JAMES MADISON UNIVERSITY

CONTRACT RENEWAL LETTER

Date:	April 02, 2019	
Contract #:	UCPJMU4135	
Service:	Information Technology Management System	
Renewal Period:	June 16, 2019 to June 15, 2020	
Renewal #:	2 of 7 One-Year	
Issued By:	James Madison University LeeAnne Beatty Smith, Buyer Senior	Ph: 540-568-7523
Contractor:	Avante Solutions Attn: Steven Waxler 738 W, Jackson Blvd, Chicago, IL 60661	Ph: 866-282-6831
Contract Administrator:	Robin Bryan, Information Technology	

Description of Renewal Notice:

In accordance with the renewal provision of the original contract all terms, conditions, and specifications of the original contract remain the same during the contract renewal period, along with any modifications that have been incorporated up until this point The contract pricing will increase by 1.4% in accordance with the CPI-W Other Services index of the US Bureau of Labor Statistics and is attached to this renewal.

The attached *James Madison University Information Technology Services Addendum* is hereby added to the above referenced contract.

All invoices shall be submitted within sixty days of contract renewal term expiration as well as for each subsequent contract renewal period. Any invoices submitted after the sixty day period will not be processed for payment.

Return one executed renewal notice to my attention within ten days.

Avante Solutions

By: _____

Steven Waxler

Name (print)

President — April 3, 2019

Title — *Date Signed*

James Madison University

By: _____

LeeAnne Beatty Smith, CPPB, VCA, CUPO

Name (print)

Buyer Senior — 4/2/19

Title — *Date Signed*

Contract #: UCPJMU4135
Contractor: Avante Solutions
Renewal Period: 6/16/2019 - 6/15/2020
Commodity: Information Technology Management System

Cherwell Service Management Licensing Pricing:

A. Perpetual/Purchased License Model Pricing:

Item	Unit Cost
Cherwell Service Management	$3,424.08/license for 1-24 concurrent licenses $2,861.91/license for 25-99 concurrent licenses $2,555.28/licenses for 100-199 concurrent licenses +199 concurrent licenses priced upon request
Annual Maintenance & Support	$613.27/license for 1-24 concurrent license(s) $511.06/license for 25-199 concurrent licenses +199 concurrent licenses priced upon request
If Cherwell hosts system, the following charges will be applicable:	
Annual Hosting Fee	$1,022.11/year for 1-49 license(s) $2,555.28/year for 50-199 licenses +199 licenses priced upon request
Annual VPN Fee- *(Optional but recommended)*	$3,066.34/year
The Cherwell license pricing is based on the number of licenses purchased and, after the initial purchase, the number of licenses currently owned. (Example: the purchase of 25 initial licenses would be $2861.91/per license. If 75 more licenses are purchased at a later date, the cost would be $2861.91/each for 74 of the licenses and 1 license at $2555.28). The same applies to Annual Maintenance and Support pricing.	

B. Subscription License Model Pricing:

Item	Unit Cost
Cherwell Service Management Subscription Fee *(monthly)*	$112.43/license for 1-24 concurrent licenses $97.10/license for 25-99 concurrent licenses $91.99/licenses for 100-199 concurrent licenses +199 concurrent licenses priced upon request
Annual Maintenance & Support	Included in Subscription Cost
Annual Hosting Fee	Included in Subscription Cost
Annual VPN Fee *(Optional and not applicable if installed on-premise)*	$3,066.34/year

Optional- Additional Hosted Non-production Environment *(one (1) included in subscription)*	$10,221.12
Subscription pricing is based on a one-year subscription term and shall be invoiced annually in advance of the subscription year.	

C. **Optional Discovery Tool Module**: asset scanning and discovery module that shall provide asset scanning and importing to the Cherwell CMDB.

1) Subscription Model pricing: $4,088.45/per year

2) Perpetual/Purchase Model pricing: $10,221.12 one-time cost plus additional $2,044.22 annual maintenance and support.

D. **Optional Reservation Manager Module**: comprehensive loan equipment management system that shall catalog, track, and manage the check-in and check-out of loan equipment.

1) One-time fee of $7,665.84 plus additional $766.58 annual maintenance and support for both licensing models.

E. **Avante Professional Services Pricing**:

1) Contractor shall invoice the Purchasing Agency monthly for actual time that work was performed by prorating the associated hourly rate (for example: 5.6 hours of work @$191.65/hour shall = $1073.24). The Purchasing Agency will not prepay for Professional Services.

2) The Professional Services rate for all work performed offsite at the Contractor's place(s) of business (not at the location of the Purchasing Agency) shall be invoiced at the hourly rate of $191.65 ($1533.20/per day).

