JAMES MADISON UNIVERSITY

CONTRACT RENEWAL LETTER

Date:	December 11, 2018	
Contract #:	UCPJMU4397	
Service:	Conference Services Management System	
Renewal Period:	March 17, 2019 to March 16, 2020	
Renewal #:	4 of 9 One-Year	
Issued By:	James Madison University LeeAnne Beatty Smith, Buyer Senior	Ph: 540-568-7523
Contractor:	Seattle Technology Group, Inc. Attn: Ryan Hamilton 1923 25th Avenue E Seattle, WA 98112	Ph: 888-551-9996 x1
Contract Administrator:	Jeremy Hawkins, University Unions	

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 remain the same 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.

Seattle Technology Group, Inc.

By: _____

Ryan Hamilton

Name (print)

President — 12/11/2018

Title — *Date Signed*

James Madison University

By: _____

LeeAnne Beatty Smith, CPPB, VCA, CUPO

Name (print)

Buyer Senior — 12/11/18

Title — *Date Signed*

Contract #: UCPJMU4397
Contractor: Seattle Technology Group, Inc.
Renewal Period: 3/17/2019 - 3/16/2020
Commodity: Conference Services Management System

Conference Programmer Licensing:

Product	Description	Initial Cost	Annual Cost
Conference Programmer (CP) Perpetual Software License	8 concurrent user license Unlimited concurrent user license	$14,000- one (1) time cost $23,000- one (1) time cost	
CP Annual Maintenance	includes unlimited phone and email support and updates		$2,520/year for 8 concurrent users $4,140/year for unlimited concurrent users
Iris Front Desk (IFD) module with unlimited users Preview Housekeeping Functionality shall be provided at no additional cost through 12/31/15.	IFD annual access One Time Set-Up Cost	 $1,000	$2,000
CP Hosting	Annual Hosting includes one (1) production database and one archive database. Additional archive databases are $250/year		$2,500
Implementation	Implementation Package including: five days on-site consulting and training; building the CP database with client rooms and buildings; creation of client contract(s) and custom reports.	$6,250- one (1) time cost does not include travel expenses	
Report Writing	Custom report creation is included in Implementation package. Custom report creation outside of this period will incur additional charges		$125/hour

Iris Registration(IR) V2 Perpetual License:

	IR Lite	**Regular**	**Plus**	**Premium**
Max User Accounts	2	5	Unlimited	Unlimited
Max Forms concurrent active forms	10	20	50	Unlimited
Max Registrants for calendar year	500*	1500*	4000*	20000
Initial Purchase Price includes two (2) hours of training**.**	$5,000	$5,000	$5,000	$5,000
Annual Maintenance	$2,500	$5,000	$7,500	$10,000
Total First year Cost	$7,500	$10,000	$12,500	$15,000
*Purchasing Agencies that exceed the maximum registration count will be charges a *per registration fee* based on the client's current tier: IR Lite: $5.00; Regular: $3.33; Plus: $1.88				

Purchasing Agency and Contractor shall mutually determine when there is a cost benefit to the Purchasing Agency for upgrading to the next tier. The Purchasing Agency shall not be invoiced for upgrading to the next tier without their written approval.

Clients that do not achieve the registration count for their current tier shall receive a refund credit toward the next year's annual charge based on the *per registration fee* . Not applicable for Premium tier.

A La Carte Pricing/Onsite Rates/Annual Maintenance Cap:

Development, Customization, Conversion, Termination Assistance, and/or Custom Report Creation shall be $125/hour.

$1250/day for onsite work not including travel expenses with a two (2) day minimum. There shall be no charge for travel days/time.

James Madison University
Information Technology Services Addendum

CONTRACTOR NAME: Seattle Technology Group, Inc.

PRODUCT/SOLUTION: Conference Services 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.

2. **Nonvisual Access To Technology:** All information technology which, pursuant to the Agreement, is purchased or upgraded by or for the use of any Commonwealth agency or institution or political subdivision of the Commonwealth (the "Technology") shall comply with Section 508 of the Rehabilitation Act (29 U.S.C. 794d), as amended. If requested, the Contractor must provide a detailed explanation of how compliance with Section 508 of the Rehabilitation Act is achieved and a validation of concept demonstration. The requirements of this Paragraph along with the Non-Visual Access to Technology Clause shall be construed to achieve full compliance with the Information Technology Access Act, §§2.2-3500 through 2.2-3504 of the Code of Virginia. Compliance may be determined by the degree to which the product meets the recommendations described in the VPAT (Voluntary Product Accessibility Template) and/or WCAG 2.0 Level AA guidelines.

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 the Agreement or as otherwise 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 read, understood, and received appropriate instruction as to how to comply with the data protection provisions of the Agreement.

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 provided for in the Agreement, 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.

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 SAS 70, SAS 70 Type II, SSAE 16, or 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 their hosting company and give the results to the University. The University should not have to request the report directly from the hosting company, or sign a nondisclosure agreement to receive it.
   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 of 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 data 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, or as negotiated and accepted by the University, 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 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.

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. In addition to any other remedies available to the University under law or equity, when applicable to the type of services being provided, Contractor will pay for or reimburse the University in full for all costs incurred by the University in investigation and remediation of such Security Breach, 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. Contractor agrees to indemnify, hold harmless and defend the University from and against any and all claims, damages, or other harm related to such Security Breach.

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 30 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 and to complete any required Commonwealth of Virginia documentation regarding the destruction of University Data.

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 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 equipment, 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 Contractor at no additional cost to the University 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 (SOC) Type II audit, or other 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 provider(s) or business partners relevant to this contract. Contractor shall also provide James Madison University with a designated point of contact for the SOC report(s) and risks related to the contract. This person shall address issues raised in the SOC report(s) 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. All documentation shall be provided free of charge and submitted to IT-Assessments@jmu.edu. The Contractor shall provide the SOC II report(s) and other necessary documentation annually 90 days prior to the contract anniversary date. The University should not have to request the SOC II reports or other assessment documents or sign a nondisclosure agreement.
        ii. vulnerability scan, performed by a scanner approved by the University, 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 a process and qualified personnel approved by the University, 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.

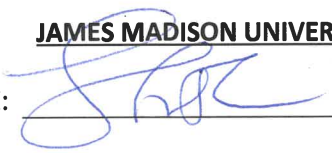
11. **Compliance:**
    a. Contractor will comply with all applicable laws and industry standards in performing services under the Agreement. Any Contractor personnel visiting the University's facilities will comply with all applicable University policies regarding access to, use of, and conduct within such facilities. The University will provide copies of such policies to Contractor upon request.
    b. 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) and 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).

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.

To the extent allowed by Virginia law, James Madison University will keep any information provided in a security audit report confidential to protect the integrity of the Contractor.

IN WITNESS WHEREOF, the parties have caused this addendum to be duly executed, intending thereby to be legally bound.

JAMES MADISON UNIVERSITY		**CONTRACTOR**	
SIGNATURE:		SIGNATURE:	
PRINTED NAME:	LeeAnne Beatty Smith	PRINTED NAME:	Ryan L. Hamilton
TITLE:	Buyer Senior	TITLE:	President
DATE:	12/11/18	DATE:	12/11/2018