JMU

JAMES MADISON
UNIVERSITY.

CONTRACT MODIFICATION

Date: April 11, 2022

Contract #: UCPJMU4135

Service: Information Technology Management System

Modification #: One

Issued By: James Madison University
Colleen Johnson, Buyer Senior
Ph: 540-568-3137
Fx: 540-568-7935

Contractor: Avante Solutions
Attn: Steven Waxler
738 W, Jackson Blvd
Chicago, IL 60661

Contract Administrator: Robin Bryan, Information Technology

Description of Modification Notice:

The following attached documents hereby are incorporated into and amend UCPJMU4135:

- Cherwell Service Management Licensing Pricing, which replaces the contract pricelist;
- Avante Solutions' Exhibit to Commonwealth of Virginia Standard Contract SOW - Migrate to Cloud, dated April 11, 2022;
- Avante Solutions' Cherwell Order Confirmation Form, dated April 11, 2022;
- Amendment to the End-User License Agreement for JMU;
- Cherwell's Hosting Services Addendum to the Cherwell End-User License Agreement, which includes:
  - Exhibit 1: Data Processing Agreement.

Except as provided herein, all terms and conditions of Contract Number UCPJMU4135 remain unchanged and in full force and effect.

Avante Solutions
By: ______________________
Steven Waxler
Name (print)
President April 19, 2022
Title *Date Signed*

James Madison University
By: ______________________
Colleen Johnson,
Name (print)
Buyer Senior 4/20/2022
Title *Date Signed*

Cherwell Service Management Licensing Pricing

A. Perpetual/Purchased License Model Pricing:

Item	Unit Cost
Cherwell Service Management	$3,558.92/license for 1-24 concurrent licenses $2,974.61/license for 25-99 concurrent licenses $2,655.90/licenses for 100-199 concurrent licenses +199 concurrent licenses priced upon request
Annual Maintenance & Support	$637.42/license for 1-24 concurrent license(s) $531.18/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	$30,000.00 Annual Fee for modern hosting option. The hosting service includes 2 environments, 1 production and 1 non-production– note the legacy hosting service is no longer offered
Encryption at Rest	Standard Encryption at Rest Included (Optional additional TDE layered encryption at rest is $10,000.00/annual fee.)
Optional – Additional Hosted Non-production Environment *(one (1) included in subscription)*	$15,000.00 per instance
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 $2,974.61/per license. If 75 more licenses are purchased at a later date, the cost would be $2,974.61/each for 74 of the licenses and 1 license at $2,655.90). The same applies to Annual Maintenance and Support pricing.	

B. Subscription License Model Pricing:

Item	Unit Cost
Cherwell Service Management Subscription Fee *(monthly)*	$116.83/license for 1-24 concurrent licenses $100.92/license for 25-99 concurrent licenses $95.61/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 For new purchases only. Perpetual licenses customers that convert to the subscription license model who would like to convert from on-premise installation to Cherwell hosted service the $30,000.00 annual fee is applicable.
Encryption at Rest	Standard Encryption at Rest Included in Subscription Cost (Optional additional TDE layered encryption at rest is $10,000.00/annual fee.)
Optional – Additional Hosted Non-production Environment *(one (1) included in subscription)*	$15,000.00 per instance
Subscription pricing is based on a three-year subscription term and shall be invoiced annually in advance of the subscription year.	

C. **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 $7,967.70 plus additional $796.77 annual maintenance and support for both licensing models.

D. **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 @$199.19/hour shall = $1,115.46). 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 $199.19 ($1,593.52/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 $252.31 ($2,018.48/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.

avante
SOLUTIONS INC.

EXHIBIT TO COMMONWEALTH OF VIRGINIA STANDARD CONTRACT

STATEMENT OF WORK – MIGRATE TO CLOUD

This Statement of Work ("**SOW**") is subject to the terms and conditions contained in the Commonwealth of Virginia Standard Contract (CVSC) Number UCPJMU4135 between the parties hereto dated March 27, 2015 and is hereby made a part thereof. All terms and conditions of the CVSC, including (but not limited to) warranties, disclaimers of warranty and limitations of liability, are expressly incorporated herein by reference. To the extent there are any conflicts or inconsistencies between this SOW and the CVSC, the provisions of the CVSC shall govern and control unless the parties have expressly provided in this SOW that a specific provision in the CVSC is amended, in which case the CVSC shall be so amended, but only with respect to this SOW. Any such conflicting terms and conditions apply only to the Services and Deliverables described in this SOW and shall have no application to Services and/or Deliverables provided pursuant to any other SOWs. All capitalized terms used but not otherwise defined have the meanings ascribed in the CVSC.

The specific terms and conditions relating to the Services and Deliverables include the following:

1. **Scope.** A detailed description of the scope of services to be provided by Avante and the Parties respective deliverables and performance obligations under this SOW are attached hereto as Schedule 1.

2. **Compensation and Pricing.** The compensation and payments due to Avante under this SOW are set forth on Schedule 2 hereto.

3. **Term/Time Frame.** The services of Avante as provided herein and the CVSC shall be performed during 2022.

4. **Other Provisions.** Upon execution, this SOW shall be deemed to be a Statement of Work entered into pursuant to the CVSC, and as such shall be attached to the CVSC as Exhibit A, made a part thereof and be controlled by and interpreted in accordance with the CVSC. All of the Schedules attached to this SOW are hereby made a part of and are incorporated into this SOW by reference. Any changes to this SOW may affect the Project's delivery dates and budget and shall only be effective on the written approval of both Parties.