3) The Professional Services rate for all work performed onsite at James Madison University (JMU) shall be invoiced at the hourly rate of $242.75 ($1942.01/per day). The onsite hourly rate shall include all travel and reimbursables to perform work on JMU campus.

4) Professional Services onsite hourly rates for Purchasing Agencies (other than JMU) accessing this contract cooperatively shall be negotiated and mutually agreed to in writing between the parties.

James Madison University
Information Technology Services Addendum

CONTRACTOR NAME: **Avante Solutions**

PRODUCT/SOLUTION: **Information Technology Management System**

Definitions:

- Agreement: The "Agreement" includes the contract, this addendum and any additional addenda and attachments to the contract, including the Contractor's Form.
- University: "University" or "the University" means James Madison University, its trustees, officers and employees.
- University Data: "University Data" is defined as any data that the Contractor creates, obtains, accesses, transmits, maintains, uses, processes, stores or disposes of in performance of the Agreement. It includes all Personally Identifiable Information and other information that is not intentionally made generally available by the University on public websites.
- Personally Identifiable Information: "Personally Identifiable Information" (PII) includes but is not limited to: Any information that directly relates to an individual and is reasonably likely to enable identification of that individual or information that is defined as PII and subject to protection by James Madison University under federal or Commonwealth of Virginia law.
- Security Breach: "Security Breach" means a security-relevant event in which the security of a system or procedure involving University Data is breached, and in which University Data is exposed to unauthorized disclosure, access, alteration, or use.
- Service(s): "Service" or "Services" means any goods or services acquired by the University from the Contractor.

1. **Rights and License in and to University Data:** The parties agree that as between them, all rights including all intellectual property rights in and to University Data shall remain the exclusive property of the University, and Contractor has a limited, nonexclusive license to use the data as provided in the Agreement solely for the purpose of performing its obligations hereunder. The Agreement does not give a party any rights, implied or otherwise, to the other's data, content, or intellectual property.

2. **Disclosure:** All goods, products, materials, documents, reports, writings, video images, photographs, or papers of any nature including software or computer images prepared or provided to the Contractor (or its subcontractors) for the University will not be disclosed to any other person or entity without the written permission of the University.

3. **Data Privacy:**
    a. Contractor will use University Data only for the purpose of fulfilling its duties under the Agreement and will not share such data with or disclose it to any third party without the prior written consent of the University, except as required by law.
    b. University Data will not be stored outside the United States without prior written consent from the University.
    c. Contractor will provide access to University Data only to its employees and subcontractors who need to access the data to fulfill obligations under the Agreement. The Contractor will ensure that the Contractor's employees, and subcontractors when applicable, who perform work under the Agreement have received appropriate instruction as to how to comply with the data protection provisions of the Agreement and have agreed to confidentiality obligations at least as restrictive as those contained in this Addendum.
        i. If the Contractor will have access to the records protected by the Family Educational Rights and Privacy Act (FERPA), Contractor acknowledges that for the purposes of the Agreement it will be designated as a "school official" with "legitimate educational

interests" in such records, as those terms have been defined under FERPA and its implementing regulations, and Contractor agrees to abide by the limitations and requirements imposed on school officials. Contractor will use such records only for the purpose of fulfilling its duties under the Agreement for University's and its End Users' benefit, and will not share such data with or disclose it to any third party except as required by law or authorized in writing by the University. Contractor acknowledges that its access to such records is limited to only those directly related to and necessary for the completion of Contractor's duties under the Agreement.

d. The Contractor shall be responsible and liable for the acts and omissions of its subcontractors, including but not limited to third-party cloud hosting providers, and shall assure compliance with the requirements of the Agreement.

4. **Data Security:**
   a. Contractor will store and process University Data in accordance with commercial best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure Contractor'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.
   b. Contractor will store and process University Data in a secure site and will provide a SOC 2 or other security report deemed sufficient by the University from a third party reviewer along with annual updated security reports. If the Contractor is using a third-party cloud hosting company such as AWS, Rackspace, etc., the Contractor will obtain the security audit report from its hosting company and give the results to the University. The University should not have to request the report directly from the hosting company.
   c. Contractor will use industry-standards and up-to-date security tools, technologies and practices such as network firewalls, anti-virus, vulnerability scans, system logging, intrusion detection, 24x7 system monitoring, and third-party penetration testing in providing services under the Agreement.
   d. Without limiting the foregoing, Contractor warrants that all electronic University Data will be encrypted in transmission (including via web interface) and stored at AES 256 or stronger.

