University of Alaska

Cloud Computing Guidelines

UNIVERSITY of ALASKA

Many Traditions One Alaska

Revised August 2016

Guidelines for the Use of 3rd Party or Cloud Computing Services at the University of Alaska

Why is this important to me?

If you manage a service and plan to outsource one, or are already, and the service will house key university data regarding students, staff, faculty, finances or research, you need to read the remainder of the guide.

Cloud computing, shared services, vendor hosted solutions are becoming more common in information technology and often bring advances in capability and capacity to organizations. BUT, they bring challenges as well. What we, as University of Alaska departments and organizations, once controlled exclusively, now involve relationships that need management to insure they work effectively and that the best interests of the University are managed well. ***Failure to properly understand and manage cloud computing relationships can result in significant institutional and individual liability, including criminal charges. It is essential that you seek review of any contract or agreement for cloud computing services as outlines in this document.***

All outsourced or vendor hosted contracts and terms and conditions should be reviewed by your Chief Information Officer, IT Security staff and the University Office of General Counsel, prior to entering into an agreement.

They will review:

- governance,
- information and data security,
- vendor qualifications,
- contract suitability,
- and risk assessment

All of these elements need to be in order before engaging in a formal relationship to avoid getting stuck with what you do not want, did not intend and other surprises after it is too late. To do this we need to be familiar with the issues and consequences of:

- our choices,
- what needs to be considered,
- organizational needs,
- types of data,
- methods of protection,
- liability and limitations,
- service level,
- and performance metrics.

Table of Contents

Cloud Computing

The Internet is sometimes referred to as the "cloud". Cloud computing is the array of Internet-based services, often available to the public, for gathering, storing, processing and sharing information. Some cloud services, such as those offered by Apple, Microsoft, or Google, may be free to end-users. For the general user who wants a convenient, Internet-based solution for storing or sharing personal information, cloud computing may provide a reasonable option. University departments seeking such services need to be aware that all services need to adhere to security policy and standards as well as confidentiality laws. This document identifies security and data privacy concerns that must be considered when purchasing or using cloud- computing services at the University. In this context, the University is a cloud-computing consumer.

Examples

There are numerous types of cloud computing services available on the Internet that may be appropriate for individual or University use. Some examples of public cloud services are:

- *External Email Services* (e.g., Hotmail, Gmail, O365, etc.)
- *Chat & Instant Messaging Services* (e.g., Yahoo, AIM, MSN, IRC, etc.)
- *Social Networking Services* (e.g., Twitter, Facebook, Instagram,Tumblr, etc.)
- *Hosted Application Services* (e.g., Google Docs, PageUp, etc.)
- *File Sharing* (e.g., Dropbox, Box.net , etc.)
- *Virtual Machines* (e.g., GoGrid and Amazon Web Services Elastic Compute Cloud and Azure are commercial web services that allow customers to rent any number of virtual computers upon which they can load and run their own software applications.)

Your Responsibility

As a member of the University community, be aware of the sensitivity or conditional uses of the data you generate, have access to, or receive. Should you ever need to store or share University information in a manner not currently provided within the University's computing environment, always consider its sensitivity before doing so.

Storage and transmission of sensitive information should be limited to cloud computing resources protected by the University's physical, technical and/or administrative processes for safeguarding data. If you are unsure of what is appropriate you can contact your campus CIO regarding what is and is not safe. When considering cloud computing services that may be entrusted with University of Alaska data or communication tools working with IT security staff to help understand and navigate issues of security and confidentiality is a good idea. In the event the service is being purchased, General Counsel, purchasing, and risk management offices may also need to be engaged to review, negotiate contracts and/or determine liability. Some data comes with licensing or other usage agreements that need to be known and followed. These can include software, commercial data products or information received by virtue of partnerships.

Any time data fitting the Universities definition of internal use or restricted is going to be exchanged with or access given to vendors, service providers, contractors, organizations, etc. outside the University the UA Information Security Officer is be notified in the process of making arrangements for this exchange or access along with the data custodian.

