EXHIBIT
"A"
UNIVERSITY OF ALASKA PURCHASE ORDER
CONFIDENTIALITY AND PRIVACY
REQUIREMENTS

1. **Definitions**: When used in this document, the following definitions shall apply:

Confidential Information - Personally Identifiable Information, Proprietary Information, and any other information marked "Confidential," provided by, or on behalf of the Buyer, in any form, including without limitation oral or written (paper or electronic) whether presented in text, graphics, charts or other formats.

Personally Identifiable Information ("PII") - Information relating to an individual that reasonably identifies the individual and, if compromised, could cause harm to that individual or to Buyer. Examples may include, but are not limited to: Social Security Numbers, credit card numbers, bank account information, student grades or disciplinary information, salary or employee performance information, donations, patient health information, information Buyer has promised to keep confidential, and account passwords or encryption keys used to protect access to PII. PII shall not include information that can not reasonably be used to identify the individual to whom it pertains.

Proprietary Information ("PI") - Data, information, or intellectual property in which the Buyer has an exclusive legal interest or ownership right which, if compromised could cause harm to Buyer. Examples may include, but are not limited to, business planning, financial information, trade secret, copyrighted material, and software together with comparable material from a third party when the Buyer has agreed to keep such information confidential.

Service Provider – The Supplier under the Purchase Order is a Service Provider hereunder.

In General: Service Provider agrees to maintain strict confidentiality concerning Confidential Information in accordance with the requirements and conditions set forth in this Section.
Exclusions: These requirements shall not apply to any information or data which:

A. is lawfully possessed by Service Provider prior to entering into this Agreement;
B. shall be lawfully acquired by Service Provider in circumstances or in a manner not resulting from, or related to, this Agreement or the performance of the Services;
C. becomes part of the public domain in any manner other than the publication thereof in violation of this Agreement or otherwise unlawfully;
D. is disclosed by Service Provider with the prior written approval of the Buyer; or
E. is otherwise required by applicable law to be disclosed by Service Provider (but then only to the extent that, and only to the recipient or recipients to whom or which such disclosure is required; and only after Buyer has failed to obtain a protective order or other appropriate relief governing disclosure of the data within 10 days after notice from Supplier of any disclosure request).

2. **Property of Buyer**: Confidential Information shall remain the sole property of Buyer. Service Provider expressly acknowledges and agrees that Service Provider has no property right or interest whatsoever in any such data.

3. **Security Safeguards**: Service Provider shall maintain adequate administrative, technical and physical safeguards against unauthorized access, use, or disclosure of Confidential Information. This requirement includes but it is not limited to, the following components.

A. Confidential information may only be stored on electronic computing devices that are current in their anti-virus software and security patches and that are protected by a firewall.
B. All access to confidential information electronically shall be via a unique user ID
C. and unique password that is not shared with others.
D. Confidential information shall not be downloaded to a portable device, such as Laptop computers, PDAs and USB drives, unless such data is protected with strong encryption.
E. Confidential information transmitted electronically must be encrypted in transmission, unless otherwise authorized by the Buyer.
F. Any use or handling of Social Security Numbers must be specifically approved by the Buyer.
G. Confidential information shall not be removed from the Service Provider's work site unless such removal is authorized by the Buyer as necessary for Agreement related purposes.
H. When Confidential Information is no longer required to perform services required under this Agreement, and is no longer required to be maintained by applicable law or the terms of this Agreement, the Serivce

Provider shall securely destroy such information and provide written confirmation to the Buyer.

I. If Service Provider retains backups of Confidential Information, such backups shall be maintained in conformity with these Security Safeguards.

J. Any question regarding the applicability of or interpretation of these requirements must be directed to Buyer's Information Security Officer or Chief Information Officer.

4. **Compliance**.

A. Laws. Service Provider shall comply with all applicable laws, ordinances, statutes regulations and other requirements established by federal, state and local governmental authorities regarding privacy and security protections for Confidential Information. Applicable statutes may include but are not limited to the Family Educational Rights and Privacy Act of 1974 (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), the U.S. Department of State International Traffic in Arms Regulations (ITAR) 22 CFR 120- 130, U.S. Department of Commerce Export Administration Regulations (EAR) 15 CRF 730 – 774, the Gramm-Leach-Bliley Act (GLBA Pub.L. 106-102, 113 Stat. 1338), and the Alaska Personal Information Protection Act (AS 45.48.010).

B. **Right to audit**. The University of Alaska, at its expense, will have the right to audit all aspects of the service provider's service, operations and partners with appropriate confidentiality agreements in place protecting the provider's intellectual property and/or trade secrets. Service providers, at their expense, have the same right to audit University of Alaska systems, operations and procedures. Notice of intent to audit and negotiation of employee time costs will take place before any audit activity requiring the cooperation of the audited party. Other.

