REGENTS' POLICY
PART II - ADMINISTRATION
Chapter 02.07 - Information Resources

P02.07.010. General Statement: Information Resources.

Within the limits of facilities, resources, and personnel, the university shall establish, through university regulation, and MAU rules and procedures, a framework for access to, and the responsible use of, university information resources.

(02-18-00)

P02.07.020. Information Resources Definitions.

A. In this chapter

1. "information resources" includes the systems and networks owned, leased, or operated by the university, as well as the software and data resident on the systems and networks; and

2. "user" means an individual, including but not limited to, students, faculty, staff and affiliates, who accesses, transmits or stores data on information resources

B. Other definitions for this chapter may be established in university regulation.

(02-18-00)

P02.07.030. Objectives for Management of Information Resources.

Information resources shall be managed in a manner that will:

A. respect First Amendment rights and privacy, including academic freedom;

B. reasonably protect against misrepresentation, tampering, destruction, liability and theft of intellectual efforts;

C. maintain the integrity of university information resources;

D. allocate finite resources based on prioritized needs; and

E. protect the confidentiality of sensitive data collected under research grants and contracts with outside agencies.

(02-18-00)

P02.07.040. Access.

Access to information resources shall be provided to university faculty, staff, students, and affiliates to further the university's mission of instruction, research and public service. Access to information resources shall be granted based on relevant factors, including legal and contractual obligations, privacy, the requester's need to know, information sensitivity, and risk of damage to or loss by the university.

(02-18-00)

P02.07.050. Standards for User Conduct.

Users:

A. by virtue of their use of information resources agree to comply with this chapter and university regulation;

B. shall obtain proper authorization to use information resources;

C. shall use information resources in a responsible manner, which includes respecting the rights of other users, the integrity of the controls and physical facilities, and compliance with license or contractual agreements, regents' policy, university regulation, and local, state, and federal law; and,

D. shall avoid disruption or threat to the viability of information resources and similar resources to which they are connected.

(02-18-00)

P02.07.060. Protection and Enforcement.

A. The university shall establish procedures designed to protect information resources from inappropriate disclosure, misrepresentation, unauthorized access, alteration, or destruction, whether deliberate or unintentional. The university does not, however, undertake responsibility for protecting individuals against the existence or receipt of material that may be offensive to them or harmful to equipment, software or data. The university shall establish procedures for securing its information resources against unauthorized access or abuse to a reasonable and economically feasible degree.

B. Violations of the standards for user conduct:

1. may subject employees to disciplinary action including termination;

2. may subject students to disciplinary action including expulsion according to the Student Code of Conduct procedures; and

3. may also subject violators to criminal prosecution.

C. All users should be aware that violations of copyright laws may also subject them and the university to substantial legal liabilities. Information Resources Personnel may implement measures, including temporary revocation of access and other protective action, to protect against disruption or damage to the university's information resources or alleged or perceived violations of copyright laws or other liabilities.

D. Only to the extent that there is a need to know in order to protect the privacy of data and communications, address a malfunction, maintain the secure and efficient operation of the system or avoid potential legal liability relating to the operation of the Information Resources system, Information Resources Personnel at the university may access the content of electronic communications and copy and examine any files or other information resident on or processed through Information Resources.

E. Information resources personnel shall, to the extent practicable, maintain confidentiality of files and information, other than evidence of conduct threatening the security of information resources, that are accessed pursuant to subsection D of this section. If, however, the director of information resources or the person fulfilling that function, in consultation with university general counsel, concludes that files or information resident on or processed through university systems suggest the reasonable possibility of a violation of state or federal statute or regulation, regents' policy , or university regulation, such files and information may, subject to subsection G. of this section, be disclosed to university personnel or law enforcement authorities without a search warrant.

F. Information Resources Personnel shall comply with all federal and state statutes and regulations that limit access to, or establish prerequisites to accessing or disclosing, files and information, including that pertaining to confidential or proprietary research, resident on or processed through Information Resources.

G. Subject to the qualifications set out in E. of this section, users may have a reasonable expectation of privacy in personal information unrelated to employment contained on information resources or in files devoted primarily to the user. University personnel, other than Information Resources Personnel, may not access or monitor information for which a user has a reasonable expectation of privacy that is residing on or transiting through the Information Resources system without a reasonable basis for suspecting that evidence of misconduct will be found.

H. Information resources personnel may not access the content of electronic communications or copy or examine any files or other information resident on or processed through Information Resources except as authorized by subsection D. of this section or upon a valid request made in accordance with regents' policy or university regulation, or as required by state or federal law.

(02-18-00)

P02.07.066. Mobile Device Security.

A. University employees and students using a laptop computer or mobile device (e.g. portable hard drives, USB flash drives, smartphones, tablets) are responsible for the university data stored, processed or transmitted via that computer or mobile device and for following the security requirements set forth in this policy and other applicable information resources policies and regulations regardless of whether that device is the property of the university or the individual.

B. The use of unprotected mobile devices to access, store, manipulate or transmit university non-public information as defined in R02.07.094 is prohibited regardless of whether or not such equipment is owned or managed by the university.

C. The chief information technology officer is responsible for coordinating with the campuses in the development of consistent measures and business practices for ensuring the security of non-public data on mobile devices.

Reference: Alaska Statutes Chapter 45.48 Personal Information Protection Act

(02-19-15)

P02.07.070. Administrative Responsibilities.

A. An MAU may establish rules and procedures to define conditions and enforcement mechanisms for use of information resources under its control. MAU statements must be consistent with this policy and university regulation and published in a manner reasonably designed to make these conditions known to users.

B. The university reserves the sole right to limit, restrict or extend access to its information resources.

(02-18-00)

P02.07.080. No Rights of Actions Against the University.

Nothing in this chapter or university regulation is intended to create, extend or support any cause of action or other claim for damages against the university or its employees acting within the scope of their employment.

(02-18-00)

UNIVERSITY REGULATION
PART II – ADMINISTRATION
Chapter VII – Information Resources

R02.07.010. General Statement – Information Resources.

MAUs shall establish rules and procedures for the management of information resources in accordance with regents' policy and university regulation.

(01-31-01)

R02.07.020. Information Resources Definitions.

In this chapter and, under the authority of P02.07.020.B, in regents' policy, unless the context requires otherwise,

A. "director of information resources" means the senior person with direct management responsibilities for information resources at an MAU, or that person's designee during periods of absence;

B. "information resources" means the information systems and information networks owned, leased, or operated by the university, regardless of the source of funding, and includes the data, software and other information resident on systems or carried over networks; in addition to this chapter, this definition applies to all information resources acquired and controlled by:

1. system administration, the financial, human resource, and student information systems operated for the entire university system;

2. university campuses, the campus-wide networks, central computing resources, licensed software or databases of main campuses and extended sites;

3. departments or other units, the departmental workstations and servers, or systems

4. individual faculty, staff, and students, in their capacity as university employees.

C. "information resources personnel" means those university employees and contractors who, as part of their assigned or delegated responsibilities, exercise management of, control of access to, maintenance of, diagnose problems on, repair, or audit software on information resources; information resources personnel may work in any unit; in addition to campus-wide service organizations and may include individuals with these responsibilities for institutes, for colleges and departments, extended sites or for specific laboratories or research projects that operate information resources;

D. “information system” means the entire suite of hardware, software, data, and network connections that stores, manipulates, and disseminates, usually over a data network, a particular category of information;

E. “manager” means a person with responsibility or authority for a particular information resource; manager responsibilities include determining access privileges of users, the procedures for input, integrity, or dissemination of data, and security measures protecting the resource;

F. “network” means the physical infrastructure that carries voice, video and data within an MAU up to and including connections to external networks or providers; a network includes switches, routers, firewalls, store and forward devices, software used to manage the network, and all cabling and connecting equipment up to but not including user devices such as desktop computers, printers, or telephone handsets;

G. “private Information” means information contained on or transiting through information resources that is:

1. labeled with the user's name and bears the designation "personal" or "private," for example "personal information of Jane Doe"; or

2. labeled with the name of a user who is a student but is not also an employee, stored in an area reserved for the exclusive use of that student, and not otherwise designated as “public” or “shared”; and

3. in either case, not commingled with information related to university operations to which other university personnel may need access within the scope and course of their employment;

H. “restricted Information” means information contained on information resources, the access to or use of which is limited or controlled by:

1. a valid contractual restriction applicable to the university of which the user is or should be aware;

2. a provision of state or federal law, regents' policy, university regulation, or agreement of the user; or

3. a clear, valid directive to the user;

I. “sensitive information” means university information contained on or transiting through information resources that is:

1. labeled with the user's name and bears the designation "sensitive," for example "sensitive information of Ron Roe;" and

2. not commingled with information related to university operations that other university personnel would normally access; but

3. to which the user's superiors or advisors might need access within the course and scope of their employment under unusual circumstances;

J. "server" means the portion of an information system consisting of hardware, operating system, and information implementing access and storage policies, but not the target data or users' information;

K. "system administrator" means a person who has functional responsibility for day-to-day efficient operation of an information resource such as a computer system, database, or network components; as such, a system administrator has extraordinary access to information on such systems to implement policies and diagnose problems;

L. "university information" means information contained on or as part of information resources that is developed or received by the university, by an employee acting within the scope of employment for the university, or by a private contractor for the university;

M. "user" means an individual who accesses, transmits, or stores information on an information resource; "user" includes students, faculty, staff, and affiliates of the university given access to university information resources; "user" also includes guests and visitors of the university, as well as members of the public who access, transmit, or store information on an information resource;

N. "written agreement" means an undertaking or assent to an undertaking of a person or entity that is reduced to some tangible, electronic, or other reliable medium; assent may be manifested through the point and click process.

(10-01-01)

R02.07.030. Objectives for Management of Information Resources.

A. Information resources regulations and the MAU rules and procedures based on them are intended to foster an environment that will:

1. respect First Amendment rights and privacy of persons, including academic freedom;

2. reasonably protect against misrepresentation, tampering, destruction, and theft of intellectual efforts;

3. maintain the integrity of university information resources;

4. allocate finite resources based on prioritized needs;

5. protect the confidentiality of private, sensitive and restricted information, including research data as well as university information;

6. satisfy requirements for privacy and confidentiality of data arising from grants or contracts with external entities such as foundations, corporate partners, or government agencies, and relevant laws;

7. facilitate and enhance communication, collaboration, and sharing of information in support of the academic mission of the university;

8. not be interpreted to impair employee rights to intellectual property; and

9. minimize legal liability of the university related to information resources.

B. Consideration of these objectives is appropriate in resolving issues not expressly governed by university regulation or MAU rules or procedures.

(01-31-01)

R02.07.041. Access Authorization: General Statement.

A. Information resources may not be accessed without express or implied authorization. Authorization granting access to information resources may be granted contingent upon the user affirming an understanding of, and agreement to, general or specific restrictions and procedures relative to access, disclosure and use.

B. Restricted information or sensitive or private information of others may only be accessed or disclosed as provided by these regulations. University information should only be accessed or disclosed as appropriate to the user's status and function.

(01-31-01)

R02.07.042. Written Authorization Requirements for Information Resources Personnel.

Written authorization of a director of information resources is required for information resources personnel to access restricted, sensitive, or private information. Written authorization may not be granted unless otherwise authorized by regents' policy or university regulation, and not until the employee has assented, by written agreement, to the following terms:

> "In consideration of my employment and the authorization to access restricted, sensitive, or private information, to the fullest extent allowed by law I promise to not disclose any information obtained in the course of performing my duties as an information resources person, except either directly to or through my supervisory chain to my director of information resources. If I claim that my director of information resources or designee has failed to report a matter of public concern, before I report such matter to appropriate authorities, I will disclose the matter in writing to the office of the university general counsel for determination of how

the information might be further disclosed in an appropriately confidential manner."

(01-31-01)

R02.07.044. Granting or Denial of Access.

Access to information resources will be granted or denied to university units, faculty, staff, students, and affiliates based upon relevant factors, including protection of intellectual property rights, legal and contractual obligations, security, privacy, the individual's need for the information or for access to the resource, and the risk of damage to, liability of, or loss by, the university.

(01-31-01)

R02.07.046. Temporary Suspension or Restriction of Access.

A. Pursuant to the guidelines set out in this section, information resources personnel may temporarily suspend or restrict access to information resources to which a particular university unit, individual, or class of individuals would otherwise have access.

B. Only persons with written authority to do so may temporarily suspend or restrict access.

C. The suspension or restriction should be no greater in scope or duration than is appropriate to protect information resources.

D. A prompt attempt should be made, when appropriate, to resolve the circumstances giving rise to the suspension or temporary restriction by making an explicit request to the user subject to the suspension or temporary restriction consistent with preserving the integrity and utility of the information resource.

E. Persons suspending or restricting access should promptly refer unresolved issues related to suspension or temporary restriction of access to appropriate MAU authorities for long term resolution and possible discipline.

(01-31-01)

R02.07.048. Disciplinary Action for Unauthorized Access or Disclosure.

A. Disciplinary action, up to and including expulsion from the university or discharge from employment, may be imposed in response to:

1. intentionally, knowingly, recklessly, or negligently accessing information resources without authorization;

2. intentionally, knowingly, recklessly, or negligently accessing information resources contrary to a prohibition or limitation, of which the user knows or should know, that is contained in a state or federal law, regents' policy, university regulation, agreement, acceptable use policy, contract or other valid restriction; or

3. intentional, knowing, reckless, or negligent unauthorized disclosure of restricted, sensitive, private or university information contrary to an agreement of the user, regents' policy, university regulation, or law.

B. In imposing disciplinary action, each MAU shall take into account evidence of the intentions of the user, that is whether the action appears to be intentional, reckless, negligent, or otherwise, the severity of the conduct, and the sensitivity and scope of the information resources compromised.

C. If users are disciplined, they will be informed of their right of appeal under regents' policy and university regulation.

(01-31-01)

R02.07.050. Standards for User Conduct.

Users are responsible for obtaining authorization for access to information resources. Use must be responsible and in accordance with state and federal law, regents' policy, university regulation, obligations of written agreements entered into by the university, MAU rules and procedures, relevant acceptable use policies and any written agreements entered into by the user.

(01-31-01)

R02.07.051. Use Guidelines.

Failure to act in accordance with the following general guidelines applied to the networked computing environment constitutes misconduct and may constitute a crime. Users are expected to:

A. recognize that the laws, regents' policy, and university regulation governing conduct generally, also govern activities conducted on information resources and not assume that because something is technologically possible that it is legal, ethical or authorized;

B. respect others' privacy and the right to freedom from harassment and intimidation and know that using of information resources to harass or disrupt the work of others is prohibited;

C. respect copyright and other intellectual property rights; copying files or passwords belonging to others or to the university may violate copyright law or constitute plagiarism or theft; software licensed by the university or otherwise resident on university equipment must be used in accordance with any applicable license agreement; violations of the terms of software license agreements are not within the scope of university employment and constitute misconduct; the university may require violators to reimburse and pay fines or damages and impose disciplinary action up to and including dismissal from employment or expulsion from the university;

D. know that any modification of information resources without authorization, including altering data, introducing viruses, or damaging files is prohibited;

E. clearly and accurately identify the author in all communications; concealment or misrepresentation of an author's name or affiliation to mask irresponsible or offensive behavior is a serious abuse; appropriating the identifiers of other individuals to misrepresent authorship or ownership constitutes fraud;

F. obtain authorization to access information resources as established in MAU rules and procedures or by the information resource personnel with authority to manage the information resource;

G. maintain the integrity of passwords and other security technologies; users must not evade, disable, or crack password or other security provisions; or circumvent, alter, or disable access permissions, records of them, or technologies implementing access restrictions; users must not share individual account passwords unless willing to accept responsibility for actions of those with whom the passwords are shared;

H. use resources efficiently and adhere to limitations or restrictions on computing resources, such as storage space, time limits, or amount of resources consumed, when asked to do so by the managers of information resources; objections to such restrictions may appropriately be brought to the proper authority, but this does not remove the user’s obligation to adhere to restrictions in force;

I. recognize the limitations on privacy inherent within the electronic environment and know that

1. intended security of electronic files may be compromised;

2. network communications and the actions of users on many shared information systems are routinely logged and archived;

3. information “deleted” by users may nevertheless be preserved in routine backup files, archives, or audit trails;

4. information resources personnel may view the contents of files as part of their responsibilities;

5. in some circumstances, law enforcement officials may receive access to users' files and records;

J. to the extent possible, take steps in advance to assure that university information in encrypted format or otherwise protected from access can be accessed by university personnel who are authorized to do so pursuant to regents' policy and university regulation; to the extent possible, provide encryption keys and passwords to appropriate university personnel in response to legitimate requests or direction.

(01-31-01)

R02.07.052. External Systems.

Users' responsibilities extend to cover systems outside the university when accessed via university information resources; for example, electronic mail or remote logins using the university's internet connections. Network or computing providers outside the university may additionally impose their own conditions of appropriate use, for which users are responsible.

(01-31-01)

R02.07.053 Personal Use of University Information Resources.

A. Employees, including student employees, do not have an inherent right to use information resources for personal purposes. Campuses or departments may prohibit or restrict use of information resources for personal purposes. Any such prohibition or restriction must, as a legal matter, not be motivated by any illegal reason. Any such prohibition or restriction should, as an internal management matter, be reasonable in light of specific needs or mission and shall be in writing.

B. To the extent not otherwise restricted or prohibited, employees, including student employees, are authorized to use information resources for personal noncommercial purposes, so long as the use is consistent with regents' policy, university regulation, MAU rules and procedures, state and federal law and management directives.

C. The Alaska Executive Branch Ethics Act (Alaska Statute 39.52) applies to all university employees. The Act prohibits the use of state or university information for the personal or financial benefit of an employee, family member or cohabitant of the employee, unless the information has been "publicly disseminated" as that term is defined by state regulation. Employees are expected to comply with the Alaska Executive Branch Ethics Act and associated regulations. Extreme care should be exercised to make sure that university information has been publicly disseminated before it is used for such personal or financial benefit.

D. The Alaska Executive Branch Ethics Act also prohibits employees from using university resources, which would include information resources, for any commercial purpose. The General Counsel has concluded that this restriction prohibits employees from gaining any commercial advantage from use of information resources that would not otherwise be available to the employee without the employee incurring additional cost and from making any use of information resources for a commercial purpose that would cause the university to incur any additional cost.

E. The Alaska Executive Branch Ethics Act does not apply to students in their capacity as students.

(01-31-01)

R02.07.054. Content Restrictions.

Managers of information resources may impose on shared information resources under their management constraints and measures designed to maintain system functionality and to assure data integrity and security. Such constraints and measures may lead to limits or restrictions on some types of activities. Restrictions based solely on the content of information must not conflict with the academic mission of the university and right to individual freedom of expression. Content restrictions are thus appropriate only in specific limited circumstances, such as the following:

A. Limited-Public Forums

Limited-public forums, as distinguished from private communication or public forums, may have content restrictions so long as they are based on topic rather than viewpoint. A discussion forum, for example, maintained specifically for the discussion of mineral resource distribution might, to keep discussions on the intended subject, reasonably prohibit discussion of the politics of states containing the resources or financial data on companies mining resources.

B. Sending Messages to Large Mailing Lists

Information resources personnel may adopt guidelines for the use of large mailing lists for unsolicited messaging which take into account the likely demand on resources, including resources required to respond to problems or complaints, relation of the sender to recipients, and appropriateness for the intended use of the system.

C. Harassing Messages

Harassing messages or public displays may be restricted and removed from University information systems.

D. Disproportionate or Debilitating Amount of Resources

Forms of activity in a networked environment that utilize a disproportionate or debilitating amount of resources.

E. Commercial Sites

Company logos or hypertext links to commercial sites on university publications, including institutional web sites, may appear to be commercial endorsements of products or services. Information resources personnel may direct that such references be clarified or removed.

F. Illegal Content

Illegal content, including obscene material, child pornography, efforts to incite violence, or communications in furtherance of conspiracy to commit a crime, is prohibited.

(01-31-01)

R02.07.061. Protection.

Each MAU shall establish rules and procedures, and shall follow practices designed to protect, to a reasonable and economically feasible degree, information resources from deliberate or unintentional inappropriate disclosure, misrepresentation, unauthorized access, alteration, or destruction. The university does not, however, undertake responsibility for protecting individuals against the existence of or receipt of material that may be offensive to them or harmful to equipment, software or data.

(01-31-01)

R02.07.062. Enforcement.

A. Violations of the standards for user, university personnel, and information resources personnel conduct that are set out in this chapter, other regulations, regents' policy, MAU rules and procedures, and other laws, may:

1. subject employees to disciplinary action including termination;

2. subject students to disciplinary action including expulsion according to the Student Code of Conduct procedures;

3. result in temporary or permanent denial of access to information resources; and

4. subject violators to criminal prosecution.

B. Violations of copyright laws may also subject a user and the university to substantial legal liabilities.

(01-31-01)

R02.07.064. Protection of Privacy and Academic Freedom.

A. The university takes privacy and academic freedom very seriously. Information resources personnel at the university may access the content of electronic communications and copy and examine any files or other information resident on or

processed through information resources only to the extent that there is a need to know in order to:

1. protect the privacy of data and communications;

2. address a malfunction;

3. maintain the secure and efficient operation of information resources; or

4. avoid potential legal liability relating to the operation of information resources.

B. Information resources personnel occupy a special relationship to information resources and those individuals who might be affected by disclosure of private, sensitive, or restricted information. To the extent practicable, information resources personnel shall maintain confidentiality of files and information, other than evidence of conduct threatening the security of information resources, accessed under A. of this section.

C. If an MAU director of information resources, in consultation with university general counsel and the system administration director of information resources, concludes that files or information resident on or processed through information resources suggest the reasonable possibility of a violation of state or federal statute or regulation, regents' policy, or university regulation such files and information may, subject to G. of this section be disclosed to university personnel or law enforcement authorities without a search warrant.

D. Information resources personnel who encounter, through the exercise of their responsibilities, what to them appears to be a reasonable likelihood of a violent criminal act imminent or in progress may report that fact to appropriate law enforcement and university authorities only if a reasonable attempt to contact the system administration director of information resources and general counsel is unsuccessful.

E. Information resources personnel shall comply with all federal and state statutes and regulations that limit access to, or establish prerequisites to accessing or disclosing, files and information, including that pertaining to confidential or proprietary research resident on or processed through information resources.

F. Subject to the above qualifications, users may have a reasonable expectation of privacy of private and sensitive information as those terms are defined in R02.07.020. University personnel, other than information resources personnel, may not access or monitor private or sensitive information that is residing on or transiting through the information resources without a reasonable basis for suspecting that evidence of misconduct will be found. Absent a legitimate concern that evidence will be lost, damaged, or destroyed unless immediate action is taken, university personnel other than information resources personnel may not access or monitor private or sensitive information of others without the consent of the holder of the private or sensitive information or the approval of general counsel and a relevant MAU human resources director, or designee.

G. Information resources personnel may not access the content of electronic communications or copy or examine any files or other information resident on or processed through information resources except as authorized by A. of this section or upon a valid request made in accordance with regents' policy or university regulation, or as required by state or federal law.

(01-31-01)

R02.07.065. Security Breach Involving Personal Information.

The regulation regarding security breaches involving personal information is located in Regulation 05.08.023.

(08-30-07)

R02.07.066. Mobile Device Security

A. Protection of Non-Public Information

1. The proper personnel within the university need to be made aware of the loss of university non-public information accessed through, stored within, manipulated by, or transmitted to, its information resources. In some instances the University has a duty to report loss of information to third parties. Therefore faculty, staff, students, affiliates, and others with access to university information resources are required to protect non-public information to which they have access and report any loss of control of that information.

2. Every user of computer equipment, including laptop computers or other mobile devices (e.g. portable hard drives, USB flash drives, smartphones, tablets) must use reasonable care to protect university non-public information, as outlined in the Regents' Policy Chapter 02.07 – Information Resources, which details examples of non-public information and the requirements for securing this data during transmission and at rest.

3. Protection of non-public information against physical theft or loss, electronic invasion, or unintentional exposure requires a variety of measures, including both user care and a combination of technical protections, such as authentication and encryption, working together to secure data and devices against unauthorized access.

4. Any user of computer equipment being used to access, store, manipulate, or transmit university non-public data is encouraged to contact the chief information technology officer (CITO) or designee to determine if appropriate protections are in place and to seek guidance as to enabling the security measures for that equipment, particularly if the equipment being used is not university-owned or operated. Regents' Policy Chapter 02.07 – Information Resources details requirements for securing this data during transmission and at rest.

B. Reporting Loss/Theft of Equipment or Data

Any university faculty, staff, students, affiliates, or others utilizing computer equipment, including any mobile device, to access, store, manipulate or transmit university non-public data are expected to secure that equipment at all times, including measures to protect data if the equipment is left unattended. The university does not reimburse for lost or stolen personally owned laptop computer(s) or other mobile device(s).

In the event any university-owned or managed laptop computer or mobile device is lost or stolen, the user should:

1. Immediately report the theft or loss to the respective campus support center/helpdesk and to the respective campus University Police Department or local law enforcement.
2. Contact the statewide or campus Office of Information Technology to report the incident and provide details to the chief information security officer to facilitate a risk assessment
3. Contact the statewide or campus Risk Management Office to file the appropriate report or claim.

In the event any computer equipment or mobile device containing university non-public information is lost or stolen, even if that equipment is not university-owned or managed, or if passwords or other system access control mechanisms protecting university non-public data are lost, stolen or disclosed, or are suspected of being lost, stolen or disclosed, all users have a duty to notify the chief information security officer within the Statewide Office of Information Technology immediately.

C. Use of Personal Mobile Devices

The use of personal laptops and other mobile devices to conduct university business involving non-public data is not encouraged but is allowed when other means are not available. Any use of personal computer equipment to access, store, manipulate or transmit university non-public data shall comply with regents' policy and university regulation.

Individuals are expected to ensure the personal computer and/or mobile device is in good order:

- The device has the latest and all necessary critical security updates installed;
- The user is using a suitable internet connection firewall (where appropriate);
- The user is using an appropriate anti-virus with up-to-date virus definitions (where appropriate);
- The user is using an appropriate anti-spyware/malware program (where appropriate) and schedule scans regularly;

- If the device is infected with a virus or other malware infection, that the user take appropriate action to disinfect the machine/device before its reconnection to the network.

Faculty, staff, students, affiliates, and others with access to university information resources acknowledge that utilization of any personally owned computer equipment, including laptop computers and mobile devices, to access, store manipulate, or transmit non-public university data or resources leads to a reduced expectation of privacy with respect to that equipment, and that the equipment is subject to inspection by the university in the event that equipment has been compromised or otherwise may have exposed non-public university data, or has been utilized in furtherance of a violation of regents' policy or university regulation, or may contain evidence relevant to a determination of whether or not such compromise, exposure, or violation may have occurred. Such inspection or examination will be limited to that degree necessary to determine whether and to what extent such compromise, exposure or violation has occurred; what safeguards were not in place or otherwise failed to prevent the occurrence; what remediation steps are appropriate; and what preventive steps will be necessary to avoid recurrence. A request for the employee to consent to the inspection of a personal device can be made by any information resources personnel. A user unwilling to cooperate in the inspection may request an immediate review by the chief information security officer or designee, who will make the final determination whether an inspection under this section is to be conducted.

Should the chief information security officer determine that an inspection is necessary, any subsequent inspection and investigation will comply with all applicable regents' policies, university regulations, state, and federal laws.

D. Securing Information on Mobile Devices

The CITO will coordinate the establishment of appropriate guidelines for securing mobile devices and will promulgate these as technology changes. For further information on reporting security incidents and implementing security practices see the Office of Information Technology website.

E. Encryption

Devices that do not support encryption must not be used to access, store, manipulate, or transmit non-public university information. Loss of encrypted data does not need to be reported. The loss of unencrypted university data must be reported to the CITO.

F. Additional Requirements.

In addition to appropriate information handling requirements determined by the general data classification under Regents' Policy Chapter 02.07 – Information Resources and university regulation, sector-specific data (e.g., Payment Card Industry Data Security Standard (PCI-DSS), Health Insurance Portability and Accountability Act (HIPAA), etc.) may have additional requirements. Individual divisions, schools, colleges, Institutes or departments may impose additional information security requirements beyond those set forth in this regulation and as may be required by sponsors, government agencies or other external entities. Users should check with the Statewide Office of Information Technology for assistance.

G. Requirements When Traveling Overseas

University personnel and students carrying university-issued laptops or mobile devices while traveling abroad, whether on business or for pleasure, must comply with data protection measures in this regulation, with U.S. trade control laws, with University Regulation 10.07.035 – Export Control Licensing, and with the laws of the destination country. U.S. export control laws may prohibit or restrict such activities absent special U.S. government licenses. For current guidance on traveling abroad with a laptop or other mobile device, users should consult with the Statewide Office of Information Technology, the relevant funding agency, or institution chief information security officer.

H. Compliance

University faculty, staff, and students must understand the restrictions described here, and that failure to comply with this policy and regulation may lead to prohibition of any use of personal devices to access, store, manipulate or transmit non-public university data, or prohibition of all access to all university information resources, public or non-public, whether through personally-owned or university-owned equipment, and may further result in disciplinary action as outlined in Regents' Policy 02.07.060 – Protection and Enforcement, up to and including termination for employees and up to and including expulsion for students.

(04-02-15)

R02.07.070. Administrative Responsibilities.

Each MAU shall make reasonable efforts to communicate to users their responsibility to comply with regents' policy, university regulation, contractual obligations, acceptable use policies, and MAU rules and procedures.

The university and information resources managers will provide appropriate security measures for all information resources that will:

A. protect the integrity of information resources;

B. safeguard the integrity and confidentiality of information to a reasonable and economically feasible degree consonant with the nature of the information in the resource;

C. minimize disruptions and unscheduled outages of access to information resources;

D. mitigate the loss or damage in the event of actions resulting in the loss of or damage to Information Resources, or the invasion of Users' privacy.

(01-31-01)

R02.07.072. Managers' Responsibilities.

A. Managers must inform themselves of evolving security threats to the information resources for which they are responsible, and must be responsive to notices of new threats and counter-measures. Before installing a server, the responsible manager must be prepared to commit the time and resources necessary to ensure proper management. Proper management includes such responsibilities as the following:

1. designating a properly trained system administrator with the time and expertise to understand the technical implications of the systems, stay current on vulnerabilities, software patches and new releases, and being able to address urgent issues on an immediate basis;

2. identifying responsibilities for data capture and maintaining the integrity of data; data integrity denotes that data accurately reflect information, have not been corrupted accidentally or deliberately, and retain consistent valid relations with other data in the system;

3. communicating to users the appropriate use of data;

4. facilitating use of security mechanisms to protect the integrity and privacy of data, including secure authentication, robust authorization or permission techniques; techniques may include encryption of network login and data retrieval, physical security of systems, and audit trails.

B. Directors of information resources are authorized to take appropriate steps, including disconnecting improperly managed systems if those systems endanger the integrity of institutional networks, systems or services. Managers are responsible for compliance with directives of the directors of information resources.

(01-31-01)

R02.07.074. System Administrator Responsibilities.

A. System administrators have unique privileges and responsibilities including the following:

1. system administrators shall protect individuals' passwords and other information or technologies that maintain integrity, confidentiality, and security of their systems;

2. system administrators shall not browse, inspect or copy users' information whether on-line or from backups, except as follows:

a. to inspect those files necessary to diagnose or respond to system malfunction, disproportionate or debilitating resource consumption, intrusion, compromised system integrity, or to respond to plausible complaint of abuse, as described in R02.07.062, but an administrator may not disclose the information content thus gained to others except upon specific authorization of the director of information resources, after consultation with the statewide director of information resources and university general counsel;

b. performance of automated system administrative functions that do not require system administrators to read individuals' information; such functions include backup and restoration, software license compliance measures or audits, removal or archiving of files based on age, size or other appropriate criteria, and removal or archiving of files of users whose accounts or permission are no longer valid;

c. upon request of, or with permission of, the user or data owner;

d. to perform routine general scans of the system they administer for intrusion, compromised security, cracking efforts, or prohibited activities such as software to crack passwords or deny service, or unauthorized copies of password files, using generally accepted security techniques;

3. system administrators shall not compile or collect information for the purpose of assessing a particular individual user's information usage patterns except as part of a duly authorized investigation;

4. systems that routinely log or otherwise collect information about individual users' information resource use must employ safeguards to prevent misuse of or inadvertent dissemination of this information; usage patterns directly attributable to particular individuals shall be considered confidential information to be seen or used only for authorized purposes; system administrators are encouraged to destroy records acquired under this paragraph when they are no longer required or suitable for authorized purposes; however, information subject to outstanding subpoena or public records request may not be destroyed;

5. system administrators shall configure software systems so as to facilitate the confidentiality of User communication;

6. system administrators shall stay abreast of any vulnerabilities of their systems and manage security in accord with appropriate recommendations; system administrators are responsible for remaining up-to-date with security issues relevant to the systems they administer, including vendor information channels and computer emergency response team bulletins;

7. system administrators should configure their systems to minimize the chance for abuse, and act promptly to end abuses upon notification.

B. Except as authorized by these regulations, system administrators shall not compile or log information on information systems for which they do not have administrative responsibilities.

(08-25-14)

R02.07.080. No Rights of Actions Against the University.

Nothing in this chapter is intended to create, extend, or support any cause of action or other claim for damages against the university or its employees acting within the scope of their employment.

(01-31-01)

R02.07.090. Data Classification Standards: General Statement

The University of Alaska (UA) generates, acquires, and maintains a large number of electronic records. In addition, UA often enters into relationships with third parties who maintain electronic records and information associated with these relationships. UA, as well as its affiliates, are often legally required to limit access to, distribution of, and/or disclosure of electronic records and information. The approach at UA is to adopt a classification scheme for all data.

(08-27-09)

R02.07.091. Data Classification Standards: Purpose

Data classification standards help personnel who own and maintain information resources and systems to determine the sensitivity of the data within those systems. This regulation is designed to prevent the following:

--Unauthorized internal access to electronic information
--Unauthorized external access to electronic information
--Illegal or otherwise inappropriate use of UA electronic information
--Loss, corruption, or theft of UA electronic information

(08-27-09)

R02.07.092. Data Classification Standards: Applicability

This classification standard applies to all data associated with UA business; to any other data caches located at any UA entity and covered by statutory or regulatory compliance requirements; and to data caches on the information systems of UA affiliates. Data associated with UA-hosted research that represents significant intellectual property interests are subject to this standard and may be subject to other specific protective requirements. These standards apply to all individuals who have access to and use UA information systems and data, particularly UA systems owners and designated custodians who have special responsibilities under the standards. Questions about the applicability of this standard can be forwarded to the UA Chief Records Officer.

(08-27-09)

R02.07.093. Data Classification Standards: Data Classification and Examples

The nature of any particular data set largely determines what measures and operational practices need to be applied to protect it. To help clarify the specific minimum requirements for UA data security, three classes of data are defined. The people who are accountable for protecting the data must understand and inventory their data assets according to these categories.

A. Restricted Data: Data classified as restricted maybe subject to disclosure laws and warrant careful management and protection to ensure its integrity, appropriate access, and availability. This information is considered private and must be guarded from disclosure. Unauthorized exposure of this information could contribute to ID theft or financial fraud, and violate State and Federal law. Unauthorized disclosure of restricted data could adversely affect the university or the interests of individuals and organizations associated with the university.

B. Internal Use Data: This class encompasses information that is generally not available to parties outside the University of Alaska community such as non-directory listings, minutes from non-confidential meetings, and internal websites. Public disclosure of this information would cause minimal trouble or embarrassment to the institution. The university may have a duty to make this data available on demand under the Alaska Public Record Act (AS 40.25.110).

C. Public Data: Public data is data published for public use or has been approved for general access by the appropriate UA authority.

In most cases categorizing the data will be obvious. When in doubt about how a particular data element or data set is classified, data custodians should use caution by defaulting to the higher class of the choices involved. In other words, it is better to err on the side of privacy and security protection until clarification is obtained.

The source data used to produce important reports, such as UA financial records, are treated as restricted or internal use even though the reports created from them are treated as public information. Data classification questions may be forwarded to the UA Chief Records Officer for review.

(08-27-09)

R02.07.094. Data Classification Standards: Categories

The Data Classification Categories table clarifies the nature of each data category and provides criteria for determining which classification is appropriate for a particular set of data. When using this table, a positive response for the most restrictive (highest risk) category in any row is sufficient to place that set of data into that category.

Data Classification Categories

Class	Restricted	Internal Use	Public
Legal Requirements	Protection of data is required by law or best practices	UA has best practice (due care) reasons to protect data	Data approved for general access by appropriate UA authority
Risk level	**High**	**Medium**	**Low**
Consequences of Exposure	The University's reputation is tarnished by public reports of its failures to protect restricted records of students, employees, clients, or research. Such failure may subject the University to litigation.	Data is disclosed unnecessarily or in an untimely fashion, which causes harm to UA business interests or to the personal interests of an individual.	Confusion is caused by corrupted information about enrollment and tuition that is displayed on the official UA web site
Examples of Specific Data	• HIPAA • FERPA • Research – EAR, export controls, ITAR, TCP, safeguarding confidential information • Information required to be protected by contract • Human subjects identifiable research data • Trade secrets, intellectual property and/or proprietary research • Attorney/client privileged records • Payment Card Industry • University banking records • Restricted police records • Computer account passwords • Gramm-Leach-Bliley • Certain affirmative action related data • Alaska Personal Information Protection Act • Library records confidentiality	• Employee Internet usage • Specific technical security measures • UA employee business-related email (including student employees, but only their work-related email) • Location of assets • Faculty promotion, tenure, evaluations • Supporting documents for UA business functions • Public research • Supporting documents for UA business functions • Aggregate human subjects research data • Animal research • Proposal records	• Campus promotional material • Annual reports • Press statements • Job titles • Job descriptions • Employee work phone numbers (with special exceptions) • University of Alaska business records • Employee work locations (with special exceptions) • Employee email addresses (with special exceptions)

(08-27-09)