IN WITNESS WHEREOF, the Parties have duly executed this SOW, to be effective as of the 11th day of April, 2022.

CUSTOMER:

Commonwealth of Virginia, James Madison University

By: ______________________

Printed Name: Colleen Johnson

Title: Buyer Senior

AVANTE:

Avante Solutions, Inc.

By: ______________________

Printed Name: Steven Waxler

Title: President

Schedule 1
Scope of Project

Scope Definition

The following items are in scope for this SOW:

- Avante will provide assistance migrating JMU's current Cherwell system from your on-premise installation to the Cherwell cloud.

Key Assumptions

The following points represent key assumptions used in the preparation of this quote:

- Documentation will be limited to the existing Cherwell published online documentation.

Schedule 2
Compensation and Pricing

Phase Deliverable	Comment	Time Effort
Professional Services	As outlined on the Scope section	40 hours
Total		**$7,967.60**

TERMS AND CONDITIONS

1. Terms of the agreement UCPJMU4135 apply to this order.
2. Current contractual rate is based on $199.19 per hour.

Remit payment to:
Avante Solutions, Inc.
728 W Jackson Blvd. Suite 105
Chicago, IL 60661
Attn: Accounts Payable

Schedule 3

Term and Time Frame

Schedule will be determined based on JMU's decision to execute the migration.

avante
SOLUTIONS INC.

Cherwell Order Confirmation Form

The purpose of this Order Confirmation Form ("Order") is to document the purchase of certain technology of Cherwell Software, LLC ("Cherwell") by Customer through Avante (as each defined below), as an authorized resale partner of Cherwell, and the terms of such purchase.

Commonwealth of Virginia, James Madison University ("Customer")
752 Ott Street
Harrisonburg, Virginia 22807
Mike Mehling
mehlinmr@jmu.edu

Date Issued: April 11, 2022

Pricing Valid for Sales Completed by: May 30, 2022
License Term: Annual
License Effective Date: Date of last signature below

Avante Solutions, Inc. ("Avante")
Rich Clark
728 W Jackson Blvd. Suite 105
Chicago, IL 60661
rclark@avantesolutions.com

Required Items			
Item	**Unit Cost**	**Units**	**Investment**
Cherwell CSM Hosting Services - Annual Cherwell hosting to include one production environment and a second dev or test environment. Additional servers are available at an additional cost.	$30,000.00	1	$30,000.00
TOTAL ANNUAL FEE			**$30,000.00**

All pricing above is in US Dollars. The above pricing does not include any applicable sales tax or similar tax. Unless otherwise approved by Avante, all payments shall be made by ACH withdrawal or wire transfer in accordance with instructions shown on the applicable invoice. Terms and conditions contained in the Commonwealth of Virginia Standard Contract (CVSC) Number UCPJMU4135 apply to this order.

Signature Section – Each party signing below represents that it has authority to bind the company or legal entity named below. By signing this document, the customer agrees that the terms in the EULA and HSA are between the Customer and Cherwell.

Customer: Commonwealth of Virginia, James Madison University		**Avante: Avante Solutions, Inc.**	
By (print name and title):	Colleen Johnson, Buyer Senior	**By (print name and title):**	Steven Waxler, President
Signature:		**Signature:**	
Date:	4/20/2022	**Date:**	April 19, 2022

AMENDMENT TO THE
AND END-USER LICENSE AGREEMENT
FOR JAMES MADISION UNIVERSITY

End-User License Agreement ("Agreement") accepted under the Cherwell Order Confirmation Form ("Order Confirmation) dated March 30, 2015 by and between James Madison University (the "Customer") and Cherwell Software, LLC ("Cherwell") is hereby amended as follows:

Customer currently has 100 CSM on-premise perpetual licenses. Customer will be moving its CSM licenses from on-premise to the Cherwell hosted environment in June, 2022 and will be entering into Cherwell Hosting Services Addendum ("HSA") which governs the use of the hosting services. With this transition to the Cherwell hosted environment, the parties agree to add a Super Cap Limitation of Liability for Data Breach under Section 4 of the EULA as follows:

> **4.1.a Super Cap Limitation of Liability.** In addition to any other remedies allowed under applicable law, for any event of Data Breach or for any security breach caused by Cherwell (other than a security breach caused by Cherwell's negligence or willful misconduct, the damages for which shall remain uncapped), the total liability for such breach shall not exceed the amount equal to five times (5x) the amount paid under the Agreement for the licensed software during the twelve (12) months preceding the security breach incident.

Except as provided above, all other provisions and terms and conditions of the Agreement remain unchanged and in full force and effect.

IN WITNESS WHEREOF, the parties hereto have executed this Amendment effective as of the last date of signature below.

Cherwell Software, LLC

By: Al Crews

Name: Al Crews

Title: VP, Americas EXM Sales

Date: 4/13/2022

James Madison University

By:

Name: Colleen Johnson

Title: Buyer Senior

Date: 4/20/2022

cherwell

HOSTING SERVICES ADDENDUM

This Hosting Services Addendum (this "Addendum") is between Cherwell Software, LLC ("Cherwell") and James Madison University ("Customer"), and is entered into pursuant to the End-User License Agreement under Order Confirmation dated March 30, 2015, together with the Commonwealth of Virginia Contract Form Addendum Contactor's Form signed September 4, 2014 (collectively the "Agreement") between Customer and Cherwell regarding certain Licensed Software. This Addendum applies when Customer has chosen to deploy the Licensed Software in a Cherwell-hosted environment and is attached to and incorporated into the Agreement.