C. Service Provider shall comply with the Payment Card Industry Data Security Standard, as applicable.

D. Export controls: Export controlled software, data and/or copies will at all times reside in the United States.

5. **Use and Disclosure Limitation**: Service Provider shall not use, provide, trade, give away, barter, lend, sell, or otherwise disclose Confidential Information, and shall not make any copies of such data or any type whatsoever, in readable or encrypted form, or in individually identifiable or aggregate form, except

A. as necessary for the services described in this Agreement to be performed; or

B. as expressly permitted by Buyer in a separate writing.

6. **Restricted Access**: Service Provider shall only permit access to Confidential Information acquired by Service Provider in connection with this Agreement, and only to employees, agents or independent contractors of Service Provider (1) who are directly involved in performing the Services for the Buyer and have a specific need to know such information, and (2) who have entered into written confidentiality agreements which impose, or are otherwise bound by, restrictions on the Confidential Information at least equivalent to those imposed under this Agreement.

7. **Breach**: Service Provider shall immediately report to Buyer any unauthorized access, use, disclosure, modification, or destruction of Buyer's Confidential Information or interference with system operations in an information system containing Buyer's Confidential Information ("Breach") of which Service Provider becomes aware. Breach notification to individuals who's identities may have been compromised is the responsibility of the party who's systems, networks or services are compromised and will take place in accordance with Alaska Statute 45.48.010 - .090.

8. **Remediation/ Mitigation**: When Service Provider learns of a Breach it shall (1) use best efforts to determine the scope and nature of the Breach, (2) work with the Buyer, in light of the circumstances and applicable law, to determine what risks are posed by the Breach and whether and how those persons whose data was accessed, acquired or disclosed should be notified, and (3) restore the reasonable integrity of the data system which hosts the Buyer's Confidential Information without compromise to forensic investigation.

9. **Service Levels:** The Buyer has the follow established service levels; Critical, Important, Routine.

Critical - 24x7x365 availability of service with required/negotiated vendor support hours for services incorporated into university operations Availability: 24 hours a day, 7 days a week, 365 days a year with the exception of scheduled maintenance not to exceed 2% of annual potential uptime (630,720 seconds or 7.3 days annually). Measurement: The vendor will report annually service uptime for the previous year prior to contract/subscription/service/license renewal in "day : hour : second" format if it is not readily available within the service already. For transactional services failed, rejected or otherwise un-completed transactions will be recorded and reported. All measurements will be taken from the Buyer's site. Reporting: Reporting will be on a quarterly basis. Performance: The service operates as agreed to.
Important - 8x5 M-F business hours availability with vendor support available, outages of the service can be tolerated for 1 hour. Availability: 24 hours a day, 7 days a week, 365 days a year with the exception of scheduled maintenance not to exceed 5% of annual potential uptime (1,576,800 seconds or 18.25 days annually). Measurement: The vendor will report annually service uptime for the previous year prior to contract/subscription/service/license renewal in "day : hour : second" format if it is not readily available within the service already. For transactional services failed, rejected or otherwise un-completed transactions will be recorded and reported. All measurements will be taken at the Service Provider's site. Reporting: Reporting will be on an annual basis. Performance: The service operates as described.
Routine - best effort or break/fix warranty support with no time commitment or sensitivity Availability: 9 hours a day, 5 days a week, 365 days a year with the exception of scheduled maintenance not to exceed 5% of annual potential uptime (1,576,800 seconds or 18.25 days annually). Measurement: The vendor will report annually service uptime for the previous year prior to contract/subscription/service/license renewal in "day : hour : second" format if it is not readily available within the service already. For transactional services failed, rejected or otherwise un-completed transactions will be recorded and reported. All measurements will be taken from the Service Provider's site and subject to service capability. Reporting: Reporting is not required. Performance: The service operates as described.

A. Unless noted otherwise on the line below all services will are established at the service level Important.
B. In the event none of the these three pre-defined services levels covers the requirements of the Buyer a custom level can be appended and titled "Exhibit B, Service Level Agreement"

10. **Indemnification**: To the fullest extent permitted by applicable law, Service Provider shall indemnify, defend and hold harmless Buyer, its Board of Regents, officers and employees (individually, an "Indemnified Party", and collectively, the "indemnified Parties"), from and against any and all loss, expense, damage, claim, demand judgment, fine, charge, lien, liability,

action, cause of action, or proceedings of any kind whatsoever (collectively, "Claims") suffered or incurred by the Indemnified Parties (including reasonable attorney's fees and expenses) arising directly or indirectly in connection with any unauthorized access, use or disclosure of Buyer's Confidential Information by Service Provider. With regard to Service Provider's obligation to defend, the Buyer shall have the right to select the legal counsel whom Service Provider shall provide to defend any Indemnified Party, subject to Service Provider's approval of the qualifications of such legal counsel and the reasonableness of counsel's hourly rates as compared to the rates of attorneys with similar experience and qualifications in the relevant area of legal expertise and in the jurisdiction where the Claims will be adjudicated. If the Buyer elects, in its sole discretion, to retain separate legal counsel, in addition to or in lieu of the counsel to be provided by Service Provider, then all costs and expenses incurred by the Buyer for such separate counsel shall be borne by the Buyer and the Service Provider shall reasonably cooperate with the Buyer and its separate legal counsel in the investigation and defense of any such claim or action. Service Provider shall not settle or compromise any claim or action giving rise to Claims in a manner that imposes any restrictions or obligations on Buyer without Buyer's prior written consent. If the Buyer elects to require that Service Provider defend a Claim pursuant to this paragraph, and Service Provider fails or declines to assume the defense of such Claim within thirty (30) days after notice thereof, the Buyer may assume the defense of such Claim for the account and at the risk of Service Provider, and any Liabilities related thereto shall be conclusively deemed a liability of Service Provider. Service Provider agrees that if it is named as a party in an action that results from or arises out of any unauthorized access, use or disclosure of Buyer's Confidential Information, and Buyer is not named as a party to such action, Service Provider shall, immediately upon receiving notice of such action, notify Buyer of the action. The indemnification rights of the Indemnified Parties contained herein are in addition to all other rights which such Indemnified Party may have in contract, at law or in equity, or otherwise. The Buyer accepts no liability for Students accepting, complying or non-compliance with the Service Provider's terms and conditions.

11. **Return of Confidential Information:** Upon the expiration or earlier termination of the Agreement or at the request of Buyer, Service Provider will either (1) at its own expense, immediately return to Buyer all Confidential Information embodied in tangible form, whether or not reduced to such form by Service Provider including all copies thereof, or (2) at the Buyer's option, certify in writing to Buyer that all such Confidential Information has been destroyed, except that Service Provider may retain Confidential Information to the extent that retention is required by law or is needed to document performance under this Agreement.

12. **External Request for Confidential Information**: In the event that the Service Provider receives a request for Confidential Information by subpoena or other legal process or from a court, governmental authority, accrediting agency, or other third party, the Service Provider shall give prompt written notice to the Buyer in order to allow the Buyer the opportunity to seek a protective order or to take other appropriate action to protect the Confidential Information.

13. **Service Provider Designation:** Service Providers who receive or have access to FERPA covered student education records or information are designated school officials with a legitimate educational interest.

14. **Terms and Conditions:** These, and all other, terms and conditions are fixed for the duration of the contract length, licensing period and/or lifetime of the current relationship between the Service Provider and Buyer. In the event re-negotiation is appropriate and desirable by both the Service Provider and Buyer 90 days notice is required. The notice will include the current language of the agreement, proposed language, the reason for the change and summaries of impact to the service, service level, cost, security and liabilities.

15. **Conflict resolution**. In the event any provisions embodied in this exhibit are found to be conflicting with other agreement language the more restrictive provision will apply.

16. **Accessibility.** Vendor represents and warrants that deliverables comply with Web Content Accessibility Guidelines (WCAG) Version 2.0 Level AA, and agrees to provide written documentation verifying accessibility, to promptly respond to and resolve accessibility complaints received from the University, and to indemnify and hold the University harmless in the event of claims arising from inaccessibility.

Exhibit B - University of Alaska
Information Resources Proposal Review

Date _____

It is likely that the University of Alaska already owns, promotes, maintains and secures the services you are seeking. Many of the services are state of the art cloud or virtual services, delivered as a substantial discount off rates available to the public or individual departments.

This review process is reserved for the rare case in which UA is unable to internally meet or externally broker an information service required for the conduct of University business.

As a first step, please contact your local Office of Information Technology at your University before submitting this form. You may discover a suitable service already in production and available to you, or you may be able to secure the assistance of IT staff in correctly completing this form.

The purpose of the review is to ensure that a) University data have appropriate protection(s); b) Information Resources controls and compliance requirements are met, and (c) information technology and business objectives are properly aligned. An information resources review must be completed for:

- Any purchase booked to accounts code 3221, 3222, 4014, regardless of the funding source;
- Any software, web or professional service which results in ***sensitive institutional or student data being stored in, transmitted through, or manipulated by non-UA hosted systems***.

Please include any contracts, terms of use, or end user licensing agreements with this form.

Unit/Department: _____ Contact Name _____ eMail: _____

Purpose / Background (proposal scope):

Alignment to University Mission:

Schedule / Time Constraints:

What start-up resources required (funding, staffing, equipment and facilities)

University of Alaska
Information Resources Proposal Review

Date _____

What on-going resources are required?

Does this proposal require access, storage or transmittal of any sensitive student, employee or other institutional data? [ ] no [ ] yes

If so, please describe.

Does this proposal involve services provided by a non-UA provider? [ ] no [ ] yes

If so, who?

Terms and Conditions reviewed by General Council? [ ] no [ ] yes, date_____

Reviewed by UA Chief Security Officer? [ ] no [ ] yes, date_____

Submitted by: Dean/Director: _____

Review by IT: _____ Date: _____

IT Comments: