REGENTS' POLICY
PART V – FINANCE AND BUSINESS MANAGEMENT
Chapter 05.08 - Business Practices

P05.08.010. Printing Standards: General Statement.

Publications produced by and for the university will be simple, low in cost and consistent. Publications will be printed on recycled paper whenever it meets specific printing needs and will be printed on both sides of the paper. A publication with actual annual general fund production costs in excess of $1,500 will contain the disclosure statement if required by AS 44.99.210.

(08-19-94)

P05.08.012. Printing Standards: Printing at Private Facilities.

A university publication will be produced at a private sector facility located in the state unless:

A. the publication cannot be produced within the time limits established by the university by a private sector facility located in the state;

B. the technical requirements for the publication exceed the capability of private sector facilities located in the state;

C. the publication can be produced at less cost by the university; or

D. in- **Printing Regulations.**

lgating university regulation with printing standards designed to promote simplicity, and consistency in accordance with this policy, the president will consider the standards y the Department of Administration under AS 44.99.200 and will allow for exceptions ndards with written justification. The standards will not apply to publications used by rsity to develop a market for the university's services or products, publications intended for foreign or out-of-state use, programs for public ceremonies, or posters, or printed exempted by A.S. 44.99.240(1).

(08-19-94)

22. Records and Information Retention and Disposition

A. The president or his/her designees will retain and dispose of all correspondence, documents, records, and information which is stored on various media in accordance with university regulation.

B. To promote economy, efficiency, and the security of university records and information,

1. the length of time that records and information must be retained before disposing or archiving,

2. identification and protection of the university's vital records,

3. identification and protection of personally identifiable information maintained by the university

4. the systematic methods and procedures for purging and the destruction of records and information that are no longer operationally, legally, or fiscally necessary,

5. reducing the multiple copies of records, and,

6. archiving or the long-term inactive storage of selected records in computer readable form, digital imaging, on microfilm, microfiche, or other such cost or space saving methods.

(04-16-10)

UNIVERSITY REGULATION
PART V – FINANCE AND BUSINESS MANAGEMENT
Chapter 05.08 - Business Practices

R05.08.022 Records and Information Retention and Disposition

A. Purpose:

E. Legal Authority:

The Records and Information Management Program is the legal authority, designated by the Board of Regents and the president of the University of Alaska, to determine how long records and information must be retained. The Records and Information Management Office is responsible for developing records retention and disposition/destruction schedules that identify records created or received by the university. It is responsible for establishing standards relating to university business requirements and needs to ensure the legal legitimacy of university record and information management-keeping systems. The program counsels and advises the university administration on the implementation of policy and procedure to promote adherence to these standards that minimize risks. It provides a wide range of services designed to ensure the university is meeting its record-keeping responsibilities. Furthermore, the records and information management program will address the following areas:

1. Develop a strategic records and information management program that ensures compliance with federal and state law, board of regents' policy and procedure, and financial accountabilities.
2. Lead in the creation, implementation, and enforcement of risk-based university-wide records policies applicable to all locations including those for storage and retrieval of active, inactive, and permanent records while promoting appropriate accountability and transparency.
3. Lead in the identification of vital records and the creation, implementation, and enforcement of a disaster recovery, business continuity, and vital records protection plan.
4. Analyze and evaluate records and information management throughout the university and recommend cost effective improvement strategies to promote and foster systematic and efficient records and information management initiatives.
5. Provide guidance to administer inventory audits of physical and el5.9(me)do-2(e)4(.00f)-2(s)-J

14. Provide guidance for establishing working relationships with business partners to ensure compliance with the Records and Information Management Program; thus, identify areas for enhancement.
15. Maintain an active program for the economical and efficient management of university records and information, in various formats.
16. Promote the use of progressive and innovative technologies to create and manage records.
17. Preserve the history and the evidence of the university for scholarly research and public good. Balance historical value with cost, practicality, clutter and other consideration.

(04-21-10)

R05.08.023. Records Management: Security Breach Involving Personal Information.

To the extent required by applicable law, the University of Alaska will notify any individual whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person as the result of a security breach. However, notice will not be required if a reasonable investigation determines that there is no reasonable likelihood of harm, in which case the university will comply with AS 45.48.010(c), including notice to the Attorney General.

For purposes of this regulation, “personal information” means information in any form on an individual that is not encrypted or redacted, or is encrypted and the encryption key has been accessed or acquired, and that consists of a combination of the individual’s name or initial and last name, and one or more 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.

The following factors, among others,

- The extent to which the compromise indicates a directed attack to acquire personal information, such as a pattern showing a machine containing personal data was specifically targeted.

Acquisition determinations will be made in accordance with delegated authority and this regulation: in the case of electronic records, by the applicable MAU Director of Information Resources, in concurrence with the chief information technology officer and general counsel; in