1. HOSTING SERVICES

1.1 Facility. Cherwell shall, either directly or indirectly through a third party hosting facility, maintain and support the hardware, servers, operating systems, database servers, networking and infrastructure necessary for Customer to access and use the Licensed Software. Cherwell's hosting facility will comply with applicable laws, rules and regulations and other processing resources as set forth in the Data Processing Addendum ("DPA") as Exhibit 1. Upon request, Cherwell will provide Customer with documentation describing such standards and measures. Cherwell shall provide a Domain Name System (DNS) Name which shall provide Customer connectivity and access to the Licensed Software. Customer's Hosted Data will not be stored outside the United States without prior written consent of Customer. Customer acknowledges and agrees that, while hosted data will not be transmitted or routed outside of the United States. Data may be accessed from Cherwell\Ivanti support operations as part of providing technical support, provided that such support operations have the Customer's consent.

1.2 Security. Hosted Data means all text, images and information provided by Customer and stored in the hosted system. Cherwell will use industry standard security measures, such as firewalls and standard encryption protocols, to protect Hosted Data Cherwell shall logically segregate Hosted Data from data belonging to other Cherwell customers. Cherwell will immediately notify Customer of a confirmed security breach that impacts Hosted Data and will provide Customer with regular status updates until the breach is resolved. Within 72 hours of final resolution of the breach, Cherwell will provide Customer with a final incident report. Except as may be strictly required by applicable law, Cherwell agrees that it will not inform any third party of any such security breach involving Hosted Data without Customer's prior written consent. In the event Cherwell engages a third party service provider to assist Cherwell in fulfilling its duties under this Addendum, Cherwell agrees that it will enter into a confidentiality agreement with the third party that is at least as protective of Customer's Confidential Information as the Agreement. In additional, Cherwell maintains security and compliance information on its Whistic site currently located at https://console.whistic.com/v2/request-profile/v2/803040d2-f220-4d45-bec0-d5ea365761dd/4b7f0384-7d2a-4446-9253-4f0fa11216bc

1.3 Hosted Data Back-Up. For the Licensed Software installed in the hosted production environment, Cherwell will (i) perform hourly differential backups and store such backups for five (5) days; and (ii) perform daily backups and store such backups for thirty-one (31) days. For hosted non-production environments, Cherwell will perform daily backups and store such backups for thirty-one (31) days. All backups are encrypted both at rest and in transit. Backups are made directly to disk and replicated to a secondary geographically disperse location. Cherwell will use commercially reasonable efforts to meet a disaster recovery time objective of two (2) hours in a disaster recovery scenario. Customer acknowledges that Cherwell may charge customer for recovering data which was lost or no longer available as a result of Customer's own actions or inactions. Cherwell shall provide Customer with full access and control over Hosted Data and the capability to download and make backups of Hosted Data at any time during the term of this Addendum. Subject to the above, Customer acknowledges that Cherwell's services are not intended to be used as the sole repository for Hosted Data and that Customer has access to and control over its Hosted Data, including the ability to make its own backups using the Cherwell Administration tool.

1.4 Business Continuity. Cherwell will maintain a defined disaster recovery plan and process designed to minimize the risks associated with a disaster affecting Cherwell's ability to provide the hosting services under this Addendum. Cherwell will test its disaster recovery plan annually. Upon request, Cherwell will provide a summary of its disaster recovery plan and test results, excluding any proprietary information.

1.5 Support. All requests for Support must be directed to the designated technical support team and not the Cherwell hosting team.

1.6 Upgrade Notification. Cherwell shall provide Customer thirty (30) days advance notice prior to applying any updates, upgrades, patches, bug fixes and new releases or versions of the Licensed Software provided as part of Maintenance (each a "Maintenance Release") to the Cherwell-hosted Licensed Software. Customer may opt out of a particular Maintenance Release, provided, however, that Customer agrees that it will not be able to decline or defer critical security patches and updates and Cherwell is free in its reasonable discretion to determine which Maintenance Releases are critical. Customer shall be responsible for applying Maintenance Releases to any locally installed portion of the Licensed Software.

2. SYSTEM AVAILABILITY; EXCUSED OUTAGES

2.1 Availability. The Licensed Software shall be available 99.98% of the time per month, except for Excused Outages. Excused Outages are defined as unavailability of the Licensed Software caused by (i) Scheduled Maintenance, as defined below; (ii) Customer's systems or Customer's actions or inactions; and (iii) circumstances beyond Cherwell's control or the control of Cherwell's authorized agent or service provider, including without limitation, acts of God, acts of government, flood, fire, earthquakes, civil unrest, acts of terror, strikes not involving employees of Cherwell or Cherwell's authorized agent or service provider, and equipment and telecommunications failures, delays outside of Cherwell's network, attacks or intrusions that are external to the

Cherwell hosting environment and/or otherwise not reasonably under Cherwell's control, provided Cherwell or its authorized agent or service provider takes reasonable and commercial care to prevent such failures, delays, attacks or intrusions.

2.2 Scheduled Maintenance. Unless otherwise provided under an Order Confirmation, Cherwell will perform Scheduled Maintenance only during the weekends, beginning no earlier than Friday at 8:00 p.m. MST and ending no later than 2:00 a.m. MST Saturday, unless otherwise agreed upon by both parties, and shall provide Customer at least seven (7) calendar days advance notice thereof, except for emergency maintenance, in which case Cherwell shall provide as much notice as reasonably practicable.

2.3 Notification and Cooperation. In addition to the Scheduled Maintenance notice above, Cherwell will promptly notify Customer of any service outages via email or telephone. All notices will include a recovery time estimate. Cherwell will attempt to resolve outages within the time estimated but any timeframes are estimates only and are not guaranteed. Cherwell will also notify Customer when the outage is resolved and services have been restored. Customer acknowledges that in certain circumstances system unavailability may be caused by issues with Customer's computers or systems and agrees to cooperate with Cherwell to determine the source of the outages. Further, Cherwell will promptly notify Customer in writing of any requests for Hosted Data and direct such request to Customer for response and direction.

2.4 Service Credit. "Service Credit" means a credit, calculated as set forth below, provided by Cherwell to Customer on its next invoice. In the event the Licensed Software is not available as set forth in Section 2.1, Customer shall be entitled to a Service Credit equal to the value of the down time (on a pro-rata basis, using Customer's annual license maintenance fee or annual hosting fee, as the case may be). In the event Customer is entitled to Service Credits over any three consecutive months, or for any five months during a 12- month period, then notwithstanding any other provision of the Agreement, Customer shall have the right to terminate this Addendum and receive a pro rata refund of any prepaid but unused subscription or hosting fee.

3 CUSTOMER ACCESS. In order to administer its installation of the Licensed Software, Customer must install the Cherwell Administration module on a local computer. However, in order to maintain the security of the hosted system while Cherwell is providing hosting services, Customer will not have direct access to the hosted environment except via the Cherwell Service Management applications and shall not install the Server portion of the Licensed Software on its own systems or premises for use in a production environment. At Customer's option, Customer may (i) access the Licensed Software in a "smart client" environment and install the Client portion of the Licensed Software on Customer's end-user computers or (ii) Customer may access the Licensed Software in a "browser client" environment without installing the Client portion of the Licensed Software on Customer's end-user computers. In either environment, however, the number of concurrent users accessing the Licensed Software must not exceed the number of concurrent users provided for under the Agreement. Customer may install copies of any portion of the Licensed Software in non-production environments, solely for purposes of testing, development or disaster recovery, provided, however, that in no eventshall such copies be used for production purposes.

4 CUSTOMER OBLIGATIONS

4.3 Restrictions. Customer shall not, and shall ensure that its employees, affiliates and clients do not: (i) knowingly or intentionally interfere with or disrupt the Licensed Software or the Cherwell systems used to host the Licensed Software, including, without limitation, transmitting viruses, worms, Trojan horses or other malicious code; (ii) attempt to gain unauthorized access to the hosted system or network or allow others to do so; or (iii) make any use of the service that violates any applicable law, rule or regulation. Cherwell may suspend services due to detection of an attack coming from Customer's systems or a reasonable determination that continued use of the service will violate applicable law or the legal rights of another person or entity.

4.2. Representation by Customer. Customer represents that it has all necessary permissions and rights to the Hosted Data and grants Cherwell a limited and non-exclusive license, for the sole purpose of providing services under this Addendum, to copy, display, distribute, download and transmit Hosted Data. To the extent Hosted Data is Confidential Information of Customer, it is subject to the terms of the Agreement, including the Confidentiality section, and to any other confidentiality agreement mutually agreed between Cherwell and Customer.

5 TERM AND TERMINATION

5.1 Effective Date and Term. Unless terminated in accordance with Section 5.2 below:

(a) For perpetual licenses, this Addendum is effective as of the Effective Date of the Agreement and the initial term of this Addendum shall be one year, unless otherwise agreed to in writing by the parties. Following the initial term, Customer may renew this Addendum for one or more additional one-year terms by providing notice to Cherwell. Payment by Customer of Cherwell's renewal invoice for the hosting service fees, which will be sent to Customer at least 30 days prior to the end of any term, shall constitute notice of Customer's election to renew.

(b) For subscription licenses, this Addendum is effective as of the Effective Date and is coterminous with the Agreement.

5.2 Termination. Either party may terminate this Addendum upon written notice to the other party if the other party fails to cure a material breach of this Addendum within thirty (30) days of written notice of the breach from the terminating party. Upon termination by Customer for an uncured breach by Cherwell, Cherwell will pay Customer a pro-rata refund of any prepaid but unused hosting fee, plus any unpaid service credits payable to Customer.

(a) With respect to perpetual licenses only, Customer may terminate this Addendum at any time, without cause, by providing written notice to Cherwell, but this does not entitle Customer to any type of refund.

(b) With respect to subscription licenses only, Customer may terminate this Addendum at any time during the then-current Term, without cause, by providing written notice to Cherwell, provided, however, such termination will result in Customer incurring additional fees of 10% of Customer's subscription fees for the remainder of the Term.

5.3 Effect of Termination. With respect to perpetual licenses, termination of this Addendum shall not terminate the Agreement nor Customer's right to use the Licensed Software as set forth in the Agreement; provided, however, that termination of this Addendum will likewise not obligate Cherwell to reinstall the Licensed Software on Customer's own systems or premises or provide professional or "migration" services related thereto, except as mutually agreed upon by the parties. Upon termination of this Addendum, Customer will have 30 days to request a copy of its data, and if requested, Cherwell shall provide such data in an industry-standard format such as a XML or .csv file at no additional charge. After the 30-day period, Cherwell has no obligation to maintain or provide Hosted Data and will destroy all Hosted Data in its possession or under its control in accordance with secure data destruction methods so as to protect against unauthorized access to destroyed Hosted Data, unless such destruction is legally prohibited. Upon request, Cherwell shall provide Customer with a certificate of destruction or other documentation indicating that it has complied with the above sentence.

Agreed upon between the Parties:

James Madison University

Signature: ______________________

Name: ColleenJohnson

Title: Buyer Senior

Date: 4/20/2022

Cherwell Software, LLC.

Signature: Al Crews

Name: Al Crews

Title: VP, Americas EXM Sales

Date: 4/16/2022

Exhibit 1

DATA PROCESSING AGREEMENT

This Data Processing Addendum ("DPA") forms a part of the Cherwell End User License Agreement and Hosting Services Addendum (collectively the "Agreement") and is made and entered into as of the last signature date below (the "Effective Date") by and between the customer identified below or in the Agreement ("Controller") and the Cherwell Software, LLC ("Cherwell" or "Processor") (individually, a "Party"; collectively, the "Parties"). Any capitalized terms not defined herein shall have the respective meanings given to them in the Agreement.

RECITALS

WHEREAS, the Parties have entered into the Agreement.

WHEREAS, in the course of providing the Services to Controller pursuant to the Agreement, Processor may Process Personal Data on behalf of Controller;

WHEREAS, to ensure adequate safeguards with respect to the Processing of Personal Data provided by Controller to the Processor the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

NOW, THEREFORE, in consideration of the foregoing premises and of the mutual promises and covenants set forth below, Controller and Processor hereby agree as follows:

AGREEMENT

1. DEFINITIONS

All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"**Applicable Data Protection Laws**" means all applicable laws, regulations, regulatory guidance, or requirements in any jurisdiction relating to data protection, privacy, or confidentiality of Personal Data including but not limited to (a) the GDPR together with any transposing, implementing or supplemental legislation, and (b) the CCPA.

"**Authorized Affiliate**" means any of Controller's Affiliates which (a) are subject to the data protection laws and regulations of the European Economic Area and/or its member states, the United Kingdom, and Switzerland, (b) are subject to data protection laws and regulations outside of the European Economic Area and/or its Member States, Switzerland, and the United Kingdom (as applicable), and (c) permitted to use the Processor for Processing pursuant to the Agreement.

"CCPA" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.*, and its implementing regulations.

"Controller" means the entity which determines the purposes and means of the Processing of Personal Data. For the avoidance of doubt, the Party identified above as "Controller" is a Controller under this DPA.

"Data Breach" means a breach of security leading to the accidental, unauthorized, or unlawful destruction, loss, alteration, disclosure of, access to, or other Processing of Personal Data transmitted, stored, or otherwise Processed.

"Data Protection Authority" means any representative or agent of a government entity or agency who has the authority to enforce Applicable Data Protection Laws.

"Data Subject" means a natural person to whom Personal Data relates.

"GDPR" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

"Personal Data" means any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with an identified or identifiable natural person or particular household. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

"Process" shall mean any operation or set of operations which is performed upon Personal Data by the or in connection with and for the purposes of the provision of the Services, whether or not accomplished by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction; and as defined by Applicable Data Protection Laws.

"Processor" means the entity which Processes Personal Data on behalf of the Controller. For the avoidance of doubt, the Party identified as "Processor" above is a Processor for this DPA.

"Services" means Processing of Personal Data by the Processor in connection with and for the purposes of the provision of the services to be provided by the Processor pursuant to the Agreement.

"Service Provider" means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that process information on behalf of a Data Controller and to which the Data Controller discloses a Data Subject's Personal Data for a Business Purpose pursuant to a written contract, provided that the contract prohibits the Service Provider from retaining, using, or disclosing the Personal Data for any purpose other than for the specific purpose of performing the services specified in the contract, or as otherwise permitted by the CCPA, including retaining, using, or disclosing the Personal Data for a Commercial Purpose other than providing the services specified in the contract with the Data Controller. The terms "Business Purpose" and "Commercial Purpose" have the same meaning as those terms are used in the CCPA. For the avoidance of doubt, Processor is a Service Provider.

"Sub-processor" means any entity which Processes Personal Data on behalf of the Processor.

2. PROCESSING OF PERSONAL DATA

2.1 Roles of the Parties. The parties acknowledge and agree that about the Processing of Personal Data, Controller is the Controller, Processor is the Processor or Service Provider. The subject matter, duration, purpose of the Processing, and the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 1.

2.2 Controller's Obligations. Controller's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Controller shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Controller acquires Personal Data and provides it to Processor.

2.3 Processor's Obligations. All Personal Data Processed by Processor pursuant to the Agreement is Confidential Information and Processor will Process Personal Data only in accordance with Controller's documented instructions set forth in Schedule 1 or as otherwise provided by Controller in writing. Processor will not sell the Personal Data Processed under this DPA and will not retain, use, or disclose Personal Data outside of the direct business relationship between Processor and Controller. Processor shall adhere to all Applicable Data Protection Laws with regard to Processing Personal Data. Where the Processor believes that compliance with any instructions by Controller would result in a violation of any Applicable Data Protection Law, the Processor shall notify Controller thereof in writing without delay. Processor shall make available to the Controller all information necessary to demonstrate Processor's compliance with its obligations under this DPA. Cherwell's liability under this DPA is set forth in the Agreement.

2.3.1. **Assistance Requirements.** Processor shall assist Controller with: compliance with Applicable Data Protection Laws; suspected and relevant Data Breaches; notifications to, or inquiries from a Data Protection Authority; notifications to, and inquiries from, Data Subjects; and Controller's obligation to carry out data protection impact assessments and prior consultations with a Data Protection Authority.

3. NOTIFICATION OBLIGATIONS

3.1 Processor's Notification Obligations. Processor shall immediately notify Controller, in writing, of the following:

3.1.1 A Data Subject's request to exercise their privacy rights such as accessing, rectifying, erasing, transporting, objecting to, or restricting their Personal Data;

3.1.2 Any request or complaint received from Controller's customers or employees;

3.1.3 Any question, complaint, investigation, or other inquiry from a Data Protection Authority;

3.1.4 Any request for disclosure of Personal Data that is related in any way to Processor's Processing of Personal Data under this DPA;

3.1.5 A Data Breach pursuant to the notification obligations set forth in Section 7.1; and

3.1.6 Where the Personal Data becomes subject to search and seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by third parties while being Processed.

Processor will assist Controller in fulfilling Controller's obligations to respond to requests relating to paragraphs (3.1.1) - (3.1.6) above and will not respond to such requests without Controller's prior written consent unless Processor is required to respond by law.

4. CONFIDENTIALITY

4.1 Confidential Information. All Information provided to Processor pursuant to the Agreement is Confidential Information.

4.2 Processor's Personnel. Processor shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities, and have executed written confidentiality agreements. Processor shall ensure that such confidentiality obligations survive the termination of their respective employment relationship with such individuals.

4.3 Limitation of Access. Processor shall ensure that Processor's access to Personal Data is limited to those personnel performing Services in accordance with the Agreement.

5. SUB-PROCESSORS

5.1 Appointment of Sub-processors. Controller acknowledges and agrees that Processor and Processor's Affiliates may engage third-party Sub-processors in connection with the provision of the Services. Processor or Processor's Affiliate shall enter into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this DPA to the extent applicable to the nature of the Services provided by such Sub-processor. Controller hereby authorizes Processor to engage its current list of Sub-processors as listed on Schedule 2 to Process

Personal Data in accordance with this DPA. Controller will not directly communicate with Processor's Sub-processors about the Services, unless agreed to by Processor in Processor's sole discretion.

5.2 Notification of Changes to Sub-processors. Processor will inform Controller of any intended changes concerning the addition or replacement of Sub-processors by providing Controller written notice. Processor will notify Controller of any intended changes concerning the addition or replacement of Sub-processors prior to its use of the Sub-processor.

5.3 Objection Right for New Sub-processors. Controller may reasonably object to Processor's use of a new Sub-processor by notifying Processor promptly in writing within fifteen (15) business days after receipt of Processor's notice. In the event Controller objects to a new Sub-processor, Processor will use reasonable efforts to make available to Controller a change in the Services to avoid Processing of Personal Data by the objected-to new Sub- processor. If Processor is unable to make available such change, Controller may terminate the applicable Agreement with respect to those Services which cannot be provided by Processor without the use of the objected-to new Sub-processor.

5.4 Liability for Acts of Sub-Processors. Processor shall be liable for the acts and omissions of its Sub-processors to the same extent Processor would be liable if performing the services of each Sub-processor directly under the terms of this DPA.

6. SECURITY

6.1 Protection of Personal Data. Processor shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data), confidentiality and integrity of Personal Data.

6.2 Audit Rights. Controller agrees its right to audit Processor may be satisfied by Processor presenting up-to-date attestations, reports or extracts from independent bodies, including without limitation external or internal auditors, Processor's data protection officer, the IT security department, data protection or quality auditors or other mutually agreed to third parties or certification by way of an IT security or data protection audit. To the extent it is not possible to satisfy an audit obligation mandated by applicable Data Protection Laws and Regulations through such attestations, reports or extracts, Controller, or Controller's designee, has the right to audit and inspect—at Controller's expense—Processor's premises, policies, procedures, and computerized systems to make sure Processor complies with the requirements in this DPA. Controller, or Controller's designee, will provide at least thirty (30) days notification before conducting an audit unless such audit is required due to a Data Breach involving Processor. Audits by Controller or Controller's designee will not violate Processor's confidentiality obligations with Processor's other clients. All audits will be conducted during normal business hours, at Processor's principal place of business or other Processor location(s) where Personal Data is accessed, processed or administered, and will not unreasonably interfere with Processor's day-to-day operations. Before the commencement of any such audit, Processor and Controller shall mutually agree upon the timing, scope, and duration of the audit. Controller may request a summary audit report(s) or audit Processor no more than once annually.

7. DATA BREACHES

7.1 Data Breach Notification. Processor shall notify Controller in writing without undue delay after becoming aware of a suspected Data Breach. In no event shall such notification be made less than 72 hours after Processor's discovery of the Data Breach.

7.2 Data Breach Management. Processor shall make reasonable efforts to identify the cause of such Data Breach and take those steps as Processor deems necessary and reasonable to remediate the cause of such a Data Breach to the extent the remediation is within Processors reasonable control.

8. TERMINATION

8.1 Termination. This DPA shall terminate automatically upon the later of (a) the termination or expiry of the Agreement or (b) Processor's deletion or return of Personal Data. Controller shall further be entitled to terminate this DPA for cause if the Processor is, in the sole opinion of Controller, in a material or persistent breach of this DPA, which, in the case of a breach capable of remedy, shall not have been remedied within ten (10) days from the date of receipt by the Processor of a notice from Controller identifying the breach and requesting its remedy.

8.1 Return or Deletion of Data. Upon termination of this DPA, Processor will delete or return all existing copies of Personal Data unless applicable law requires continued retention of the Personal Data. Upon the request of Controller, the Processor shall confirm compliance with such obligations in writing and delete all existing copies. In instances where local law requires the Processor to retain Personal Data, Processor will protect the confidentiality, integrity, and accessibility of the Personal Data; will not actively Process the Personal Data; and will continue to comply with the terms of this DPA.

9. MECHANISMS FOR INTERNATIONAL TRANSFERS

9.1 Transfers Outside of the EU. In the course of the provision of Services under the DPA, it may be necessary for Controller to transfer Personal Data from the European Union, the European Economic Area and/or their member states, Switzerland, or the United Kingdom, to Processor in a country that does not have an adequacy decision from the European Commission or is not located in the European Economic Area. In the event of such a transfer, the Standard Contractual Clauses set forth in Schedule 2 shall apply.

9.2. Alternative Data Transfer Mechanisms. The Parties acknowledge that the laws, rules and regulations relating to international data transfers are rapidly evolving. In the event that Controller adopts another mechanism authorized by applicable laws, rules or regulations to transfer Personal Data (each an "Alternative Data Transfer Mechanism"), the Parties agree to work together in good faith to implement any amendments to this Agreement necessary to implement the Alternative Data Transfer Mechanism.

10. MISCELLANEOUS PROVISIONS

10.1. Amendments. This DPA may not be amended or supplemented, nor shall any of its provisions be deemed to be waived or otherwise modified, except through a writing duly executed by authorized representatives of both parties.

10.2 Governing Law. This DPA shall be governed by the governing law set forth in the Agreement.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the Effective Date.

CONTROLLER: **James Madison University**

Signature: ____________________

Name: Colleen Johnson

Title: Buyer Senior

Date: 4/20/2022

Cherwell Software, LLC

Signature: Al Crews

Name: Al Crews

Title: VP, Americas EXM Sales

Date: 4/16/2022

List of Schedules:

Schedule 1: Description of the Processing

Schedule 2: Standard Contractual Clauses

SCHEDULE 1

Description of the Processing

Subject-Matter
The subject-matter of the Processing:
Provision of IT software licensing, support services and implementation, whether on-premises or as a hosted SaaS solution, regarding the administration and facilitation of essential business processes in the field(s) of unified endpoint management, IT service management, IT asset management, security, reporting and analytics, and supply chain.

IT services include the use of software as an on-premise installation or a SaaS solution including installation of modules (including without limitation, incident, change, asset, configuration and release management modules); self-service and service catalogues; support and maintenance including, without limitation, remote access; and patches, app control, endpoint/mobile security and privilege management.

Duration
Duration of the Processing:
As set forth in the Agreement.

Extent, Type and Purpose of the Processing
The extent, type and purpose of the Processing is as follows:
As set forth in the Agreement.

Data Subjects
Personal Data Processing may relate to the following categories of Data Subjects:
Customers, prospects; employees; suppliers; commercial representatives; contacts; contractors (including contingent workers); volunteer; temporary and casual workers; freelancers, agents, consultants and other professional respondents, and their respective dependents, beneficiaries and emergency contacts; perspective employees and temporary staff of customers; complainants, correspondents and enquirers; advisers, consultants and other professional experts; employees or contact persons of data exporter's prospects, customers, business partners and vendors; business partners and vendors of data exporter (who are natural persons); and data exporter's users authorized by data exporter to use the software and related services.

Categories of Data
The Personal Data Processed may concern the following categories of data:
Application Use Data (e.g. log-files); identification data and employee master data (which may include title, name, address, telephone number, fax number, company address, email address); cookies and session information; goods and services provided – products purchased, products shipped or downloaded, payments processed; internet protocol (IP) address and other computer identifiers; contact details (e.g. telephone, e-mail); contract master data and customer history (e.g. contractual relationship, interest in products or contracts); billing and payment data; planning and management data; user-provided content; and other, as described in the Agreement.

SCHEDULE 2

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1
Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:
(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and
(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer") have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2
Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3
Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
(ii) Clause 8 - Clause 8.1(b), 8.9(a), (c), (d) and (e);
(iii) Clause 9 - Clause 9(a), (c), (d) and (e);
(iv) Clause 12 - Clause 12(a), (d) and (f);
(v) Clause 13;
(vi) Clause 15.1(c), (d) and (e);
(vii) Clause16(e);
(viii) Clause 18 - Clause 18(a) and (b);

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4
Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5
Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6
Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 - Optional
Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8
Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non- compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9
Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub- processors in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub- processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub- processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10
Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11
Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

   (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

   (ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12
Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13
Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14
Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15
Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

<u>SECTION IV – FINAL PROVISIONS</u>

Clause 16
Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17
Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Data Exporter's Member State.