Units or departments that are considering using cloud-computing services should contact their purchasing and IT departments, as well as University General Counsel, prior to entering into any contract. The Institutional Review Board (IRB) should be consulted if a unit or department is planning to share human subjects' research data within a cloud computing service.

Considerations

Has the external cloud computing resource been approved for use within the University?

If in doubt ask your local information security staff or campus CIO as there can be significant hidden or duplicated cost and risk.

Is there an alternative cloud computing resource already available within the University?

This can include Google Apps for Education (email, chat, document sharing, etc.) or other resources that can provide the functionality desired.

Does the cloud service have a contractual relationship with the University?

This will be a good indicator of an approved cloud computing resource. However discretion still needs to be used with respect to what kind of data you plan to introduce to the service.

How sensitive is the information you intend to give to the provider of a cloud based service?

Often when data leaves the University it is viewable by administrative and other staff at the service provider. Sensitive information regarding staff, students, affiliates, agreements, correspondence etc. should not be hosted off University IT resources or with services not contractually engaged.

Do you have the authority to make decisions about how public or private the data is?

Often there are agreements, governing regulation, University policy or legal requirements that need to be reviewed and provided for in disclosure of sensitive or restricted data. If you are unsure of what might be required it never hurts to ask. Your campus CIO or Information Security Officer can identify requirements and risks that need to be provided for and assist with their implementation.

Is it personally identifiable information?

Personally identifiable information (PII) according to University Regulation R05.08.023 is the combination of a persons first and last name or first initial and last name when either is accompanied by any of the following:

- social security number;
- driver's license number or state identification card number;
- the individual's account number, credit card account number, or debit card account number in combination with any required security code, access code, or password that would permit access to an individual's financial account;
- passwords, PINs, or access codes for financial accounts.

PII placed outside the University's control puts the University and the individual(s) it identifies at risk. Placing it in cloud computing resources not provided by the University is inconsistent with the protection the University and applicable law affords PII. You could create a large expense and embarrassment for the University and yourself if required confidentiality is lost.

Could the data's exposure create liability or image problems for the University?

If the answer to this is yes, cloud computing services without University approval are not suitable for this material. Additionally it may cause the University to have to notify the state and individual(s) involved in accordance with the Alaska Personal Information Protection Act (AS 45.48.010 - .090).

Guidelines

There are a number of information security and data privacy concerns regarding use of cloud computing services at the University. They include:

- Loss of University control of data, leading to a loss of security or reduced effectiveness
- Loss of privacy of data, potentially due to aggregation with data from other cloud consumers
- University dependency on a third party for critical infrastructure and data handling processes
- Potential security and technological defects in the infrastructure provided by a cloud vendor
- No University control over the third parties that a cloud vendor might contract with
- Loss of the University's own competence in managing the security of computing infrastructure

There are also legal concerns with the use of cloud computing. A cloud-computing relationship is governed by contract law. Disputes over the terms of the contract could be costly and lengthy to resolve. Since cloud-computing relationships are governed by contract, it is important that the following items be considered prior to entering into any contract to use or purchase cloud computing services:

- Data definition and use
- General data protection terms
- Compliance with legal and regulatory requirements
- Data access and handover process at the end of the relationship
- Breach liability assignment
- Service level expectations and performance metrics.

All of these items should be addressed in a cloud-computing contract, as well as items that are particular to the specific infrastructure or application services that are used or purchased.

Data Definition and Use

Both the University and cloud-computing vendor must understand the type of data that they might transfer back and forth because of their relationship. A contract must have clear terms that define the data owned by each party and the stages of data use, transmission and storage. The parties also must clearly define data that must be protected, whose custody it is in at various stages and an assignment of liability at each stage.

The contract must specifically state what data the University owns. It must also classify the type of data shared in the contract according to the University's classification schema: Public, Internal Use, or Restricted.

Units must exercise extreme caution when sharing University internal-use or restricted data within a cloud computing service. The contract must specify how the cloud-computing vendor can use University data. Vendors cannot use University data in any way that violates the law or University policies.