5. **Data Authenticity, Integrity and Availability:**
   a. Contractor will take reasonable measures, including audit trails, to protect University Data against deterioration or degradation of data quality and authenticity. Contractor shall be responsible for ensuring that University Data, per the Virginia Public Records Act, is "preserved, maintained, and accessible throughout their lifecycle, including converting and migrating electronic records as often as necessary so that information is not lost due to hardware, software, or media obsolescence or deterioration."
   b. Contractor will ensure backups are successfully completed at the agreed interval and that restoration capability is maintained for restoration to a point-in-time and\or to the most current backup available.
   c. Contractor will maintain an uptime of 99.99% or greater as agreed to for the contracted services via the use of appropriate redundancy, continuity of operations and disaster recovery planning and implementations, excluding regularly scheduled maintenance time.

6. **Employee Background Checks and Qualifications:**
   a. Contractor shall ensure that its employees have undergone appropriate background screening and possess all needed qualifications to comply with the terms of the Agreement including but not limited to all terms relating to data and intellectual property protection.
   b. If the Contractor must under this agreement create, obtain, transmit, use, maintain, process, or dispose of the subset of University Data known as Personally Identifiable Information or financial or business data, the Contractor shall perform the following background checks on all employees who have potential to access such data in accordance with the Fair Credit Reporting Act: Social

Security Number trace; seven (7) year felony and misdemeanor criminal records check of federal, state, or local records (as applicable) for job related crimes; Office of Foreign Assets Control List (OFAC) check; Bureau of Industry and Security List (BIS) check; and Office of Defense Trade Controls Debarred Persons List (DDTC).

7. **Security Breach:**
   a. Response: Immediately (within one day) upon becoming aware of a Security Breach, or of circumstances that could have resulted in unauthorized access to or disclosure or use of University Data, Contractor will notify the University, fully investigate the incident, and cooperate fully with the University's investigation of and response to the incident. Except as otherwise required by law, Contractor will not provide notice of the incident directly to individuals whose Personally Identifiable Information was involved, regulatory agencies, or other entities, without prior written permission from the University.
   b. Liability:
      i. If Contractor must under this agreement create, obtain, transmit, use, maintain, process, or dispose of the subset of University Data known as Personally Identifiable Information, the following provisions apply. In addition to any other remedies available to the University under law or equity, Contractor will reimburse the University in full for all costs incurred by the University in investigation and remediation of any Security Breach caused by Contractor, including but not limited to providing notification to individuals whose Personally Identifiable Information was compromised and to regulatory agencies or other entities as required by law or contract; providing one year's credit monitoring to the affected individuals if the Personally Identifiable Information exposed during the breach could be used to commit financial identity theft; and the payment of legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the Security Breach.
      ii. If Contractor will NOT under this agreement create, obtain, transmit, use, maintain, process, or dispose of the subset of University Data known as Personally Identifiable Information, the following provisions apply. In addition to any other remedies available to the University under law or equity, Contractor will reimburse the University in full for all costs reasonably incurred by the University in investigation and remediation of any Security Breach caused by Contractor.

8. **Requests for Data, Response to Legal Orders or Demands for Data:**
   a. Except as otherwise expressly prohibited by law, Contractor will:
      i. immediately notify the University of any subpoenas, warrants, or other legal orders, demands or requests received by Contractor seeking University Data;
      ii. consult with the University regarding its response;
      iii. cooperate with the University's requests in connection with efforts by the University to intervene and quash or modify the legal order, demand or request; and
      iv. Upon the University's request, provide the University with a copy of its response.
   b. Contractor will make itself and any employees, contractors, or agents assisting in the performance of its obligations under the Agreement, available to the University at no cost to the University based upon claimed violation of any laws relating to security and\or privacy of the data that arises out of the Agreement. This shall include any data preservation or eDiscovery required by the University.
   c. The University may request and obtain access to University Data and related logs at any time for any reason and at no extra cost.

9. **Data Transfer Upon Termination or Expiration:**
   a. Contractor's obligations to protect University Data shall survive termination of the Agreement until all University Data has been returned or securely destroyed, meaning taking actions that render data written on media unrecoverable by both ordinary and extraordinary means.

b. Upon termination or expiration of the Agreement, Contractor will ensure that all University Data are securely transferred, returned or destroyed as directed by the University in its sole discretion within 60 days of termination of the Agreement. Transfer/migration to the University or a third party designated by the University shall occur without significant interruption in service. Contractor shall ensure that such transfer/migration uses facilities, methods, and data formats that are accessible and compatible with the relevant systems of the University or its transferee, and to the extent technologically feasible, that the University will have reasonable access to University Data during the transition.

