UNIVERSITY of ALASKA

Many Traditions One Alaska

Date: September 27, 2017

To: Karl Kowalski, IT Council Chair

From: Lisa Hoferkamp, Faculty Alliance Chair

Subject: Email Administrative Policy

The Faculty Alliance (FA) has reviewed the DRAFT Email Administrative Policy that was made available on August 22, 2017 and would like to submit the following for consideration.

The general sentiment of the FA is that the document requires a more balanced approach to workplace use of email. The document should state the rights and responsibilities of both users and providers, i.e. UA employees and the Office of Information Technology (OIT). Included in the document should not only be precise descriptions of user obligations but also equally precise descriptions of how those obligations may be met. Most users are unfamiliar with IT terminology thus may misinterpret directions provided on the current version of the policy. More specific to faculty users, assurances regarding privacy (especially with regard to FERPA) as well as free speech rights and intellectual property rights should be included in the policy. Finally, OIT's responsibility to provide useful, secure and reliable email service would be a positive addition.

An unedited version of FA comments are provided as comments in the copy DRAFT Email Administrative Policy found below.

Respectfully,

Lisa Hoferkamp

Lisa Hoferkamp
Chair, Faculty Alliance

DRAFT

University of Alaska Administrative Guidelines: Use of Email

1. Purpose The purpose of this document is to ensure that use of email at the University of Alaska is consistent with direction from the UA President, Board of Regents, and industry best practice.

Electronic Mail is a tool provided by the University and is a staple of correspondence used to to improve education and administrative efficiency. Employees have the responsibility to use this resource in an efficient, ethical and lawful manner. Use of University Email Accounts evidences the user's agreement to be bound by these guidelines.

Institutions & departments are free to make more restrictive guidelines, processes or procedures, consistent with UA policy and regulation, than are embodied below. Should a department’s practices be in conflict with the provisions below, these guidelines will supercede.

1.1. Scope This document applies to all employees of UA and any other individuals who use or maintain a University of Alaska provisioned email account.

2. Compliance Statement Complete listings of all University Policies and Regulation can be found here: https://www.alaska.edu/bor/policy-regulations/

2.1 Email System UA provides one email system for use by all employees. Institutions and departments are required to use this system as their primary system.

Use of alternate systems for subordinate purposes must be approved by the Information Resources Director and CISO.

Forbidding units from standing up their own email systems for customized purposes would drastically limit the sort of in-class demonstrations, system administration, and computer security training projects that we do in Computer Science.

2.2 Account Creation University Email Accounts are created based on the individual's official name as reflected in the UA official system of record (Banner). Requests for name changes to correct a discrepancy between an email account name and official University records will be processed, in which case the email account name will be corrected. This could be due to error or a person legally changing their name. Requests for mail aliases based on name preference, middle name, etc., may be evaluated on a case-by-case basis.

This policy does not agree with Title IX guidelines, which recommend allowing students to be called by their preferred name, and allow them to change that name.

Faculty, staff, or departments can request temporary email privileges for users outside of the University. Full time Faculty or Staff requesting these types of accounts will be required to submit user information, rationale for account, expiration date, & sponsor information. Such requests shall be approved by the

appropriate Director level manager.

2.3 Ownership of Email Data University email service is an information resource as defined in Regents' Policy and Regulation on Information Resources 02.07.020-094 for conducting UA business and will be managed as such. Therefore, data residing in said information resource are UA records and shall be classified and governed as an information/record asset per Regents' Policies 02.07.090-04 and subject to retention under Policy 05.08.022 and accompanying regulation 05.08.023.

2.4 Record Retention It is the responsibility of the employee to preserve University records, including those delivered via email or instant messages in a manner consistent with the UA records retention policy (Please refer to UA Records Retention policy 05.08.22):

1. Records that fall into a data classification that has a required retention lifecycle by

Regents' Policy or Law. 2. Records that contain knowledge of matters in which it can be reasonably anticipated that

a court action will be filed. 3. Records for which a subpoena has been served or notice of same has been given. 4. Records that are sought pursuant to an audit or similar pending or possible investigation.

In many cases, individual or departmental email accounts do not meet these standards. For additional guidance, departments should consult with their IT support organization.

