was known by the Receiving Party at the time of disclosure; (d) was developed independently by the Receiving Party without use of the Confidential Information; (e) becomes known to the Receiving Party from a source other than the disclosing Party through lawful means; (f) is disclosed by the disclosing Party to others without confidentiality obligations; or (g) is required by law to be disclosed.
2. “Data” means all information, whether in oral or written (including electronic) form, created by or in any way originating with the A&M System and all information that is the output of any computer processing, or other electronic manipulation, of any information that was created by or in any way originating with the A&M System in the course of using and configuring the Services provided under this Agreement, and includes the A&M System Data and Protected Information.
3. “Data Compromise” means any actual or reasonably suspected unauthorized access to or acquisition of computerized Data that compromises the security, confidentiality, or integrity of the Data, or the ability of the A&M System to access the Data.
4. “Protected Information” includes but is not limited to personally-identifiable information, student records, protected health information, or individual financial information that is subject to Texas, other state, or federal laws restricting the use and disclosure of such information, including, but not limited to the federal Gramm-Leach-Bliley Act (15 U.S.C. §§ 6801 through 6809; the federal Family Educational Rights and Privacy Act (20 U.S.C. § 1232g); and the privacy and information security aspects of the Administrative Simplification provisions of the federal Health Insurance Portability and Accountability Act (45 CFR Part 160 and Subparts A, C, and E of Part 164).

B. Data Privacy

1. ASYSCO will use the Data only for the purpose of fulfilling its duties under this Agreement and for the A&M System’s sole benefit, and will not share such Data with or disclose it to any third party without the prior written consent of the A&M System or as otherwise required by law. Consent is hereby given for ASYSCO to share such Data with Anubex NV. By way of illustration and not of limitation, ASYSCO will not use such Data for ASYSCO’s own benefit and, in particular, will not engage in “data mining” of the Data or communications, whether through automated or human means, except as specifically and expressly required by law or authorized in writing by the A&M System.

2. All Data must be stored on servers located solely within the Continental United States.

3. ASYSCO will provide access to the Data only to those ASYSCO employees, contractors and subcontractors (“ASYSCO Staff”) who need to access the Data to fulfill ASYSCO’s obligations under this Exhibit B and the Agreement. ASYSCO will ensure that, prior to

being granted access to the Data, ASYSCO staff who perform work under this Agreement have successfully completed annual instruction of a nature sufficient to enable them to effectively comply with all Data protection provisions of this Exhibit B and the Agreement; and possess all qualifications appropriate to the nature of the employees' duties and the sensitivity of the Data they will be handling.

4. The A&M System is subject to the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g and its implementing regulations ("FERPA"). To the extent ASYSCO has access to "Education Records", ASYSCO is deemed a "school official" as each of these terms is defined in FERPA. In addition, ASYSCO agrees to abide by the limitations and requirements imposed on school officials in FERPA.

5. The A&M System represents that it may be deemed a "financial institution" subject to the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809 and its implementing regulations ("GLB"). Without representing that it is subject to GLB, ASYSCO acknowledges that it may have access under the Agreement to the A&M System's financial information and other nonpublic personal information protected under GLB. To assist the A&M System in meeting its GLB obligations, ASYSCO must implement, maintain, and use appropriate and sufficient administrative, technical, and physical security measures to protect the confidentiality and integrity of all electronically maintained or transmitted Data. ASYSCO must protect the Data according to commercially acceptable standards and no less rigorously than it protects its own confidential information.

C. <u>Data Security and Integrity</u>

1. All facilities used by ASYSCO and its subcontractors to store and process the Data must implement and maintain administrative, physical, technical, and procedural safeguards and best practices at a level sufficient to secure such Data from unauthorized access, destruction, use, modification, or disclosure. Such measures will be no less protective than those used to secure ASYSCO's own Data of a similar type, and in no event less than reasonable in view of the type and nature of the Data involved.

2. ASYSCO shall maintain the administrative, physical, technical, and procedural infrastructure associated with the provision of the Services to the A&M System in a manner that is, at all times during the term of this Agreement, at a level equal to or more stringent than those specified in ISO, NIST FIPS, or SSAC-16/SOC2.

3. Without limiting the foregoing, ASYSCO warrants that all Data will be encrypted in transmission (including via web interface) and in storage at a level equivalent to or stronger than 128-bit level encryption or 3DES.

4. ASYSCO shall at all times use industry-standard and up-to-date security tools, technologies and procedures including, but not limited to anti-virus and anti-malware protections and intrusion detection and reporting methods in providing Services under this Agreement.

5. Prior to the Effective Date of this Agreement, ASYSCO will at its expense conduct or have conducted the following, and thereafter, ASYSCO will at its expense conduct or have

conducted the following upon request by the A&M System and immediately after any actual or reasonably suspected Data Compromise:

(a) A SSAE 16/SOC 2 audit of ASYSCO's security policies, procedures and controls and certification under NIST FIPS 200 AND SP 800-53 or ISO 27001/27002.
(b) A vulnerability scan, performed by an A&M System-approved third-party scanner, of ASYSCO's systems and facilities that are used in any way to deliver Services under this Agreement;
(c) A formal penetration test, performed by process and qualified personnel approved by the A&M System, of ASYSCO's systems and facilities that are used in any way to deliver Services under this Agreement.

6. ASYSCO will provide the A&M System the reports or other documentation resulting from the above audits, certifications, scans and tests within seven (7) business days of ASYSCO's receipt of such results.

7. Based on the results of the above audits, certifications, scans and tests, ASYSCO will, within thirty (30) calendar days of receipt of such results, promptly modify its security measures in order to meet its obligations under this Agreement, and provide the A&M System with written evidence of remediation.

8. The A&M System may require, at its expense, ASYSCO to perform additional audits and tests, the results of which will be provided to the A&M System within seven (7) business days of ASYSCO's receipt of such results.

9. ASYSCO shall protect the Data against deterioration or degradation of quality and/or authenticity, including, but not limited to annual third-party Data integrity audits. ASYSCO must provide A&M System the results of the above audits, along with ASYSCO's plan for addressing or resolving any shortcomings identified by such audits, within seven (7) business days of ASYSCO's receipt of such results.

D. <u>Response to Legal Orders, Demands, or Requests for Data</u>

1. Except as otherwise expressly prohibited by law, ASYSCO will:

(a) If required by a court of competent jurisdiction or an administrative body to disclose the Data, ASYSCO will notify the A&M System in writing immediately upon receiving notice of such requirement and prior to any such disclosure;
(b) Consult with the A&M System regarding its response;
(c) Cooperate with any reasonable A&M System request in connection with efforts by the A&M System to intervene and quash or modify the legal order, demand or request; and
(d) Upon the A&M System's request, provide the A&M System with a copy of ASYSCO's response.

2. If the A&M System receives a subpoena, warrant, or other legal order, demand or request seeking the Data maintained by ASYSCO, the A&M System will promptly provide a copy to ASYSCO. ASYSCO will supply the A&M System with copies of Data required for the

A&M System to respond within forty-eight (48) hours after receipt of copy from the A&M System, and will cooperate with A&M System's reasonable requests in connection with its response.

E. Data Compromise Response

1. ASYSCO shall report, either orally or in writing, to the A&M System any Data Compromise involving the Data, or circumstances that could have resulted in unauthorized access to or disclosure or use of the Data, not authorized by this Agreement or in writing by the A&M System, including any reasonable belief that an unauthorized individual has accessed the Data. ASYSCO shall make the report to the A&M System immediately upon discovery of the unauthorized disclosure, but in no event more than forty-eight (48) hours after ASYSCO reasonably believes there has been such unauthorized use or disclosure. Oral reports by ASYSCO regarding Data Compromises will be reduced to writing and supplied to the A&M System as soon as reasonably practicable, but in no event more than forty-eight (48) hours after oral report.

2. Immediately upon becoming aware of any such Data Compromise, ASYSCO shall fully investigate the circumstances, extent and causes of the Data Compromise, and report the results to the A&M System and continue to keep the A&M System informed on a daily basis of the progress of its investigation until the issue has been effectively resolved.

3. ASYSCO's report discussed herein shall identify: (a) the nature of the unauthorized use or disclosure; (b) the Data used or disclosed; (c) who made the unauthorized use or received the unauthorized disclosure (if known); (d) what ASYSCO has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure; and (e) what corrective action ASYSCO has taken or shall take to prevent future similar unauthorized use or disclosure.

4. Within five (5) calendar days of the date ASYSCO becomes aware of any such Data Compromise, ASYSCO shall have completed implementation of corrective actions to remedy the Data Compromise, restore the A&M System access to the Services as directed by the A&M System, and prevent further similar unauthorized use or disclosure.

5. ASYSCO, at its expense, shall cooperate fully with the A&M System's investigation of and response to any such Data Compromise incident.

6. Except as otherwise required by law, ASYSCO will not provide notice of the incident directly to the persons whose Data were involved, regulatory agencies, or other entities, without prior written permission from the A&M System.

7. Notwithstanding any other provision of the Agreement, and in addition to any other remedies available to the A&M System under law or equity, ASYSCO will promptly reimburse A&M System in full for all costs incurred by A&M System in any investigation, remediation or litigation resulting from any such Data Compromise, including but not limited to providing notification to third parties whose Data were compromised and to regulatory bodies, law-enforcement agencies, or other entities as required by law or contract; establishing and monitoring call center(s), and credit monitoring and/or identity restoration services to assist each person impacted by a Data Compromise in such a fashion that, in the A&M System's sole discretion, could lead to identity theft; and the

payment of legal fees and expenses, audit costs, fines and penalties, and other fees imposed by regulatory agencies, courts of law, or contracting partners as a result of the Data Compromise.

F. Data Retention and Disposal

1. Using appropriate and reliable storage media, ASYSCO will regularly backup the Data and retain such backup copies for a minimum of twelve (12) months.

2. At the A&M System's election, ASYSCO will either securely destroy or transmit to the A&M System repository any backup copies of the Data. ASYSCO will supply the A&M System with a certificate indicating the records disposed of, the date disposed of, and the method of disposition used.

3. ASYSCO will immediately place a "hold" on Data destruction or disposal under its usual records retention policies of records that include the Data, in response to an oral or written request from the A&M System indicating that those records may be relevant to litigation that the A&M System reasonably anticipates. Oral requests by the A&M System for a hold on record destruction will be reduced to writing and supplied to ASYSCO for its records as soon as reasonably practicable under the circumstances. A&M System will promptly coordinate with ASYSCO regarding the preservation and disposition of these records. ASYSCO shall continue to preserve the records until further notice by the A&M System.

G. Data Transfer Upon Termination or Expiration

1. Upon termination or expiration of the Agreement, ASYSCO will ensure that all Data are securely transferred to the A&M System, or a third party designated by the A&M System, within thirty (30) calendar days thereafter. The Data returned shall be in the following format: Standard SQL server backup format and by the following method: Secure FTP/TSL. ASYSCO will ensure that such migration uses facilities and methods that are compatible with the relevant systems of the A&M System, and that the A&M System will have access to the Data during the transition. In the event that it is not possible to transfer the aforementioned data to A&M System in a format that does not require proprietary software to access the data, ASYSCO shall provide the A&M System with an unlimited use, perpetual license to any proprietary software necessary in order to gain access to the Data.

2. ASYSCO will provide the A&M System with no less than ninety (90) calendar days' notice of impending cessation of its business or that of any ASYSCO subcontractor and any contingency plans in the event of notice of such cessation. This includes immediate transfer of any previously escrowed assets and Data and providing the A&M System access to ASYSCO's facilities to remove and destroy the Data.

H. HIPAA Specific Provisions

1. Definitions. Except as otherwise defined in this Exhibit B, all capitalized terms used in this Exhibit B shall have the meanings set forth in HIPAA.

"Business Associate" shall refer to ASYSCO and shall have the same meaning to the term "Associate" under the Privacy Rule, including, but not limited to, 45 CFR Section 160.103.

"Breach" shall mean the acquisition, access, use or disclosure of Protected Health Information in a manner not permitted by the HIPAA Privacy Rule that compromises the security or privacy of the Protected Health Information as defined, and subject to the exceptions set forth, in 45 CFR § 164.402.

"Covered Entity" shall refer to the A&M System and shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 CFR Section 160.103.

"Data Aggregation Services" shall mean the combining of PHI or EPHI by Business Associate with the PHI or EPHI received by Business Associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of, payment to, and treatment of patients by the respective covered entities.

"Electronic Protected Health Information" shall mean Protected Health Information that is transmitted or maintained in Electronic Media.

"HIPAA" shall mean the Health Insurance Portability and Accountability Act of 1996 and the implementing regulations, as amended and supplemented by the HITECH Act and its implementing regulations, as each is amended from time to time.

"HIPAA Breach Notification Rule" shall mean the federal breach notification regulations, as amended from time to time, issued under HIPAA and set forth in 45 CFR Part 164 (Subpart D).

"HIPAA Privacy Rule" shall mean the federal privacy regulations, as amended from time to time, issued under HIPAA and set forth in 45 CFR Parts 160 and 164 (Subparts A & E).

"HIPAA Security Rule" shall mean the federal security regulations, as amended from time to time, issued under HIPAA and set forth in 45 CFR Parts 160 and 164 (Subparts A & C).

"HITECH Act" shall mean Subtitle D of the Health Information Technology for Economic and Clinical Health Act provisions of the American recovery and Reinvestment Act of 2009, 42 U.S.C. §§ 17921-17954, and all its implementing regulations, when and as each is effective and compliance is required.

"Protected Health Information of PHI" shall mean Protected Health Information, as defined in 45 CFR § 160.103, and is limited to the Protected Health Information received, maintained, created or transmitted on behalf of, Covered Entity by Business Associate in performance of the Underlying Services.

"Underlying Services" shall mean, to the extent and only to the extent they involve the creation, maintenance, use, disclosure or transmission of Protected Health Information, the services performed by Business Associate for Covered Entity pursuant to the Underlying Services Agreement.

Underlying Services Agreement" shall mean the Agreement to which this Exhibit B is attached pursuant to which Business Associate access to, receives, maintains, creates or transmits PHI for or on behalf of Covered Entity in connection with the provision of the services described in that agreement(s) by Business Associate to Covered Entity or in performance of Business Associate's obligations under such Agreement.

2. Business Associate Obligations. Business Associate may receive from Covered Entity, or create or receive or maintain on behalf of Covered Entity, health information that is protected under applicable state and/or federal law, including without limitation, PHI and EPHI. All references to PHI herein shall be construed to include EPHI. Business Associate agrees not to use or disclose (or permit the use or disclosure of) PHI in a manner that would violate the Privacy Standards, Security Standards the HITECH Act, or Texas law, including without limitation the provisions of Texas Health and Safety Code Chapters 181 and 182 as amended by HB 300 (82nd Legislature), effective September 1, 2012, in each case including any implementing regulations as applicable (collectively referred to hereinafter as the "Confidentiality Requirements") if the PHI were used or disclosed by Covered Entity in the same manner.

3. Use of Protected Health Information. Except as otherwise required by law, Business Associate shall use PHI in compliance with 45 C.F.R. § 164.504(e). Furthermore, Business Associate shall use PHI (i) solely for Covered Entity's benefit and only for the purpose of performing services for Covered Entity as such services are described in Exhibit A of the Agreement and as necessary for the Business Associate or to carry out its legal responsibilities, provided that such uses are permitted under federal and state law. For avoidance of doubt, under no circumstances may Business Associate sell PHI in such a way as to violate Texas Health and Safety Code, Chapter 181.153, as amended by HB 300 (82nd Legislature), effective September 1, 2012, nor shall Business Associate use PHI for marketing purposes in such as manner as to violate Texas Health and Safety Code Section 181.152, or attempt to re-identify any information in violation of Texas Health and Safety Code Section 181.151, regardless of whether such action is on behalf of or permitted by the Covered Entity.

4. Disclosure of Protected Health Information. Subject to any limitations in the Agreement or this Exhibit B, Business Associate may disclose PHI to any third-party persons or entities as necessary to perform its obligations under the Agreement and as permitted or required by applicable federal or state law. Business Associate recognizes that under the HIPAA/HITECH Omnibus Final Rule, Business Associates may not disclose PHI in a way that would be prohibited if Covered Entity made such a disclosure. Any disclosures made by Business Associate will comply with minimum necessary requirements under the Privacy Rule and related regulations. Business Associate shall not, and shall provide that its directors, officers, employees, subcontractors, and agents, shall not disclose PHI to any other person (other than members of their respective workforce), unless disclosure is required by law or authorized by the person whose PHI is to be disclosed. Any such disclosure other than as specifically permitted in the immediately preceding sentences shall be made only if such person to whom a disclosure (a "disclosee") has previously signed a written agreement that:

(a) Binds the disclosee to the provisions of the Agreement and this Exhibit B pertaining to PHI, for the express benefit of Covered Entity, Business Associate and, if disclosee is other than Business Associate, the disclosee;
(b) Contains reasonable assurances from disclosee that the PHI will be held confidential as provided in the Agreement and this Exhibit B, and only disclosed as required by law for the purposes for which it was disclosed to disclosee; and,
(c) Obligates disclosee to immediately notify Business Associate of any breaches of the confidentiality of the PHI, to the extent disclosee has obtained knowledge of such breach.

Business Associate shall not disclose PHI to any member of its workforce and shall provide that its subcontractors and agents do not disclose PHI to any member of their respective workforces, unless Business Associate or such subcontractor or agent has advised such person of Business Associate's obligations under the Agreement and this Exhibit B, and of the consequences for such person and for Business Associate or such subcontractor or agent of violating them as memorialized in a business associate agreement pursuant to the HIPAA/HITECH Omnibus Final Rule. Business Associate shall take and shall provide that each of its subcontractors and agents take appropriate disciplinary action against any member of its respective workforce who uses or discloses PHI in contravention of the Agreement or this Exhibit B. In addition to Business Associate's obligations under Section 9, below, Business Associate agrees to mitigate, to the extent commercially practical, harmful effects that are known to Business Associate and is the result of a use or disclosure of PHI by Business Associate or Recipients in violation of the Agreement or this Exhibit B.

5. Access to and Amendment of Protected Health Information. To the extent applicable, Business Associate shall (a) provide access to, and permit inspection and copying of, PHI by Covered Entity; and (b) amend PHI maintained by Business Associate as requested by Covered Entity. Any such amendments shall be made in such a way as to record the time and date of the change, if feasible, and in accordance with any subsequent requirements promulgated by the Texas Medical Board with respect to amendment of electronic medical records by HIEs. Business Associate shall respond to any request from Covered Entity for access by an individual within seven (7) days of such request and shall make any amendment requested by Covered Entity within twenty (20) days of the later of (x) such request by Covered Entity or (y) the date as of which Covered Entity has provided Business Associate with all information necessary to make such amendment. Business Associate may charge a reasonable fee based upon the Business Associate's labor costs in responding to a request for electronic information (or the fee approved by the Texas Medical Board for the production of non-electronic media copies). Business Associate shall notify Covered Entity within five (5) days of receipt of any request for access or amendment by an individual. Covered Entity shall determine whether to grant or deny any access or amendment requested by the individual. Business Associate shall have a process in place for requests for amendments and for appending such requests and statements in response to denials of such requests to the Designated Record Set, as requested by Covered Entity.

6. Accounting of Disclosures. Business Associate shall make available to Covered Entity in response to a request from an individual, information required for an accounting of disclosures of PHI with respect to the individual in accordance with 45 CFR § 164.528, as

amended by Section 13405(c) of the HITECH Act and any related regulations or guidance issued by HHS in accordance with such provision.

7. Records and Audits. Business Associate shall make available to the United States Department of Health and Human Services or its agents, its internal practices, books, and records relating to the use and disclosure of PHI received from, created, or received by Business Associate on behalf of Covered Entity for the purpose of determining Covered Entity's compliance with the Confidentiality Requirements or the requirements of any other health oversight agency, in a time and manner designated by the Secretary.

8. Implementation of Security Standards; Notice of Security Incidents. Business Associate will use appropriate safeguards to prevent the use or disclosure of PHI other than as expressly permitted under the Agreement or this Exhibit B. Business Associate will implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the PHI that it creates, receives, maintains or transmits on behalf of Covered Entity. Business Associate acknowledges that the HITECH Act requires Business Associate to comply with 45 C.F.R. §§164.308, 164.310, 164.312 and 164.316 as if Business Associate were a Covered Entity, and Business Associate agrees to comply with these provisions of the Security Standards and all additional security provisions of the HITECH Act. Furthermore, to the extent feasible, Business Associate will use commercially reasonable efforts to secure PHI through technology safeguards that render such PHI unusable, unreadable and indecipherable to individuals unauthorized to acquire or otherwise have access to such PHI in accordance with HHS Guidance published at 74 Federal Register 19006 (April 17, 2009), or such later regulations or guidance promulgated by HHS or issued by the National Institute for Standards and Technology ("NIST") concerning the protection of identifiable data such as PHI. Lastly, Business Associate will promptly report to Covered Entity any successful Security Incident of which it becomes aware. At the request of Covered Entity, Business Associate shall identify: the date of the Security Incident, the scope of the Security Incident, the Business Associate's response to the Security Incident and the identification of the party responsible for causing the Security Incident, if known.

9. Data Breach Notification and Mitigation.

   (a) Business Associate agrees to implement reasonable systems for the discovery and prompt reporting to Covered Entity of any "breach" of "unsecured PHI" as those terms are defined by 45 C.F.R. §164.402. Specifically, a breach is an unauthorized acquisition, access, use or disclosure of unsecured PHI, including ePHI, which compromises the security or privacy of the PHI/ePHI. A breach is presumed to have occurred unless there is a low probability that the PHI has been compromised based on a risk assessment of at least the factors listed in 45 C.F.R. § 164.402(2)(i)-(iv) (hereinafter a "HIPAA Breach"). The Parties acknowledge and agree that 45 C.F.R. § 164.404 governs the determination of the date of discovery of a HIPAA Breach. In addition to the foregoing and notwithstanding anything to the contrary herein, Business Associate will also comply with applicable state law, including without limitation, Section 521 Texas Business and Commerce Code, as amended by HB 300 (82nd Legislature), or such other laws or regulations as may later be amended or adopted. In the event of any conflict between this section, the Confidentiality

Requirements, Section 521 of the Texas Business and Commerce Code, and any other later amended or adopted laws or regulations, the most stringent requirements shall govern.

(b) Discovery of Breach. Business Associate will, following the discovery of a HIPAA Breach, notify Covered Entity without unreasonable delay and in no event later than the earlier of the maximum of time allowable under applicable law or three (3) business days after Business Associate discovers such HIPAA Breach, unless Business Associate is prevented from doing so by 45 C.F.R. §164.412 concerning law enforcement investigations. For purposes of reporting a HIPAA Breach to Covered Entity, the discovery of a HIPAA Breach shall occur as of the first day on which such HIPAA Breach is known to the Business Associate or, by exercising reasonable diligence, would have been known to the Business Associate. Business Associate will be considered to have had knowledge of a HIPAA Breach if the HIPAA Breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the HIPAA Breach) who is an employee, officer or other agent of the Business Associate.

(c) Reporting a Breach. Without unreasonable delay and no later than the earlier of the maximum of time allowable under applicable law or five (5) business days following a HIPAA Breach, Business Associate shall provide Covered Entity with sufficient information to permit Covered Entity to comply with the HIPAA Breach notification requirements set forth at 45 C.F.R. § 164.400 et seq. Specifically, if the following information is known to (or can be reasonably obtained by) the Business Associate, Business Associate will provide Covered Entity with:

(1) contact information for individuals who were or who may have been impacted by the HIPAA Breach (e.g., first and last name, mailing address, street address, phone number, email address);
(2) a brief description of the circumstances of the HIPAA Breach, including the date of the HIPAA Breach and date of discovery;
(3) a description of the types of unsecured PHI involved in the HIPAA Breach (e.g., names, social security number, date of birth, addressees, account numbers of any type, disability codes, diagnostic and/or billing codes and similar information);
(4) a brief description of what the Business Associate has done or is doing to investigate the HIPAA Breach, mitigate harm to the individual impacted by the HIPAA Breach, and protect against future HIPAA Breaches; and,
(5) appoint a liaison and provide contact information for same so that Covered Entity may ask questions or learn additional information concerning the HIPAA Breach.

Following a HIPAA Breach, Business Associate will have a continuing duty to inform Covered Entity of new information learned by Business Associate regarding the HIPAA Breach, including but not limited to the information described above.

10. Termination. Upon the termination of the Agreement for any reason, Business Associate agrees:

(a) to return to Covered Entity or to destroy all PHI received from Covered Entity or otherwise through the performance of services for Covered Entity, that is in the possession or control of Business Associate or its agents. Business Associate agrees that all paper, film, or other hard copy media shall be shredded or destroyed such that it may not be reconstructed, and EPHI shall be purged or destroyed concurrent with NIST Guidelines for media sanitization at http://www.csrc.nist.gov/; or,

(b) in the case of PHI which is not feasible to "return or destroy," to extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI. Business Associate further agrees to comply with other applicable state or federal law, which may require a specific period of retention, redaction, or other treatment of such PHI.

I. Miscellaneous.

This Exhibit B is subject to the other terms and conditions of the Agreement.

EXHIBIT C – INSURANCE

ASYSCO shall obtain and maintain, for the duration of this Agreement or longer, the minimum insurance coverage set forth below. With the exception of Professional Liability (E&O), all coverage shall be written on an occurrence basis. All coverage shall be underwritten by companies authorized to do business in the State of Texas or eligible surplus lines insurers operating in accordance with the Texas Insurance Code and have a financial strength rating of A- or better and a financial strength rating of VII or better as measured by A.M. Best Company or otherwise acceptable to A&M System. By requiring such minimum insurance, the Owner shall not be deemed or construed to have assessed the risk that may be applicable to ASYSCO under this Agreement. ASYSCO shall assess its own risks and if it deems appropriate and/or prudent, maintain higher limits and/or broader coverage. ASYSCO is not relieved of any liability or other obligations assumed pursuant to this Agreement by reason of its failure to obtain or maintain insurance in sufficient amounts, duration, or types. No policy will be canceled without unconditional written notice to A&M System at least ten days before the effective date of the cancellation.

Insurance:

Coverage	**Limit**
A. **Worker's Compensation**	
Statutory Benefits (Coverage A)	Statutory
Employers Liability (Coverage B)	$1,000,000 Each Accident
	$1,000,000 Disease/Employee
	$1,000,000 Disease/Policy Limit

Workers' Compensation policy must include under Item 3.A. on the information page of the workers' compensation policy the state in which work is to be performed for A&M System. Workers' compensation insurance is required, and no "alternative" forms of insurance will be permitted

B. **Automobile Liability**

Business Auto Liability Insurance covering all owned, non-owned or hired automobiles, with limits of not less than $1,000,000 Single Limit of liability per accident for Bodily Injury and Property Damage;

If a separate Business Auto Liability policy is not available, coverage for hired and non-owned auto liability may be endorsed on the Commercial General Liability policy.

Additional Endorsements

The Auto and Commercial General Liability Policies shall name the Texas A&M University System Board of Regents for and on behalf of The Texas A&M University System as additional insured's.

C. **Commercial General Liability**	
Each Occurrence Limit	$1,000,000
General Aggregate Limit	$2,000,000
Products / Completed Operations	$1,000,000
Personal / Advertising Injury	$1,000,000

Damage to rented Premises	$300,000
Medical Payments	$5,000

The required commercial general liability policy will be issued on a form that insures ASYSCO's or its subcontractors' liability for bodily injury (including death), property damage, personal and advertising injury assumed under the terms of this Agreement

D. **Professional Liability (Errors & Omissions)** Insurance with limits of not less than $1,000,000 each occurrence, $2,000,000 aggregate. Such insurance will cover all professional services rendered by or on behalf of ASYSCO and its subcontractors under this Agreement. Renewal policies written on a claims-made basis will maintain the same retroactive date as in effect at the inception of this Agreement. If coverage is written on a claims-made basis, ASYSCO agrees to purchase an Extended Reporting Period Endorsement, effective for two (2) full years after the expiration or cancellation of the policy. No professional liability policy written on an occurrence form will include a sunset or similar clause that limits coverage unless such clause provides coverage for at least three (2) years after the expiration of cancellation of this Agreement.

E. **ASYSCO will deliver to A&M System**:

Evidence of insurance on a Texas Department of Insurance approved certificate form verifying the existence and actual limits of all insurance after the execution and delivery of this Agreement and prior to the performance of any services by ASYSCO under this Agreement. Additional evidence of insurance will be provided on a Texas Department of Insurance approved certificate form verifying the continued existence of all required insurance no later than thirty (30) days after each annual insurance policy renewal.

All insurance policies, with the exception of worker's compensation, employer's liability and professional liability will be endorsed and name The Board of Regents for and on behalf of The Texas A&M University System and The Texas A&M University System as Additional Insureds up to the actual liability limits of the policies maintained by ASYSCO. Commercial General Liability and Business Auto Liability will be endorsed to provide primary and non-contributory coverage. The Commercial General Liability Additional Insured endorsement will include on-going and completed operations and will be submitted with the Certificates of Insurance.

All insurance policies will be endorsed to provide a waiver of subrogation in favor of The Board of Regents of The Texas A&M University System and The Texas A&M University System. No policy will be canceled without unconditional written notice to A&M System at least ten days before the effective date of the cancellation. ***All insurance policies*** will be endorsed to require the insurance carrier providing coverage to send notice to A&M System ten (10) days prior to the effective date of cancellation, material change, or non-renewal relating to any insurance policy required in this Section.

Any deductible or self-insured retention must be declared to and approved by A&M System prior to the performance of any services by ASYSCO under this Agreement. ASYSCO is responsible to pay any deductible or self-insured retention for any loss. All deductibles and self-insured retentions will be shown on the Certificates of Insurance.

Certificates of Insurance and Additional Insured Endorsements as required by this Agreement will be mailed, faxed, or emailed to the following A&M System contact in Section 8.V.

The insurance coverage required by this Agreement will be kept in force until all services have been fully performed and accepted by A&M System in writing, except as may be noted.