c. In the event that the University requests destruction of its data, Contractor agrees to securely destroy all data in its possession and in the possession of any subcontractors or agents to which Contractor might have transferred University data. Contractor agrees to provide documentation of data destruction to the University.

d. Contractor will notify the University of impending cessation of its business and any contingency plans. This includes immediate transfer of any previously escrowed assets and data and providing the University access to Contractor's facilities to remove and destroy University-owned assets and data. Contractor shall implement its exit plan and take all necessary actions to ensure a smooth transition of service with minimal disruption to the University. The Contractor will also provide, as applicable, a full inventory and configuration of servers, routers, other hardware, and software involved in service delivery along with supporting documentation, indicating which if any of these are owned by or dedicated to the University. Contractor will work closely with its successor to ensure a successful transition to the new service, with minimal downtime and effect on the University, all such work to be coordinated and performed in advance of the formal, final transition date.

10. **Audits:**

a. The University reserves the right in its sole discretion to perform audits of the Contractor to ensure compliance with the terms of the Agreement. Contractor shall reasonably cooperate in the performance of such audits. This provision applies to all agreements under which Contractor must create, obtain, transmit, use, maintain, process, or dispose of University Data.

b. If Contractor must under the Agreement create, obtain, transmit, use, maintain, process, or dispose of the subset of University Data known as Personally Identifiable Information or financial or business data, Contractor will at its expense conduct or have conducted at least annually a(n):

   i. American Institute of CPAs Service Organization Controls 2 (SOC 2) audit, or other independent security audit with audit objectives deemed sufficient by the University, which attests to Contractor's security policies, procedures, and controls. Contractor shall also submit such documentation for any third-party cloud hosting provider(s) they may use (e.g. AWS, Rackspace, Azure, etc.) and for all subservice providers or business partners relevant to the Agreement. Contractor shall also provide James Madison University with a designated point of contact for the SOC reports and risks related to the contract. This person shall address issues raised in the SOC reports of the Contractor and its relevant providers and partners, and respond to any follow up questions posed by the University in relation to technology systems, infrastructure, or information security concerns related to the contract.

   ii. vulnerability scan of Contractor's electronic systems and facilities that are used in any way to deliver electronic services under the Agreement; and

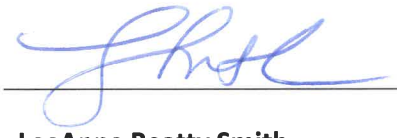
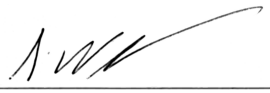
   iii. formal penetration test performed by qualified personnel of Contractor's electronic systems and facilities that are used in any way to deliver electronic services under the Agreement.

c. Additionally, Contractor will provide the University upon request the results of the above audits, scans and tests, and will promptly modify its security measures as needed based on those results in order to meet its obligations under the Agreement. The University may require, at University expense, the Contractor to perform additional audits and tests, the results of which will be provided promptly to the University.

11. **Compliance:**
    a. Contractor will comply with all applicable laws and industry standards in performing services under the Agreement. Any Contractor personnel visiting the University's facilities will comply with all applicable University policies regarding access to, use of, and conduct within such facilities. The University will provide copies of such policies to Contractor upon request.
    b. To the extent applicable to the design and intended use of the service, Contractor warrants that the service it will provide to the University is fully compliant with and will enable the University to be compliant with relevant requirements of all laws, regulation, and guidance applicable to the University and/or Contractor, including but not limited to: the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH), Gramm-Leach-Bliley Financial Modernization Act (GLB), Payment Card Industry Data Security Standards (PCI-DSS), Americans with Disabilities Act (ADA), Federal Export Administration Regulations, and Defense Federal Acquisitions Regulations.

12. **No End User Agreements:** Any agreements or understandings, whether electronic, click through, verbal or in writing, between Contractor and University employees or other end users under the Agreement that conflict with the terms of the Agreement, including but not limited to this Addendum, shall not be valid or binding on the University or any such end users.

IN WITNESS WHEREOF, the parties have caused this addendum to be duly executed, intending thereby to be legally bound. In the event of conflict or inconsistency between terms of the Agreement and this Addendum, the terms of this Addendum shall prevail.

	JAMES MADISON UNIVERSITY		**CONTRACTOR**
SIGNATURE:		SIGNATURE:	
PRINTED NAME:	**LeeAnne Beatty Smith**	PRINTED NAME:	Steven Waxler
TITLE:	**Buyer Senior**	TITLE:	President
DATE:	4/2/19	DATE:	April 3, 2019