2.5 Data Backup Email backup is the responsibility of the employee. UA only maintains backups for eDiscovery purposes.

This is not a rational policy: employees do not have the expertise, access, or technology support to provide real backups.

Evidently OIT is not set up to recover from accidental deletions; email is dumped as a large reformatted backup searchable by keyword.

2.6 Privacy and Right of University Access While the University will make every attempt to keep email messages secure, privacy is not guaranteed and users should have no general expectation of privacy in email messages sent through University Email Accounts. Under certain circumstances, it may be necessary for Information Resources Personnel or other appropriate University officials to access University Email Accounts (P02.07.060.D). These circumstances may include, but are not limited to, ("but are not limited to" is not a comforting phrase here. Would it be reasonable for OIT personnel to secretly examine and forward copies of emails sent between a faculty senate president and faculty union president regarding CBA negotiations?) maintaining the system, investigating security or abuse incidents or investigating violations of this or other University policies, or violations of the vendor's Acceptable Use Policy or the University's contracts with the vendor.

Consistent with the provisions set out in UA Regulation (02.07.064) Information Resources Personnel or University officials may access a University e-mail content in order to protect the privacy of data and communications, address a malfunction, maintain the secure and efficient operation of information resources or avoid potential legal liability relating to the operation of information resources. In the event that an employee will not, or can not, access the University Email Account him/herself for any reason (such as death, disability, illness or separation from the University for a period of time or permanently), e-mail content may be accessed upon supervisor request in consultation with General Counsel and Human Resources Director(s). Such access will be on an as-needed basis and any email accessed will only be disclosed to individuals who have been properly authorized, have an appropriate need to know, or as required by law.

All email users are bound by the appropriate acceptable use policy of both University of Alaska and the

current vendor. The vendor retains the right to access to the accounts for violations of its Acceptable Use Policy.

2.7 Appropriate Use and User Responsibility Highly sensitive information such as Social Security number, bank account information, tax forms, background checks, and sensitive research data should not be transferred unsecured via email. For guidance on transferring sensitive information securely, contact your local IT support office.

FERPA forbids transmitting or discussing grades over email. You are allowed to use Blackboard to transmit grades. Presumably you have to discuss them only in person, in the privacy of your office?

Technically FERPA does allow transmission of grades by email but institutions will be held liable if email is sent to anyone but the intended student, and email can be spoofed. But point taken. My understanding is that faculty to student communication via respective UA email accounts is considered "private." Many faculty accept homework and take-home exams by email and I think this could be considered sensitive information. Maybe not "highly sensitive" as stated here but I'm not sure the distinction.

Is this consistent with the faculty requirement that we discuss sensitive or protected information with students (e.g. grades) only through UA email?

Data that is controlled for export under United States Export Control laws shall not be stored or transmitted via email under any circumstance.

ITAR covers an enormous swath of information technology, many of which might reasonably be discussed in computer or engineering courses.

Individuals who communicate with persons in other countries may be subject to the laws of those other countries and the rules and policies on others systems and networks. Users are responsible for ascertaining, understanding and complying with the laws, rules, policies, contracts and licenses applicable to their particular uses.

Mass distribution of email via distribution lists, mail merge, or ‘‘reply all” features of email should be carefully considered and only used for legitimate purposes as per guidelines established by each University and the restrictions under State or Federal Law.

By Alaska law, University resources including email may not be used for partisan political purposes. Partisan political purpose is defined by law: anything done with the purpose of differentially benefiting or harming a candidate or potential candidate, political party or group. (See AS 39.52.120(b)(6).)

Users may not share passwords. Each individual is responsible for his/her account, including the safeguarding of access to the account. All email originating from an account is assumed to have been authored by the account holder, and it is the responsibility of that holder to ensure compliance with these guidelines.

Faculty, staff and students are expected to read email on a regular basis and manage their accounts appropriately. An email message regarding University matters sent from an administrative office, faculty, or staff member is considered to be an official notice. Students who choose to use another email system are responsible for receiving University-wide broadcast messages and personal mail by checking the University's official email system and the University’s Website or setting up and maintaining message forwarding, as appropriate.