Clause 18
Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the Data Exporter's Member State.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX TO THE STANDARD CONTRACTUAL CLAUSES

ANNEX I

A. LIST OF PARTIES

Data exporter(s): James Madison University

Name, Surname:
Position:
Email:

Signature:
Date: 4/20/2022

Data importer(s): Cherwell Software, LLC

Name, Surname: Al Crews
Position: VP, Americas EXM Sales
Email: al.crews@ivanti.com

Signature: Al Crews 4/16/2022
Date:

B. DESCRIPTION OF TRANSFER

The personal data transferred concern the following categories of data:

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data:

None

Processing operations

The personal data transferred will be subject to the following basic processing activities:

Provision of IT software licensing, support services and implementation, whether on-premises or as a hosted SaaS solution, regarding the administration and facilitation of essential business processes in the field(s) of unified endpoint management, IT service management, IT asset management, security, reporting and analytics, and supply chain.

IT services include the use of software as an on-premise installation or a SaaS solution including installation of modules (including without limitation, incident, change, asset, configuration and release management modules); self-service and service catalogues; support and maintenance including, without limitation, remote access; and patches, app control, endpoint/mobile security and privilege management.

C. COMPETENT SUPERVISORY AUTHORITY

The Supervisory Authority of the Data Exporter's Member State.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

The following describes the technical and organizational security measures implemented by Processor:

Security Awareness Training
Processor has security awareness training which includes mandatory security training about the handling and securing of confidential information and sensitive information such as personally identifiable information, financial account information, and health information consistent with applicable law, and periodic security awareness communications and security courses that focus on end-user awareness.

Security Policies and Procedures
Processor has information security, use and management policies which dictate the actions of employees and contractors regarding appropriate use, access to and storage of confidential and sensitive information; restrict access to confidential and sensitive information to members of Processor's workforce who have a "need to know" such information; prevent terminated employees from accessing Processor's information post-termination; and impose disciplinary measures for failure to abide by such policies. System access to Processor resources denied unless specifically assessed and access granted. Processor performs background checks of its employees at time of hire, as permitted by law.

Physical and Environmental Access Controls
Processor limits physical access to its information systems and facilities using physical controls (e.g., coded pass access) that provide reasonable assurance that access to its data centers is limited to authorized individuals and employs camera or video surveillance systems at critical internal and external entry points. Processor applies air temperature and humidity controls for its data centers and protects against loss due to power failure.

Logical Access Controls
Processor employs logging and monitoring technology to help detect and prevent unauthorized access attempts to its networks and production systems. Processor's monitoring includes a review of changes affecting systems' handling authentication, authorization, and auditing; privileged access to Processor's production systems.

Vulnerability Management
Processor regularly performs vulnerability scans and addresses detected vulnerabilities in accordance with their risk. Processor products are also subject to periodic vulnerability assessment and penetration testing.

Disaster Recovery and Back-up Controls
Processor performs periodic backups of production file systems and databases according to a defined schedule and maintains a formal disaster recovery plan for the production cloud data center, including regular testing.

Cyber Incident Response Plan
Processor employs an incident response plan to manage and minimize the effects of unplanned cyber events that includes procedures to be followed in the event of an actual or potential security breach, including: an internal incident response team with a response leader; an investigation team performing a root causes analysis and identifying affected parties; internal reporting and notification processes; documenting responsive actions and remediation plans; and a post-incident review of events.

Storage and Transmission Security
Processor employs technical security measures to guard against unauthorized access to Processor data that is being transmitted over a public electronic communications network or stored electronically.

Secure Disposal
Processor employs policies and procedures regarding the disposal of tangible and intangible property containing Processor data so that Processor data cannot be practicably read or reconstructed.

Risk Identification & Assessment

Processor employs a risk assessment program to help reasonably identify foreseeable internal and external risks to Processor's information resources and determine if existing controls, policies, and procedures are adequate to address the identified risks.

Vendor & Services Providers

Third-party service providers or vendors (collectively, "Suppliers") with access to Processor's confidential information are subject to risk assessments to gauge the sensitivity of Processor's information being shared. Suppliers will be expected to comply with any pertinent contract terms relating to the security of Processor data, as well as any applicable Processor policies or procedures. Periodically, Processor may ask a Supplier to re-evaluate its security posture to help ensure compliance.

Schedule 2 : Processor -

SubProcessors Cherwell Software, LLC

(rev April 2022)

NAME	LOCATION	FUNCTION
Cherwell Software Limited	United Kingdom	Product and Support
Ivanti U.K. Ltd	United Kingdom	Product and Support
Ivanti, LLC	United States	Product and Support

2nd Level Subprocessors of Cherwell Software, LLC

NAME	LOCATION	FUNCTION
Amazon AWS	USA	Cloud computing platform
Azure	USA	Cloud computing platform
Cloudflare, Inc.	Global	Web Application Firewall in all regions
Critical Start	USA	SIEM services
TalkDesk, Inc	Global	Cherwell utilizes Talkdesk's enterprise cloud contact centre
Microsoft	Global	Cherwell leverages the Microsoft Office 365 suite of applications and services within its organisation
Palo Alto Networks	Global	NextGen network firewall and endpoint security
Dynatrace LLC	USA	Monitoring Platform
LogicMonitor	USA	Monitoring Platform
CrowdStrike	Global	Endpoint and Cloud Workload Protection
Atlassian	Global	Multiple services, including status page, wiki
Beyond Trust	USA	Remote support, session security
New Relic	Global	Monitoring Platform
SalesForce	USA	CRM
Slack	USA	Messaging
Okta	Global	Identity Provider
Hosted FTP	USA	File transfer to and from Customer
EraSearch	USA	Monitoring Platform