There are times when the University requires access to data in the accounts or under the control of an identity they sponsored in a cloud computing services. Data ownership and the University's right to access data regardless of what user or identity it is associated with needs to be established. The process for obtaining this kind of access needs to be detailed in procedure.

General Data Protection Terms

The University must specify particular data protection terms in a contract with a cloud-computing vendor. The University does this to create a minimum level of security for University data. A minimum level of security ensures that the University data is kept confidential, is not changed inappropriately, and is available to the University as needed.

The University will consider the following contract terms to ensure a minimum level of information security protection:

- Data transmission and encryption requirements
- Authentication and authorization mechanisms
- Intrusion detection and prevention mechanisms
- Logging and log review requirements
- Security scan and audit requirements
- Security training and awareness requirements
- Establish breach responsibility boundaries
- Data disposition
- Service termination terms

Contracting parties in consultation with their associated campus IT department can use resources developed by the National Institute of Standards and Technology (NIST) to make sure that a contract includes the appropriate controls. The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) has also prepared information security controls guidance.

Compliance with Legal and Regulatory Requirements

The University has many federal laws that it must follow, these include 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 and the Gramm-Leach-Bliley Act (GLBA Pub.L. 106-102, 113 Stat. 1338), and the Americans with Disabilities Act (ADA) of 2008 (P.L. 110-325)

State laws may also affect a relationship with a cloud-computing vendor. For instance, in Alaska the University must follow rules about protecting Social Security and credit card numbers and follow requirements for notification of a breach (AS 45.48.010 Alaska Personal Information Protection Act). The actions of University employees are also governed by the Alaska Executive Branch Ethics Act.

A relationship with a cloud-computing vendor may also be impacted by private industry regulations. For example, units at the University that accept credit cards also must follow the Payment Card Industry (PCI) Data Security Standard (DSS) issued by the major credit card companies.

Finally, cloud-computing services that use, store, or process University data must also follow applicable University policies and regulations. Such policies may include Information Technology policies and the University's data handling requirements.

At a minimum, a cloud-computing contract should address the following regulatory requirements:

- FERPA language if student data is used or transmitted between the parties (units or departments will also need to notify the Office of the Registrar if they plan to share student information within a cloud computing service).
- GLBA language if financial data is used or transmitted between the parties (units or departments will also need to notify the Chief Information Security Officer they plan to share financial information within a cloud computing service).
- HIPAA language if health information is used or transmitted between the parties (units or departments will also need to notify the Chief Information Security Officer at the University if they plan to share health information within a cloud computing service).
- ADA language to ensure compliance for individuals with disabilities.
- Language protecting the intellectual property rights of the University.

- Language requiring the cloud-computing vendor to notify the University, in advance and prior to responding, if it receives any court order, subpoena, discovery request, or any request of any kind seeking access or production of any University data.
- Language requiring a cloud-computing vendor to cooperate with security incident investigation so that the University can meet its own regulatory notification requirements.
- Language requiring a cloud-computing vendor to assist the University with third party litigation that occurs because of the cloud-computing relationship.
- Language outlining a cloud computing vendor's obligation to preserve data for a specified period of time and indefinitely in the event of litigation to which hosted data may be related.
- Language requiring a cloud-computing vendor to notify the University if the security of any cloud-computing service is compromised in a breach and any University data is potentially exposed.
- Language requiring the cloud-computing vendor to assist with entering into a cloud services contract and exiting a cloud services contract.
- Language regarding contract termination and return or destruction of University owned data.

Each cloud-computing contract presents unique legal and regulatory issues. Before entering any contract, you should consult with the University General Counsel and Chief Information Security Officer to ensure compliance.

Accessibility: If the Cloud solution includes any end-user-facing human interface, such as an end-user device software component or web site form, file upload system, etc. the Contractor hereby warrants that the products or services to be provided under this agreement comply with the accessibility guidelines of "Section 508 of the Rehabilitation Act of 1973" as amended as of the date of this agreement, and the "Web Content Accessibility Guidelines (WCAG) 2.0" published by <http://www.w3.org/TR/WCAG20/>www.w3.org.