2.8 Departmental Accounts Requests for shared departmental accounts will be accommodated, but require a designation of an account holder or holders, who will administer the addition, deletion, or modification

of names within the account, as well as manage the account as per these guidelines.

2.9 Personal Email Accounts Employees may not use non-university issued email accounts to conduct University of Alaska business or store University email records. University employees and students should take no action based on decisions or directions communicated to them from non-university email accounts.

2.10 Inappropriate Use Online conduct, including use of email, is governed by UA policy and regulation including R02.07.050. Users should familiarize themselves with these guidelines. A non-exhaustive set of prohibited use is provided below. Users receiving such email should immediately contact their campus IT support organization, who in certain cases may also inform Public Safety, Human Resources, The Dean of Students or The Office of General Counsel.

The exchange of any email content outlined below is prohibited:

● Infringes on another person's copyright, trade or service mark, patent, or other property right or is intended to assist others in defeating those protections;

● Violates, or encourages the violation of, the legal rights of others or federal and state laws;

● Is for any malicious, unlawful, invasive, infringing, defamatory, or fraudulent purpose;

● Intentionally distributes viruses, worms, Trojan horses, malware, corrupted files, hoaxes, or other items of a destructive or deceptive nature;

It seems reasonable to expect to discuss or distribute such things, with clear labels and cautions, when teaching a computer security course.

● Interferes with the use of the email services, or the equipment used to provide the email services, by customers, authorized resellers, or other authorized users;

● Alters, disables, interferes with or circumvents any aspect of the email services;

● Creates a risk to a person's safety or health, creates a risk to public safety or health, compromises national security, or interferes with an investigation by law enforcement;

● Improperly exposes trade secrets or other confidential or proprietary information of another person;

● Misrepresents the identity of the sender of an email.

● Using or attempting to use the accounts of others, with or without their permission.

This list is not intended to be exhaustive but rather to provide some illustrative examples.

2.11 Email Forwarding Employees may not blanket forward all their~~forward copies of~~ university email to be stored in another provider. This action may subject an employee to disciplinary action up to and including termination. Students and Alumni may forward email to other electronic mail service providers. In doing so it is agreed the University is not responsible for the security or privacy of the forwarded messages.

How do we determine whether the intent is to "store in another provider" a forwarded copy?

I agree that this is contradictory and ridiculously harsh. It also seems to not match up with the CBA and with the definition of tenure.

Above, we require employees to provide their own email backups. Here, we prevent employees from forwarding their emails to a backup email storage service. There is a contradiction here.

Rationale: if a student emails a faculty member their homework, and the faculty's email is all

forwarded to yahoo, both the faculty and university could have FERPA issues.

3. Non-Compliance Non-compliance with email administrative standards will be referred to the Information Resources Director, who may, in turn, refer matters to an employee's supervisor, the Provost, Human Resources and/or law enforcement. Disciplinary actions can include, but are not limited to, revocation of email accounts, reprimands, probation, expulsion or termination for the act of not complying or inability to perform vital functions related to course work or job duties.

This seems unnecessarily heavy handed, and does not appear to match up with the CBA-defined disciplinary process.

4. Best Practices Best practices are not requirements but options that can be taken or awareness that is important to communicate.

4.1 SPAM & Phishing All incoming email is scanned for viruses, phishing attacks and SPAM. Suspected messages are blocked from the user's inbox. Due to the complex nature of email, it is impossible to guarantee protection against all SPAM and virus infected messages. It is therefore incumbent

on each individual to use proper care and consideration to prevent the spread of viruses. In many cases, viruses or phishing appear to be sent from a friend, coworker, or other legitimate source. Do not click links or open attachments unless the user is sure of the nature of the message. If any doubt exists, the user should contact the Service Desk at helpdesk@alaska.edu

Phishing messages attempting to imitate University of Alaska login pages can be forwarded to helpdesk@alaska.edu where they may be added to the filter list.

5. Definitions SPAM is defined as unsolicited and undesired advertisements for products or services sent to a large distribution of users. Phishing is defined as the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.

6. Approval and Revisions Version 1.0 Approved August 9, 2017 by University of Alaska Chief Information Technology Officer, Karl Kowalski.

Resources Current Vendor's Use Policy http://www.google.com/a/help/intl/en/admins/use_policy.html