MISSISSIPPI UNIVERSITY FOR WOMEN

Request for Proposals **(RFP#316006371)**

Oracle Cloud Implementation and Migration Services

ISSUE DATE: January 2, 2024

ISSUING AGENCY: Office of Resources Management

Mississippi University for Women 1100 College Street

Columbus, MS 39701

Sealed Proposals, subject to the conditions made a part hereof, will be received February 2, 2024 at 2:00 PM in the MUW Office of Resources Management, same address above, for furnishing services and potentially, optional services as described herein.

IMPORTANT NOTE: Indicate firm name, and RFP number on the front of each sealed proposal envelope or package.

All inquiries concerning this RFP should be directed to:

Melissa Buxton

Office of Resources Management (Same address above) [mcbuxton@muw.edu](mailto:mcbuxton@muw.edu)

1. Any addendum associated with this RFP will be posted at [<https://www.muw.edu/resources/purchasing/bids>](http://www.procurement.msstate.edu/procurement/bids/index.php) located under RFP
2. Note 2: It is the respondent’s responsibility to assure that all addenda have been reviewed and if applicable, signed and returned.
3. UNIVERSITY OVERVIEW

Mississippi University for Women (MUW) is a publicly supported institution of higher education and is accredited by the Commission on Colleges of the Southern Association of Colleges and Schools to award bachelors, masters, and doctoral degrees. The University operates on the semester system with the fall semester beginning in August and ending before Christmas. The spring semester begins in January and ends in May. The total enrollment is over 2,300. The University offers undergraduate and graduate programs of study leading to degrees in the Colleges of Arts and Sciences, College of Professional Studies, College of Nursing and Health Sciences, and the School of Education.

Additional information about MUW can be found at our website www.muw.edu.

II. PURPOSE OF THE REQUEST FOR PROPOSAL

1. Statement of Need

Mississippi University for Women (MUW) is seeking proposals from qualified service providers capable of providing comprehensive migration and implementation services to ensure a seamless and secure transition of critical administrative application systems to the Oracle Cloud Infrastructure environment. The migration will include but is not be limited to the institution’s Ellucian Banner ERP and accompanying degree audit solution, Degree Works. MUW expects the selected vendor to assist in the build out of the compute, virtual network, databases, disaster recovery, and the appropriate security measures.

The key benefits the University anticipates from such a service include:

**Cost Savings:**

Reduced Capital Expenses: Cloud computing eliminates the need for significant upfront investments in hardware, data centers, and infrastructure. Cloud services are paid for on a consumption-based model, which often leads to cost savings, and provides the advantage of instant scalability on an as need basis.

**Reliability and Availability:**

High Availability: Oracle Cloud offers high availability and redundancy, reducing the risk of downtime. Multiple availability zones and regions can be chosen to enhance the resilience of our systems.

Disaster Recovery: Oracle Cloud provides disaster recovery solutions, making it easier to implement and maintain disaster recovery plans.

**Security:**

Built-in Security: OCI includes robust security features, such as encryption, identity and access management, and network security, which can help protect your data and applications.

Compliance: Oracle Cloud meets various industry-specific compliance standards and regulations, which can simplify compliance efforts for your organization.

**Automation and Management:**

Automation Tools: OCI provides tools for automating infrastructure provisioning, management, and scaling, which can reduce administrative overhead.

Monitoring and Analytics: You can utilize built-in monitoring and analytics tools to gain insights into the performance and health of your systems.

By migrating to the Oracle Cloud, Mississippi University for Women will be taking another step towards future-proofing University administrative system technologies, that will provide access to the latest Oracle features, functionality, and tools in securing student, staff and faculty data, and improving efficiency of the University as a whole.

1. Service/Product Requested

Mississippi University for Women is seeking proposals from qualified service providers for the migration of on-premise Oracle databases and Tomcat applications to the Oracle Cloud Infrastructure (OCI). The purpose of this RFP is to identify a vendor capable of providing comprehensive migration services to ensure a seamless and secure transition of critical systems to the cloud environment.:

* Oracle Tenancy Subscription
* Oracle Database installation/migration
* Oracle Virtual Cloud Network
* APEX Installation / Migration
* Ellucian Banner Migration
* Degree Works Migration
* Ellucian Ethos
* Ellucian Service Systems
* OCI Security and Governance
* OCI Backup and Disaster Recovery

1. Assets for Migration (Current virtual machines, not limited to)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Quantity** | **Server type** | **Server Description** | **Environment** | **OS** |
| 2 | DB | Oracle DB Banner/DegreeWorks | Prod | Linux |
| 2 | DB | Oracle DB Banner/DegreeWorks | Test | Linux |
| 1 | JOBSUB | Source Code | Prod | Linux |
| 1 | JOBSUB | Source Code | Test | Linux |
| 7 | TOMCAT | Applications - Banner | Prod | Linux |
| 4 | TOMCAT | Applications - Banner | Test | Linux |
| 1 | TOMCAT | Ethos Identity | Prod | Linux |
| 1 | TOMCAT | Ethos API | Test | Linux |
| 1 | TOMCAT | Ethos API | Prod | Linux |
| 1 | DegreeWorks | Applications | Prod | Linux |
| 1 | DegreeWorks | Applications | Test | Linux |
| 1 | Proxy (HTTPD) | Web | Prod | Linux |
| 1 | TOMCAT | Ellucian Solution Manager (ESM) | Prod/Test | Linux |
| 1 | TOMCAT | QuickLaunch Middleware/Portal | Prod | Linux |
| 1 | TOMCAT | Oracle REST Data Services | Prod | Linux |
| 1 | TOMCAT | Third-Party Integrations/Data Transfers | Prod | Linux |

* INQUIRIES ABOUT RFP
  1. Bidders are not permitted to communicate with University staff regarding this solicitation during the time period between the Request for Proposal issue date and the announcements of awards, except during:
* Prospective respondents may make written inquiries concerning this request for proposal during the “Questions from Vendor” timeframe to obtain clarification of requirements and only to Melissa Buxton via electronic email at mcbuxton@muw.edu. Responses to these inquiries may be made by addendum to the Request for Proposal (RFP). All inquiries should be marked

**“URGENT INQUIRY. MUW RFP** #**316006371**

* Oral presentations or demonstrations, if conducted
* ADDENDUM OR SUPPLEMENT TO RFP
  1. In the event it becomes necessary to revise any part of this RFP, an addendum to this RFP will be provided to each respondent who received the original RFP. Respondents shall not rely on any other interpretations, changes or corrections.

III. ADMINISTRATIVE INFORMATION

1. Due Date – **February 2, 2024**

All materials must be submitted to:

Resources Management

Mississippi University for Women

1100 College Street

Columbus, MS 39701

1. Schedule of Critical Dates

The following dates are for planning purposes only unless otherwise stated in this RFP progress towards their completion is at the sole discretion of the university.

|  |  |
| --- | --- |
| RFP Posted | January 8, 2024 |
| Questions from Vendors Deadline | January 19, 2024 |
| MUW Q&A Response Deadline | January 26, 2024 |
| Proposal Submission Deadline – 2:00 p.m. CST | February 2, 2024 |
| Evaluation Period | February 5– February 16, 2024 |
| Presentations – Full day 2-3 vendors | February 13, 2024 |
| Notification of Intent to Award | February 26, 2024 |
| Board Approval | March 21, 2024 |
| Contract Effective Date (Estimated) | April 1, 2024 |

The proposal package must be received on or before **2:00 p.m. on February 2, 2024**. It is the responsibility of the respondent to ensure that the proposal package arrives in the Resources Management office on-time. The proposal package should be delivered or sent by mail to:

Resources Management

Mississippi University for Women

1100 College Street

Columbus, MS 39701

Your response must include the signature page included in this RFP (See Appendix A) and contain the signature of an authorized representative of the respondent’s organization. The signature on the “Original” signature page should be in blue ink

MUW reserves the right to reject any and all proposals and to waive informalities and minor irregularities in proposals received and to accept any portion of a proposal or all items bid if deemed in the best interest of the University to do so.

Proposals received after the stated due date and time will be returned unopened. Submission via facsimile or other electronic means will not be accepted.

1. PROPOSAL SUBMISSION

All proposals must be submitted physically. MUW requests ONE (1) original proposal and FOUR (4) copies in addition to ONE (1) thumb drive / electronic copy to be included. All packages must be clearly marked on the outside with “**RFP#316006371**” and the Proposer’s name and address.

Award of the contract resulting from this RFP will be based upon requirements set forth in this RFP. Selection of vendor(s) will be at the discretion of the University and will be based on the proposal that the University deems to be the most responsive and serves the bests interests of the University in terms of:

* Cost
* Functionality
* Vendor stability
* Vendor ability to meet the schedule of events, timeframe and references

At a minimum, the following items should be included in the contents of the Technical Proposal:

1. COVER LETTER, indicating the scope of the proposal. The letter should include an overview of the services being offered. The letter should include a statement of exceptions to any of the terms and conditions outlined in this RFP. (Cover letter should be no more than 3 pages in length.)
2. CORPORATE STRUCTURE AND CREDENTIALS
   * 1. Number of years of experience
     2. Staffing levels and support proposed
     3. Examples of three previous Ellucian Banner migrations
     4. (3) References from Ellucian Banner Institutions that vendor has migrated
3. SCOPE, APPROACH, AND METHODOLOGY

This section should include a description of each major type of work being requested of the Vendor. The proposal should reflect each of the sections listed:

* Hardware and software requirements (if applicable)
* Alliance/partnerships, if applicable, with other Vendors
* Project implementation plan with timeline
* Hosting/Tenancy information
* Information on where documents will be stored and security precautions
* Define level and availability of customer service
* Past / future schedule of updates
* Downtime information for updates
* Limitations of number of documents that can be stored
* List of available training
* Tools to monitor integrity of document repository

1. PROJECT REQUIREMENTS

This section identifies key functional requirements and expectations for given migration to be detailed in the vendor’s response. This list should not be viewed as all-inclusive and the RFP decision may include criteria not explicitly defined in this section.

Please provide documentation on how your proposed solution meets the following needs:

**Assessment and Planning:**

* Conduct a detailed assessment of the existing on-premise Oracle databases and Tomcat applications.
* Develop a comprehensive migration strategy and roadmap, outlining the scope, timeline, resources, and dependencies.
* Identify potential risks and mitigation strategies associated with the migration process.

**Migration Execution:**

* Set up the necessary OCI resources and networking configurations to support the migrated systems.
* Migrate Oracle databases to OCI, ensuring data integrity, security, and minimal downtime.
* Migrate Tomcat applications to OCI, optimizing performance and ensuring compatibility with the new environment.
* Conduct thorough testing and validation of the migrated systems to ensure functionality and performance meet or exceed on-premise benchmarks.

**Security and Compliance:**

* + Implement security best practices, including encryption, access controls, and monitoring, to ensure data protection in the cloud environment.
  + Ensure compliance with relevant data protection regulations and industry standards during and after migration.

**Documentation and Knowledge Transfer:**

* Provide detailed documentation of the migration process, configurations, and setup instructions.
* Conduct knowledge transfer sessions for the Client's IT team to facilitate the ongoing management and maintenance of the migrated systems.

**Post-Migration Support:**

* + Provide post-migration support and troubleshooting assistance to address any issues that may arise after the migration.

1. SECURITY AND COMPLIANCE
2. Provide a statement stating whether your company is compliant with FERPA and/or GLBA requirements.
3. Provide a completed Higher Education Cloud Vendor Assessment Tool (HECVAT) (lite version available at: <https://www.ren-isac.net/public-resources/hecvat.html>).
4. Provide proof of ISO/IEC 27001:2013 Certification for an information security management system (SMS).
5. Vendor should possess the following specializations from Oracle:
   * + Oracle Cloud Platform Data Management
     + Oracle Cloud Platform Integration
     + Oracle Cloud Platform Security
6. COST PROPOSAL
   * 1. Fees for initial purchase of required hardware or software (including all preparation, installation, rollout, training and first year maintenance and support)
     2. Required Annual Maintenance Costs after initial purchase. This includes software, hardware, transaction fees, etc.
     3. Optional fee schedule
   1. The proposal package must be received on or before **2:00 p.m. on February 2, 2024**. It is the responsibility of the respondent to ensure that the proposal package arrives in the Resources Management office on-time. The proposal package should be delivered or sent by mail to:

Resources Management

Mississippi University for Women

1100 College Street, W-Box 1628

Columbus, MS 39701

* 1. Your response must include the signature page included in this RFP (See Appendix A) and contain the signature of an authorized representative of the respondent’s organization. The signature on the “Original” signature page should be in blue ink
  2. MUW reserves the right to reject any and all proposals and to waive informalities and minor irregularities in proposals received and to accept any portion of a proposal or all items bid if deemed in the best interest of the University to do so.
  3. **Proposals received after the stated due date and time will be returned unopened. Submission via facsimile or other electronic means will not be accepted.**

1. DISCUSSIONS/EVALUATION CRITERIA/AWARD PROCESS
   1. MUW reserves the right to conduct discussions with any or all respondents, or to make an award of a contract without such discussions based only on evaluation of the written proposals. MUW reserves the right to contact and interview anyone connected with any past or present projects with which the respondent has been associated. MUW likewise reserves the right to designate a review committee to evaluate the proposals according to the criteria set forth under this section. MUW may make a written determination showing the basis upon which the award was made and such determination shall be included in the procurement file.
   2. MUW reserves the right to award this contract in whole or in part depending on what is in the best interest of MUW with MUW being the sole judge thereof.
   3. The evaluation factors set forth in this section are described as follows:
      1. The Vendor’s ability to perform the migration meeting the overall objective and services described in the RFP
      2. Vendor’s partnership with Oracle
      3. Competitive fees
      4. Availability and access to technical support
      5. Vendor’s experience providing OCI migrations for other institutions of higher education
      6. Compliance with applicable State and Federal laws and regulations
   4. The committee may invite finalists for interviews and/or presentations
   5. Failure to attend a requested interview presentation before the committee may result in a proposal not being considered.
   6. Upon award of contract(s), successful respondent(s) will be asked to provide an implementation plan and timeline and obtain MUW’s input and concurrence before moving forward.
   7. Proposals will be scored based on the following weights (100 points total):

Corporate Structure/Years of Experience/References – 20 pts Operation Plan/Ease of Use/Services Offered – 30 pts

Fees and other Projected Financial Impact to MUW 50 pts.

1. TWO-PHASE, BEST AND FINAL OFFER
   1. If the initial proposals do not provide MUW with a clear and convincing solution, or if MUW feels it is appropriate to offer the potential providers an opportunity to submit revised proposals, MUW reserves the right to use a two-phase approach and/or invite Best and Final Offers (BAFO). Based on the information obtained through the proposal submittals (Phase-One), MUW may choose a specific business model, and potential providers may be asked to submit revised proposals based upon that specific model.
   2. The evaluation committee may develop, for distribution to the top-ranked firms, refined written terms with specific information on what is being requested as a result of information obtained through initial RFP submittal process. Proposers may be asked to reduce cost or provide additional clarification to specific sections of the RFP. Selected proposers are not required to submit a BAFO and may submit a written response notifying the solicitation evaluation committee that their response remains as originally submitted.
2. TERM OF CONTRACT
   1. It is MUW’s intention to enter into a five (5) year contract beginning upon receipt of all required approvals (estimated April 1, 2024).
   2. MUW reserves the right to terminate this agreement with thirty (30) days’ notice, by the Director of Resources Management via certified mail to the address listed on the signature page of this RFP (See Appendix A) if any of the terms of the proposal and/or contract are violated.
   3. In the event the contractor fails to carry out and comply with any of the conditions and agreements to be performed under the specifications, MUW will notify the contractor, in writing, of such failure or default. In the event the necessary corrective action has not been completed within a ten (10) day period, the contractor must submit, in writing, why such corrective action has not been performed. The University reserves the right to determine whether or not such noncompliance may be construed as a failure of performance of the contractor.
   4. Termination of contract by contractor without cause can only occur with at least one- hundred and twenty (120) days’ notice prior to the proposed termination of the contract.
   5. In the event MUW employs attorneys or incurs other expenses it considers necessary to protect or enforce its rights under this contract, the contractor agrees to pay the attorney’s fees and expenses so incurred by MUW.
3. ACCEPTANCE TIME
   1. Proposal shall be valid for one-hundred and eighty (180) days following the proposal due date.
4. RFP CANCELLATION
   1. This RFP in no manner obligates MUW to the eventual purchase of any services described, implied or which may be proposed until confirmed by a written contract. Progress towards this end is solely at the discretion of MUW and may be terminated without penalty or obligations at any time prior to the signing of a contract. MUW reserves the right to cancel this RFP at any time, for any reason, and to reject any or all proposals or any parts thereof.
5. INDEPENDENT CONTRACTOR CLAUSE
   1. The contractor shall acknowledge that an independent contractor relationship is established and that the employees of the contractor are not, nor shall they be deemed employees of MUW and that employees of MUW are not, nor shall they be deemed employees of the contractor.
6. OTHER CONTRACT REQUIREMENTS
   1. Award Terms: This contract shall be awarded at the discretion of the University based on the capabilities and overall reputation of the Supplier, as well as the cost. Acceptance shall be confirmed by the issuance of a contract from the University.
   2. University Addendum: The awarded contractor(s) will be expected to enter into a contract that is in substantial compliance with MUW adhering to the State of Mississippi laws and regulations. See Appendix B.
   3. Information Security: The contract must include the Information Security provision outlined in Appendix C
   4. Piggy Back Clause: The state requests the right to use the results of this RFP in future projects. Please see Appendix D for contract language to include.
   5. The Procurement Process: The following is a general description of the process by which a firm will be selected to fulfill this Request for Proposal.
      1. Request for Proposals (RFP) is issued to prospective suppliers.
      2. A deadline for written questions is set.
      3. Proposals will be received as set forth in Section III.
      4. Unsigned proposals will not be considered (APPENDIX A).
      5. All proposals must be received by MUW no later than the date and time specified on the cover sheet of this RFP.
      6. At that date and time, the package containing the proposals from each responding firm will be opened publicly and the name of each respondent will be announced.
      7. Proposal evaluation: The University will review each proposal.
      8. At their option, the evaluators may request oral presentations or discussions for the purpose of clarification or to amplify the materials presented in the proposal
      9. Respondents are cautioned that this is a request for proposals, not a request to contract, and the MUW reserves the unqualified right to reject any and all proposals when such rejection is deemed to be in the best interest of the University.
      10. The proposals will be evaluated according to the criteria set forth in Section V.

**APPENDIX A: SIGNATURE PAGE**

**Provide information requested, affix signature and return this page with your proposal: NAME OF FIRM: COMPLETE ADDRESS:**

**TELEPHONE NUMBER:**

**AREA CODE/NUMBER**

**FACSIMILE NUMBER: \_**

**AREA CODE/NUMBER**

**E-MAIL ADDRESS:**

**AUTHORIZED**

**SIGNATURE: PRINTED NAME: TITLE:**

**APPENDIX B: UNIVERSITY ADDENDUM**

MANDATORY ADDENDUM TO

ALL MISSISSIPPI UNIVERSITY FOR WOMEN CONTRACTS

January 2019 Edition

Notwithstanding any provision to the contrary contained in any contract in which Mississippi University for Women (MUW) is a party, MUW does not waive any rights, benefits or prohibitions that may be provided under any applicable law. Every provision to the contrary in any contract to which MUW is a party is void and deleted. The following is a non-exhaustive list of provisions that shall be exceptions to any contrary provision in any contract to which MUW is a party:

1. MUW does not indemnify or hold harmless any party.

1. MUW does not make any warranty.

1. MUW does not waive any claim, present, past or future.

1. MUW does not waive its sovereign immunity. Mississippi University for Women shall only be responsible for liability resulting from the actions/inactions of its officers, agents, and employees acting within the course and scope of their official duties.

1. MUW does not waive its Eleventh Amendment immunity under the United States Constitution.

1. The law applicable to this contract shall be the laws of the State of Mississippi. The choice of law doctrine shall not be used to apply the laws of another state. The forum through which to attempt to pursue claims arising under this contract is the State of Mississippi state court system and no other.

1. Contractual provisions for actions or results that are inconsistent with or in violation of the policies of Mississippi University for Women or the State of Mississippi Board of Trustees of State Institutions of Higher Learning, or both, are deleted.

1. MUW does not agree to a factual description of the current interpretation of the law.

1. MUW does not assign its interest in penalties, such as liquidated damages, to the non-MUW party.

1. MUW does not limit the liability of a non-MUW party for negligence or intentional or reckless torts.

1. MUW does not limit the liability of any non-MUW party to the amount of the contract or to any other set amount.

1. MUW does not exclude any non-MUW party's warranties of merchantability and fitness for a particular use or any common law warranties to which MUW is entitled.

1. MUW does not waive any type or category of damages.

1. MUW does not agree that another party may prosecute or defend legal actions in the name of MUW

unless the provision also conditions the prosecution of such actions on receipt by the party desiring to proceed in the name of MUW with the requirement that such authority may only be allowed if the advance, written approval of the Attorney General of the State of Mississippi is obtained on a case-by case basis.

1. MUW does not agree to pay extra compensation, fees, or allowances after service is rendered or a contract made, or for any payment not authorized by law.

1. MUW does not agree to any provisions in which the credit of the State of Mississippi is pledged or loaned in aid of any person, association, or corporation.

1. Provisions that limit the time frame for MUW to pursue legal actions are deleted.

1. MUW does not agree to submit to binding arbitration.

1. MUW does not agree to pay any party any amount as compensation for MUW employing the other

party’s employees.

1. MUW will make payments for all amounts owed under this agreement no later than forty-five (45) days after receipt of the invoice and receipt, inspection and approval of the goods or services in accordance with Miss. Code Ann. § 31-7-305.
2. The contracting parties are on notice that MUW is a public entity of the State of Mississippi and that all parties that wish to conduct business with MUW are obligated to verify through their own legal counsel, not through MUW officials, and through public laws and regulations whether MUW has the authority to enter such a contract, whether the provisions of the contract are enforceable as to MUW, and whether the MUW official executing the contract has the authority so to do.
3. The contracting parties are on notice that MUW is subject to the Mississippi Public Records Act, Miss. Code Ann. § 25-6-1, *et seq*. No party to this agreement shall be liable to the other party for disclosures of information required by court order or required by law.
4. It is expressly understood and agreed that the obligation of MUW to proceed under this agreement is conditioned upon the availability and receipt of funds by MUW to specifically perform the obligations set forth for MUW under the agreement.
5. In compliance with the Mississippi Transparency and Accountability Act, all payments made by MUW may be posted on a public website beginning on July 1, 2012. The information posted will include the date of payment, vendor name, vendor's city and state, and the payment amount. The release of this information supersedes any applicable non-disclosure or confidentiality obligations of MUW.

1. Any Contractor/Seller of MUW shall ensure compliance with the Mississippi Employment Protection Act, Miss. Code Ann. § 71-11-1, *et seq.* to -3, and shall register and participate in the status verification system for all newly hired employees. The term “employee” as used herein means any person that is hired to perform work within the State of Mississippi. As used herein, “status verification system” means the Illegal Immigration Reform and Immigration Responsibility Act of 1996 that is operated by the United States Department of Homeland Security, also known as the E-Verify Program, or any other successor electronic verification system replacing the E-Verify Program. Contractor/Seller shall maintain records of such compliance and, upon request of the State and approval of the Social Security Administration or Department of Homeland Security, where required, to provide a copy of each such verification to the State. Any person assigned by a Contractor/Seller to perform services for MUW shall meet the employment eligibility requirements of all immigration laws of the State of Mississippi. Any breach of these warranties may subject Contractor/Seller to the following: (a) termination of this Agreement and ineligibility for any state or public contract in Mississippi for up to three years, with notice of such cancellation/termination being made public, or (b) the loss of any license, permit, certification or other document granted to Contractor/Seller by an agency, department or governmental entity for the right to do business in Mississippi for up to one year, or (c) both. In the event of termination/cancellation, Contractor/Seller may also be liable for any additional costs incurred by MUW or the State due to contract cancellation or loss of license or permit.

1. Contractor recognizes that MUW, as a state agency of the State of Mississippi, enters into a contract only to the extent authorized by Mississippi law, including the opinions of the Mississippi Attorney General. Any provision of a contract that is not authorized or inconsistent with Mississippi law, including the opinions of the Mississippi Attorney General, is deleted.

1. This Addendum complies with the provision that amendments to the contract must be in writing and approved by both parties, and the Addendum is expressly incorporated in the contract.

|  |  |
| --- | --- |
| Agreed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Name      \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Title    On behalf of Mississippi University for Women: | Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Agreed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Name | Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

# Vice President for Administration/Chief Financial Officer

Title

**APPENDIX C: INFORMATION SECURITY PROVISION**

**Information Security**. Vendor shall be responsible for establishing and maintaining an information security program that is designed to (i) ensure the security and confidentiality of data transmitted by UNIVERSITY to Vendor or data otherwise obtained by Vendor from or about UNIVERSITY (“UNIVERSITY Data”), (ii) protect against any anticipated threats or hazards to the security or integrity of UNIVERSITY Data, and (iii) protect against unauthorized access to or use of UNIVERSITY Data that could result in substantial harm or inconvenience to UNIVERSITY or any of its stakeholders.   Vendor shall establish, employ and at all times maintain physical, technical and administrative security safeguards and procedures sufficient to prevent any unauthorized processing of and/or use, access, alteration, disclosure, erasure, copying, exhibition, transmission, or destruction of UNIVERSITY Data while such information is in Vendor’s possession or control and will ensure that such information is not processed in other ways contradictory to privacy and/or data protection laws.  Vendor will maintain sufficient procedures to detect and respond to security breaches involving UNIVERSITY Data and will inform UNIVERSITY immediately when it suspects or learns of malicious activity involving UNIVERSITY Data, including an estimate of the activity’s effect on UNIVERSITY and the corrective action taken. Such procedures shall include, but not be limited to, logging of all access to confidential or sensitive data, use of firewalls for all external data connections, and timely implementation of updates and patches.

At a minimum, Vendor’s safeguards for the protection of UNIVERSITY Data shall include: (i) limiting access to UNIVERSITY Data to authorized personnel of Vendor and utilizing policies that promote the least internal access; (ii) securing business facilities, data centers, paper files, servers, back-up systems (at a strategically located off-site location) and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability; (iii) implementing network, device application, database and platform security; (iv) securing information transmission, storage and disposal; (v) implementing authentication (two-factor or more secure method) and access controls within media, applications, operating systems and equipment; (vi) encrypting (with AES-256 bit or better encryption) UNIVERSITY data stored on any mobile media; (vii) encrypting UNIVERSITY Data transmitted over public or wireless networks; (viii) strictly segregating UNIVERSITY Data from information of Vendor or its other customers so that UNIVERSITY Data is not commingled with any other types of information; (ix)  implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law; and (x) providing appropriate privacy and information security training to Vendor’s employees.

Vendor must obtain the written approval of UNIVERSITY before subcontracting any portion of this Agreement. All subcontracts shall incorporate the terms of this Agreement so as to require subcontractors to meet or exceed the Vendor’s security obligations, including all data security requirements.

**APPENDIX D: PIGGY BACK CLAUSE FOR CONTRACT**

***Right to Use Proposals in Future Projects***

The State reserves the right to evaluate the awarded proposal from this RFP, including all products and services proposed therein, along with the resulting contractual terms, for possible use in future projects if (a) it is deemed to be in the best interest of the State to do so; and (b) the Vendor is willing to extend a cost less than or equal to that specified in the awarded proposal and resulting contract.  A decision concerning the utilization of a vendor’s proposal for future projects is solely at the discretion of the State and requires the agreement of the proposing Vendor.  The State’s decision to reuse an awarded proposal will be based upon such criteria as:  (1) the customer’s business requirements; (2) elapsed time since the award of the original project; and/or (3) research on changes in the Vendor, market, and technical environments since the initial award.

**APPENDIX E: ENTERPRISE CLOUD AND OFFSITE HOSTING SECURITY POLICY**

**Mississippi Department of Information Technology Services**

**Security Services Division**

**State of Mississippi Enterprise Cloud and Offsite Hosting Security Policy**

**Title 36: Technology**

**Part 3: Enterprise Cloud and Offsite Hosting Security Policy**

**Part 3 Chapter 1: General Policy**

*Rule 1.1 Purpose*

This document formally promulgates the State of Mississippi Enterprise Cloud and Offsite Hosting Security Policy. The goal of this policy is to improve the security posture of the State by establishing minimum security requirements that all agencies will adhere to, for the utilization of offsite hosting facilities including cloud computing.

Source: *Miss. Code Ann.* § *25-53-201.*

*Rule 1.2 Authority*

To fulfill the statutory requirements for cybersecurity, the State of Mississippi will have a comprehensive cybersecurity program (the Enterprise Security Program) to provide coordinated oversight of the cybersecurity efforts across all state agencies, including cybersecurity systems, services and development of policies, standards and guidelines.

The Mississippi Department of Information Technology Services (ITS) administers the Enterprise Security Program to execute the duties and responsibilities of the cybersecurity program.

Source: *Miss. Code Ann.* § *25-53-201.*

*Rule 1.3 Scope*

This policy applies to all state agencies; State of Mississippi employees; trusted partners; or any entity, as provided by law, authorized to operate, manage, or use State of Mississippi information and information technology (IT) systems (hereafter referred to collectively as “SOM Assets”). Agency is defined as and includes all the various state agencies, officers, departments, boards, commissions, offices, and institutions of the state (§ 25-53-3 (2)(e)).

A. This policy includes a subset of technical requirements that are only applicable to agencies participating in the Enterprise State Network. Agencies that do not participate in the Enterprise State Network, and thus do not have the benefit of the technical controls in place, must develop agency-specific security policies that are:

1. Appropriate to their respective environments, and

2. Consistent with the intent of this policy.

B. This policy addresses information regardless of what form it takes (i.e., electronic, printed, etc.), what technology is used to handle it, or what purpose(s) it serves.

C. This policy encompasses systems, automated and manual for which the agencies have administrative responsibility, including systems managed or hosted by third parties on behalf of the agencies.

Source: Miss. Code Ann. § 25-53-201.

*Rule 1.4 Cloud and Offsite Hosting Contracts and Amendments*

Each agency must ensure that new contracts and amendments include the terms and conditions approved by ITS.

A. Contracts already in force will be expected to include the terms and conditions approved by ITS at the time of next renewal, modification, or renegotiation.

B. The terms and conditions clauses are mandatory for every engagement and exceptions will be considered non-compliant. Agencies can view the mandatory terms and conditions on the ITS website.

Source: Miss. Code Ann. § 25-53-201.

*Rule 1.5 Cloud and Offsite Hosting Security*

Each agency must ensure the implementation of reasonable measures to preserve the confidentiality, integrity, and availability of State of Mississippi information and information technology (IT) systems (hereafter referred to collectively as “SOM Assets”) from unauthorized use, access, disclosure, modification, or destruction. For any measure that the agency cannot directly implement due to the SOM Asset being managed by another organization, contractor, or other source, the agency must implement periodic verification/audit to ensure that the measure is properly implemented.

A. Each agency must ensure adherence to all applicable security requirements established by the State of Mississippi Enterprise Security Policy.

1. Each agency must ensure adherence to the baseline security controls for Cloud and Offsite Hosting implementations. The baseline security controls can be found on the ITS website.

B. Each agency must adhere to the following for all assets encrypted at rest.

1. Evaluate the risks with available key location and key management implementations and select the implementation that adequately protects the data;

2. Implement security controls to reduce and mitigate risks when encryption of data at rest is not possible; and

3. Secure and maintain adequate liability coverage when encryption of data at rest is not possible.

Source: Miss. Code Ann. § 25-53-201.

*Rule 1.6 Policy Application*

Each agency must adhere to all requirements in this policy.

A. Each agency shall adhere to the more restrictive policy when conflicts exist between this policy and agency policies.

B. Each agency shall determine the level of compliance with this policy and confirm in writing their compliance level in accordance with compliance reporting requirements of the State of Mississippi Enterprise Security Policy.

1. Documentation must include details of where compliance with the requirements of this policy is not met and plans for mitigating the deficiencies.

Source: Miss. Code Ann. § 25-53-201.

*Rule 1.7 Maintenance of the State of Mississippi Cloud and Offsite Hosting Security Policy*

The revision date for this policy is July 1, 2018.

A. ITS is responsible for routine maintenance and review of this policy. Routine maintenance and review are required to ensure that this policy is up-to-date with respect to the technological advances and changes in the business requirements of state agencies, potential threats, applicable legislation and other changes that impact information security policies, standards, guidelines and recommendations. A detailed description of the policy and standards review process is included in the Enterprise Security Program document. The Program document is available on the ITS website.

Source: Miss. Code Ann. § 25-53-201.

*Rule 1.8 Exceptions to the State of Mississippi Cloud and Offsite Hosting Security Policy, Standards, Guidelines and Recommendations*

A. The only permitted exceptions to the State of Mississippi Cloud and Offsite Hosting Security Policy are those that are approved in writing by ITS for an agency’s specific purpose and are only applicable to that agency’s operations for the duration of time defined by the exception. A detailed description of the policy and standards exception process is included in the Enterprise Security Program document. The Program document is available on the ITS website.

B. Each agency must inquire with the vendor and appropriate agency staff to ascertain if design alternatives, configuration changes, or additional products or services are available to attain compliance prior to submitting a request for an exception.

C. Prior to selecting and procuring information technology products and services, each agency must consider all enterprise policies and standards when specifying, scoping, and evaluating solutions to meet current and planned requirements.

Source: Miss. Code Ann. § 25-53-201.

**APPENDIX F: NON-PUBLIC DATA OWNED BY THE STATE OF MISSISSIPPI**

Per rule 1.4 of the State of Mississippi Enterprise Cloud and Offsite Hosting Security Policy, each agency must ensure that new contracts and amendments include the terms and conditions approved by ITS. The terms and conditions provided below are applicable for State of Mississippi data that the agency has categorized as ***non-public*** data.

**Data Ownership:** The State of Mississippi (“State”) shall own all right, title and interest in all data used by, resulting from, and collected using the services provided. The Service Provider shall not access State User accounts, or State Data, except (i) in the course of data center operation related to this solution; (ii) response to service or technical issues; (iii) as required by the express terms of this service; or (iv) at State ’s written request.

**Data Protection:** Protection of personal privacy and sensitive data shall be an integral part of the business activities of the Service Provider to ensure that there is no inappropriate or unauthorized use of State information at any time. To this end, the Service Provider shall safeguard the confidentiality, integrity, and availability of State information and comply with the following conditions:

a) All information obtained by the Service Provider under this contract shall become and remain property of the State.

b) At no time shall any data or processes which either belongs to or are intended for the use of State or its officers, agents, or employees be copied, disclosed, or retained by the Service Provider or any party related to the Service Provider for subsequent use in any transaction that does not include the State.

**Data Location:** The Service Provider shall not store or transfer State data outside of the United States. This includes backup data and Disaster Recovery locations. The Service Provider will permit its personnel and contractors to access State data remotely only as required to provide technical support.

**Encryption:**

a) The Service Provider shall encrypt all non-public data in transit regardless of the transit mechanism.

b) For engagements where the Service Provider stores non-public data, the data shall be

**encrypted at rest**. The key location and other key management details will be discussed and negotiated by both parties. Where encryption of data at rest is not possible, the Service Provider must describe existing security measures that provide a similar level of protection. Additionally, when the Service Provider cannot offer encryption at rest, it must maintain, for the duration of the contract, cyber security liability insurance coverage for any loss resulting from a data breach. The policy shall comply with the following requirements:

* + - The policy shall be issued by an insurance company acceptable to the State and valid for the entire term of the contract, inclusive of any term extension(s).
    - The Service Provider and the State shall reach agreement on the level of liability insurance coverage required.
    - The policy shall include, but not be limited to, coverage for liabilities arising out of premises, operations, independent contractors, products, completed operations, and liability assumed under an insured contract.
    - At a minimum, the policy shall include third party coverage for credit monitoring. notification costs to data breach victims; and regulatory penalties and fines.
    - The policy shall apply separately to each insured against whom claim is made or suit is brought subject to the Service Provider’s limit of liability.
    - The policy shall include a provision requiring that the policy cannot be cancelled without thirty (30) days written notice.
    - The Service Provider shall be responsible for any deductible or self-insured retention contained in the insurance policy.
    - The coverage under the policy shall be primary and not in excess to any other insurance carried by the Service Provider.
    - In the event the Service Provider fails to keep in effect at all times the insurance coverage required by this provision, the State may, in addition to any other remedies it may have, terminate the contract upon the occurrence of such event, subject to the provisions of the contract.

**Breach Notification and Recovery:** Unauthorized access or disclosure of non-public data is considered to be a security breach. The Service Provider will provide immediate notification and all communication shall be coordinated with the State. When the Service Provider or their sub-contractors are liable for the loss, the Service Provider shall bear all costs associated with the investigation, response and recovery from the breach including but not limited to credit monitoring services with a term of at least 3 years, mailing costs, website, and toll-free telephone call center services. The State shall not agree to any limitation on liability that relieves a Contractor from its own negligence or to the extent that it creates an obligation on the part of the State to hold a Contractor harmless.

**Notification of Legal Requests:** The Service Provider shall contact the State upon receipt of any electronic discovery, litigation holds, discovery searches, and expert testimonies related to, or which in any way might reasonably require access to the data of the State. The Service Provider shall not respond to subpoenas, service of process, and other legal requests related to the State without first notifying the State unless prohibited by law from providing such notice.

**Termination and Suspension of Service:** In the event of termination of the contract, the Service Provider shall implement an orderly return of State data in CSV or XML or another mutually agreeable format. The Service Provider shall guarantee the subsequent secure disposal of State data.

a) Suspension of services: During any period of suspension of this Agreement, for whatever reason, the Service Provider shall not take any action to intentionally erase any State data.

b) Termination of any services or agreement in entirety: In the event of termination of any services or of the agreement in its entirety, the Service Provider shall maintain the existing level of security as stipulated in the agreement and shall not take any action to intentionally erase any State data for a period of 90 days after the effective date of the termination. After such 90-day period, the Service Provider shall have no obligation to maintain or provide any State data and shall thereafter, unless legally prohibited, dispose of all State data in its systems or otherwise in its possession or under its control as specified in section 7(d) below. Within this 90-day timeframe, Service Provider will continue to secure and back up State data covered under the contract.

c) Post-Termination Assistance: The State shall be entitled to any post-termination assistance generally made available with respect to the Services unless a unique data retrieval arrangement has been established as part of the Service Level Agreement.

d) Secure Data Disposal: When requested by the State, the provider shall destroy all requested data in all of its forms, for example: disk, CD/DVD, backup tape, and paper. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST) approved methods. Certificates of destruction shall be provided to the State.

**Background Checks:** The Service Provider shall conduct criminal background checks and not utilize any staff, including sub-contractors, to fulfill the obligations of the contract who has been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or any misdemeanor offense for which incarceration for a minimum of one (1) year is an authorized penalty. The Service Provider shall promote and maintain an awareness of the importance of securing the State's information among the Service Provider's employees and agents.

**Security Logs and Reports:** The Service Provider shall allow the State access to system security logs that affect this engagement, its data, and/or processes. This includes the ability to request a report of the activities that a specific user or administrator accessed over a specified period of time as well as the ability for an agency customer to request reports of activities of a specific user associated with that agency.

* + These mechanisms should be defined up front and be available for the entire length of the agreement with the Service Provider.

**Contract Audit:** The Service Provider shall allow the State to audit conformance including contract terms, system security and data centers as appropriate. The State may perform this audit or contract with a third party at its discretion at the State’s expense.

**Sub-contractor Disclosure:** The Service Provider shall identify all of its strategic business partners related to services provided under this contract, including but not limited to, all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Service Provider, who will be involved in any application development and/or operations.

**Sub-contractor Compliance:** Service Provider must ensure that any agent, including a Service Provider or subcontractor, to whom the Service Provider provides access agrees to the same restrictions and conditions that apply through this Agreement.

**Processes and Procedures:** The Service Provider shall disclose its non-proprietary security processes and technical limitations to the State so that the State can determine if and how adequate protection and flexibility can be attained between the State and the Service Provider. For example: virus checking and port sniffing — the State and the Service Provider shall understand each other’s roles and responsibilities.

**Operational Metrics**: The Service Provider and the State shall reach agreement on operational metrics and document said metrics in the Service Level Agreement. At a minimum the SLA shall include:

a) Advance notice and change control for major upgrades and system changes

b) System availability/uptime guarantee/agreed-upon maintenance downtime

c) Recovery Time Objective/Recovery Point Objective

d) Security Vulnerability Scanning

**APPENDIX G:** **PUBLIC DATA OWNED BY THE STATE OF MISSISSIPPI**

Per rule 1.4 of the State of Mississippi Enterprise Cloud and Offsite Hosting Security Policy, each agency must ensure that new contracts and amendments include the terms and conditions approved by ITS. The terms and conditions provided below are applicable for State of Mississippi data that the agency has categorized as ***public*** data.

**Data Ownership:** The State of Mississippi (State) shall own all right, title and interest in all data used by, resulting from, and collected using the services provided. The Service Provider shall not access State User accounts, or State Data, except (i) in the course of data center operation related to this solution, (ii) response to service or technical issues, (iii) as required by the express terms of this service, or (iv) at State ’s written request.

**Data Protection:** Protection of personal privacy and sensitive data shall be an integral part of the business activities of the Vendor to ensure that there is no inappropriate or unauthorized use of State information at any time. To this end, the Vendor shall safeguard the confidentiality, integrity, and availability of State information and comply with the following conditions:

a) At no time shall any data or processes which either belong to or are intended for the use of State or its officers, agents, or employees be copied, disclosed, or retained by the Service Provider or any party related to the Service Provider for subsequent use in any transaction that does not include the State.

**Data Location:** The Service Provider shall not store or transfer State data outside of the United States. This includes backup data and Disaster Recovery locations. The Service Provider will permit its personnel and contractors to access State data remotely only as required to provide technical support.

**Notification of Legal Requests:** The Service Provider shall contact the State upon receipt of any electronic discovery, litigation holds, discovery searches, and expert testimonies related to, or which in any way might reasonably require access to the data of the State. The Service Provider shall not respond to subpoenas, service of process, or other legal requests related to the State without first notifying the State unless prohibited by law from providing such notice.

**Termination and Suspension of Service:** In the event of termination of the contract, the Service Provider shall implement an orderly return of State data in CSV or XML or another mutually agreeable format. The Service Provider shall guarantee the subsequent secure disposal of State data.

a) Suspension of services: During any period of suspension of this Agreement, for whatever reason, the Service Provider shall not take any action to intentionally erase any State data.

b) Termination of any services or agreement in entirety: In the event of termination of any services or agreement in entirety, the Service Provider shall maintain the existing level of security as stipulated in the agreement and shall not take any action to intentionally erase any State data for a period of 90 days after the effective date of the termination. After such 90-day period, the Service Provider shall have no obligation to maintain or provide any State data and shall thereafter, unless legally prohibited, dispose of all State data in its systems or otherwise in its possession or under its control as specified in section 7(d) below. Within this 90-day timeframe, vendor will continue to secure and back up State data covered under the contract.

c) Post-Termination Assistance: The State shall be entitled to any post-termination assistance generally made available with respect to the Services unless a unique data retrieval arrangement has been established as part of the Service Level Agreement.

**Background Checks:** The Service Provider shall conduct criminal background checks and not utilize any staff, including sub-contractors, to fulfill the obligations of the contract who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or any misdemeanor offense for which incarceration of a minimum of one (1) year is an authorized penalty. The Service Provider shall promote and maintain an awareness of the importance of securing the State's information among the Service Provider's employees and agents.

**Security Logs and Reports:** The Service Provider shall allow the State access to system security logs that affect this engagement, its data, and/or processes. This includes the ability to request a report of the activities that a specific user or administrator accessed over a specified period of time as well as the ability for an agency customer to request reports of activities of a specific user associated with that agency.

* + These mechanisms should be defined up front and be available for the entire length of the agreement with the Vendor.

**Contract Audit:** The Service Provider shall allow the State to audit conformance including contract terms, system security and data centers as appropriate. The State may perform this audit or contract with a third party at its discretion at the State’s expense.

**Sub-contractor Disclosure:** The Service Provider shall identify all of its strategic business partners related to services provided under this contract, including but not limited to, all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Service Provider, who will be involved in any application development and/or operations.

**Sub-contractor Compliance:** Vendor must ensure that any agent, including a vendor or subcontractor, to whom the Vendor provides access agrees to the same restrictions and conditions that apply through this Agreement.

**Processes and Procedures:** The Service Provider shall disclose its non-proprietary security processes and technical limitations to the State so that the State can determine if and how adequate protection and flexibility can be attained between the State and the vendor. For example: virus checking and port sniffing — the State and the vendor shall understand each other’s roles and responsibilities.

**Operational Metrics**: The Service Provider and the State shall reach agreement on operational metrics and document said metrics in the Service Level Agreement. Examples include but are not limited to:

a) Advance notice and change control for major upgrades and system changes

b) System availability/uptime guarantee/agreed-upon maintenance downtime

c) Recovery Time Objective/Recovery Point Objective

d) Security Vulnerability Scanning