If the solution includes any end-user-facing human interface, such as an end-user device software component, web pages or site, video or audio playback, file upload system, mobile device components, etc., the Contractor agrees to promptly respond to and resolve any complaint regarding accessibility of its products or services which is brought to its attention and vendor further agrees to indemnify and hold harmless the University or any university entity using the Contractor's products or services from any claim arising out of its failure to comply with the aforesaid requirements.

The University, at its discretion, may at any time test the vendor's products or services covered by this agreement to ensure compliance with Section 508 and WCAG 2.0. Testing that results in findings of non-compliance, shall result in a 25% reduction in the total cost of the products and/or services covered by this agreement if the non-compliance is not corrected within 30 days of being reported to the vendor in writing. The University will pay all withheld amounts to the vendor upon correction of the non-compliance and acceptance. Said acceptance not to be unreasonably withheld.

Failure to comply with these requirements shall constitute a breach and be grounds for termination of this agreement and a pro-rated refund of fees paid from the University for the remainder of original contract period.

Data Access and Handover Process at the End of the Relationship

Before a relationship is established the conditions under which it can be ended, the responsibilities of involved parties and steps to disengage should be defined. Without these pieces the process of ending a relationship can become daunting and costly. Starting with a defined set of conditions either side can use to initiate discontinuation of services reduces the unknowns. The following should be established up front and before engagement:

- Who can elect termination of service and how notice is given.
- Elements of the disentanglement such as how reacquisition of real, data or intellectual property is handled.
- Assignment of duties of the University, the vendor and/or a new cloud-computing

service vendor.
- Time requirements for responses or actions that need to be taken.
- Responsibility for costs associated with disentanglement.
- Procedures for maintaining the integrity of data or intellectual property throughout the process, and any penalties for not doing so and how integrity is to be established.

Breach Liability Assignment

When entrusting a 3rd party with access to University data the process of transferring, storing and processing that data needs to be evaluated and minimum levels of assurance established for the data in each of those states. Establishing who has possession of it and the responsibility to protect it needs to be done before an adverse event involving University data takes place. Ideally the cloud computing service vendor should accept liability for any data loss that takes place on the systems, networks or applications they manage to deliver a service. Without General Counsel's approval an agent of the University should not agree to indemnify a cloud-computing vendor.

Service Level Expectations and Performance Metrics

When entering into a cloud-computing contract, it is also important to make sure that the contract specifies service level expectations and includes performance metrics. The University should consider the following contract terms to address service level and performance metrics:

- Language regarding service availability time and service outages
- Language regarding routine maintenance timeframes
- Language regarding hardware upgrades to cloud-computing services
- Language regarding software updates to cloud-computing services
- Language regarding changes to the cloud-computing services

Reference Material:

7 things you should know about…; Cloud computing http://net.educause.edu/ir/library/pdf/EST0902.pdf

University of Alaska Data Classification Standards http://www.alaska.edu/records/dataclass/

University of Alaska Board of Regents' Policy http://www.alaska.edu/bor/policy-regulations/

Alaska Personal Information Protection Act http://www.law.state.ak.us/consumer/4548.html

FERPA at University of Alaska http://www.alaska.edu/studentservices/ferpa/

HIPAA at University of Alaska http://www.alaska.edu/benefits/health-plan/hipaa-privacy/

Alaska Personal Information Protection Act Alaska Statute: AS 45.48
http://www.law.state.ak.us/department/civil/consumer/4548.html

Purdue University Cloud Computing Guidelines:
http://www.purdue.edu/securepurdue/bestpractices/Cloud%20Consumers.cfm

U.S. Department of Commerce Export Administration Regulations (EAR) 15 CRF 730 – 774

U.S. Department of State International Traffic in Arms Regulations (ITAR) 22 CFR 120- 130)

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.

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: